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

Business Architecture Document for Smart Metering GB

Version 2.0 Status: APPROVED

Date: 17th May 2018

Change History

Version Number	Status	Date of Issue	Reason for Change
0.01	Initial Draft		Initial draft for layout of sections
0.1	Initial Draft for TABASC Review	08/09/2016	Draft issued to TABASC (Stage 1)
0.2	Second Draft for TABASC Review	08/12/2016	Draft issued to TABASC (Stage 2)
0.3	Third Draft for TABASC Review	09/03/2017	Draft issued to TABASC (Stage 3)
0.4	Final Draft for Review	07/06/2017	Draft issued to TABASC, PMA and SSC for final review
0.5	Final for Review	10/08/2017	Final draft issued to TABASC
0.6	For final approval	08/09/2017	Final draft issued to SEC Panel
1.0	Approved	22/09/2017	Approved by SEC Panel, includes updates to refer to current SEC Version
1.1	Approved	06/11/2017	Minor updates to amend SEC version references to SEC 5.11
2.0	Draft	14/03/2018	BAD Version 2.0 (draft 0.1) updates prepared and issued for review
2.0	Draft	10/05/2018	BAD Version 2.0 (draft 0.3) updates prepared and issued for final TABASC review and approval
2.0	Approved	17/05/2018	Approved by TABASC, includes updates to refer to current SEC Version and associate references.

Contents

1 Introduction

The purpose of this document is to lay out the current GB Smart Metering Business Architecture that exists under the Smart Energy Code (SEC), identifying the relevant regulatory instruments that give the Business Architecture meaning and force.

The SEC defines the Business Architecture as:

[The] business architecture which is designed to enable Parties to use the Services and / or to enable Parties, Energy Consumers and those acting on behalf of Energy Consumers to access the functionality described in the Technical Specifications.

This document broadly consists of the following elements:

- Background information about the Business Architecture;
- Target operating model that supports the Business Architecture; and
- Business processes that exists within the Business Architecture (illustrated by use cases, and relevant regulations).

The Business Architecture Document (BAD) is supported by a Business Architecture Model (BAM) that provides a high level view of the processes, associated regulations and where appropriate, Modification Proposals to the relevant elements of the Business Architecture.

SEC Section F1.4 sets out the duties of the Technical Architecture and Business Architecture Sub-Committee (TABASC), which in respect of Business Architecture may be paraphrased as:

- Develop and thereafter maintain the BAD
- Provide advice and support to the Panel in respect of Modification Proposals that may result in changes to the Technical Code Specifications (for instance SEC Appendix AD – DCC User Interface Specification) or that may result in changes to the end to end Technical and / or Business Architecture.
- Provide advice and support to the Panel in respect of Disputes that may relate to the Technical Code Specifications (for instance SEC Appendix AD – DCC User Interface Specification) or the end to end Technical and / or Business Architecture.
- Review (as directed by the Panel) the effectiveness (including in its ability to meet SEC Objectives) of the Business Architecture and report to the Panel on the findings of such review.
- Support the Panel in the Business Architecture aspects of the annual report which the Panel is required to prepare and publish.

- Generally, provide the Panel with advice and support in respect of any aspects of the Business Architecture.

2 Background

This section explains how the Business Architecture was developed.

The Smart Metering Implementation Programme (SMIP) established the Business Process Design Group (BPDG) in 2011. The BPDG was formed of stakeholders from across the energy industry and was charged with providing input and support to the SMIP in order to identify and develop the business processes that industry participants would require to operate Smart Meters via the DCC. The process areas include:

- Install and Commission Smart Meter;
- Operate Smart Meter;
- Decommission Smart Meter;
- Change of Supplier (CoS);
- Access Control;
- Service Management.

The development of these processes, into a Business Process Model (BPM) saw the identification of actors involved, the decision points required and the communications between actors that would enable the model to work. The User Gateway Catalogue (UGC) which laid out, at a high level the Service Requests available to groups of users, for the operation of Smart Meters in GB was developed as a consequence of this work.

The BPM was iterated over time and through consultation with the industry participants and subsequently formed the input to a number of key SMIP artefacts and elements, including:

- The Security Model (where the BPM provided the abstract business processes that formed the basis of the trusty modelling work);
- The functional requirements for the Data and Communications Company (DCC) and its Data Service Provider (DSP) and Communications Service Providers (CSPs); and
- Various sections and subsidiary documents of the SEC including the DCC User Interface Specification (DUIS) and the Message Mapping Catalogue (MMC).

In 2015, a requirement was placed on the Panel to develop and maintain a BAD.

3 Scope

A Technical and Business Design Group (TBDG), a SMIP Transitional Governance Group commissioned the End to End Design Issues Sub-Group (EEDIS) to develop the scope of the BAD. The scope developed by the EEDIS included the Service Requests that are available to each User Role and the processes that apply to them and the interactions between the DCC and Users over various interfaces giving Users access to the DCC Services. In addition, the processes and key infrastructures that secure communications between the DCC and Users as well as any prerequisites that need to be in place to support these processes and interactions we included in the scope.

The following processes were proposed to be included:

- How Devices are added, updated and removed from the Smart Metering Inventory (SMI). This includes the assurance mechanisms that exist under the SEC.
- How to install Smart Metering Equipment Technical Specification 2 (SMETS2) Devices and commission them via the DCC. This includes when SM WAN is not available on the installation date.
- How to read, configure and operate Devices post installation, including the management of Security Credentials.
- How to decommission and replace Devices.
- Certain DCC functions supporting the provision of DCC Services such as Incident Management, Communications Hub (CH) ordering as well as specific processing that the DCC undertakes such as managing Schedules or operating Threshold Anomaly Detection (TAD).

It is worth noting that the design of the DCC Service to support SMETS1 Devices has still to be finalised and that no rights or obligations that may arise from the SMETS1 Service have been laid out in the SEC at this time[1]. The only exception to this is SEC Section N 'SMETS1 Meters', which lays out the route by which the DCC should develop a feasibility report for the enrolment and adoption of SMETS1 Devices into the DCC. Thus, this document does not reflect any of the SMETS1 Business Architecture. Likewise, any new or amended rights or obligations that arise from future SEC releases or changes, beyond Release 2.0, have not been included in this document.

4 Target Operating Model

The SMIP described the vision for Smart Metering[2]:

1.1. The Government is committed to every home in Great Britain having smart energy meters, empowering people to manage their energy consumption and reduce their carbon emissions. Businesses and public sector users will also have smart or advanced energy metering suited to

[1] It is expected that the earliest that SMETS1 Services will be implemented and delivered by the DCC will be delivered in Q4 2018.

[2] https://www.ofgem.gov.uk/ofgem-publications/63541/smart-metering-prospectus.pdf.

their needs. The rollout of smart meters will play an important role in Great 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. The smart meter roll out is integral to the Green Deal, the Government's overarching policy to enable households to reduce the amount of energy they use by improving their energy efficiency.

1.2. Smart meters will provide consumers with more visibility and control of their energy consumption and spending, with real-time information available through in-home displays and other initiatives tailored to consumer needs and preferences. Supported by the Green Deal and other national, local and community-based initiatives to promote energy efficiency, consumers will be empowered to use this information to change their consumption behaviour, thereby becoming more energy efficient and reducing their carbon emissions.

1.3. Smart meters will allow consumers to play a more active role in the energy market and make related cost and carbon savings. Consumers will be able to switch more easily between suppliers and benefit from more innovative energy tariffs, including time-of-use tariffs that support the shift of energy consumption to lower cost time periods.

1.4. Subject to appropriate consumer permissions and protections, suppliers and others will be able to use consumption data to provide better energy efficiency products and advisory services, including automation of energy services to reduce costs and increase comfort and control. The data provided by smart metering may also help inform community initiatives designed to tackle climate change.

1.5. Consumers' interests and benefits will be at the heart of smart metering delivery and consumer protections will need to keep pace with technological change. Vulnerable consumers will need to be protected and the privacy of consumer data assured. Specifications will be required to ensure effective and secure end-to-end operation of the smart metering system, to streamline the change of supplier process and to increase transparency of tariffs, thereby increasing competition. Combined with accurate billing, these features will provide an improved customer experience.

1.6. The smart metering system will enable simplified and improved industry processes. For example, accurate data and improved industry data flows and management systems will enable suppliers to radically simplify and improve the speed and efficiency of customer processes. This will include switching supplier, moving home, bill queries, debt management and tariff changes. Both suppliers and their customers will benefit from an end to estimated bills and site visits to obtain meter readings, as well as the improvement in the ability to detect electricity outages or potential fraud.

1.7. Smart metering will enable the energy industry to manage the generation and distribution system more cost effectively and will facilitate increased use of renewable energy. Time-of-use tariffs and other incentives to manage demand will help to reduce peak demand, which will in turn reduce the need for investment in network and generation capacity. Subject to appropriate consumer permissions and protections, smart metering data will enable network operators to make better informed investment decisions and will support network operators to develop

'smart grids', using the data to plan and manage the distribution and transmission systems so as to reduce costs, losses and outages.

1.8. The smart metering system will provide infrastructure with the potential to support other initiatives. Subject to the introduction of appropriate regulatory arrangements, this may provide a means of supporting smart water metering. With an increasing proportion of consumers owning electric vehicles, there will be potential to charge these vehicles at home using smart meter controls that maximise the use of cheap, low-carbon electricity, or refuel at alternative charging points while paying for the electricity through the customer's energy bill.

4.1 Programme Outcomes

The list below provides a view of the outcomes that the SMIP is intended to facilitate through the roll out and operation of Smart Meters[3]:

1. Energy Consumers will reduce their gas and electricity consumption leading to energy bill savings and a reduction in carbon emissions for Great Britain (GB).

2. Energy Consumer choice and market competition will be achieved by making it simpler for Energy Consumers to switch their energy supplier and by removing barriers for new market entrants in energy supply and new energy services markets.

3. Gas and Electricity Smart Meters with In-Home Display (IHD) linked by a Home Area Network (HAN) - including pre-payment functionality - will be available to all of the GB population, irrespective of where they live and the roll-out will complete by end 2020.

4. The delivery of efficiency and cost savings for energy suppliers and network companies and the minimisation of system costs including through: business process simplification; better targeted network investment; and reduced investment in, and use of, peak electricity generation plant, to enable energy suppliers to reduce energy bills.

5. The system will support (and enable) other critical energy policy commitments, in particular the smart grid, that will enable more effective demand management in the future supporting a world with more reliance on more intermittent new energy supplies such as renewables.

6. The Smart Metering System (SMS) will be able to facilitate new and innovative products and services for the home including third party access that can, with Energy Consumer consent, utilise energy data to support consumers in managing their energy usage – providing improved information to support behaviour change and an interface to smart appliances. Longer term, with the growth of electric vehicles and heating, the ability to control demand will be key to maintaining security of energy supply.

[3] https://www.ofgem.gov.uk/ofgem-publications/63541/smart-metering-prospectus.pdf.

4.2 Programme Objectives

The objectives of the SMIP for the rollout and operation of Smart Meters[4] are:

1. To promote cost-effective energy savings, enabling all Energy Consumers to better manage their gas and electricity energy consumption and expenditure and deliver carbon savings.

2. To promote cost-effective and smoother electricity demand, to support (and enable) other critical energy policy commitments, in particular the smart grid, that will enable more effective demand management in the future.

3. To promote effective competition in all relevant markets (gas and electricity supply, metering provision and energy services and home automation) by removing barriers for new market entrants in energy supply (as an illustration of the competition challenge, less than 1% of GB domestic energy supply is handled outside of the Big 6 energy providers).

4. To deliver improved customer service and consumer choice by energy suppliers, ensuring easier switching, price transparency, accurate bills and new tariff and payment options.

5. To deliver customer support for the SMIP, based on recognition of the Energy Consumer benefits and fairness, and confidence in the arrangements for data protection, access and use.

6. To ensure that timely information and suitable functionality is provided through Smart Meters and the associated communications architecture, to support development of smart grids.

7. To enable simplification of industry processes, resulting in cost savings and service improvements.

8. To ensure that the dependencies on smart metering of wider areas of potential public policy benefit are identified and included within the strategic business case for the SMIP, where they are justified in cost-benefit terms and do not compromise or put at risk other SMIP objectives.

9. To deliver the necessary design requirements, commercial and regulatory framework and supporting activities so as to achieve the timely development and cost-effective implementation of smart metering, and meeting published Programme milestones.

10. To ensure that the Critical National Infrastructure (CNI), metering and data management arrangements meet national requirements for security and resilience and commands the confidence of stakeholders.

11. To manage the costs and benefits attributable to the Programme, to deliver the net economic benefits set out in the Strategic Business Case[5] and to enable suppliers to reduce energy bills.

[4] https://www.ofgem.gov.uk/ofgem-publications/63541/smart-metering-prospectus.pdf.
[5] https://www.gov.uk/government/publications/smart-meter-roll-out-gb-cost-benefit-analysis.

4.3 DCC Services

To deliver these outcomes, the DCC has been created to provide communication services to its Users to enable them to communicate with SMS. These services include: CH related services, Enrolment Services, Core Communication Services, Local Command Services, Elective Communication Services and Smart Metering Key Infrastructure (SMKI) Services.

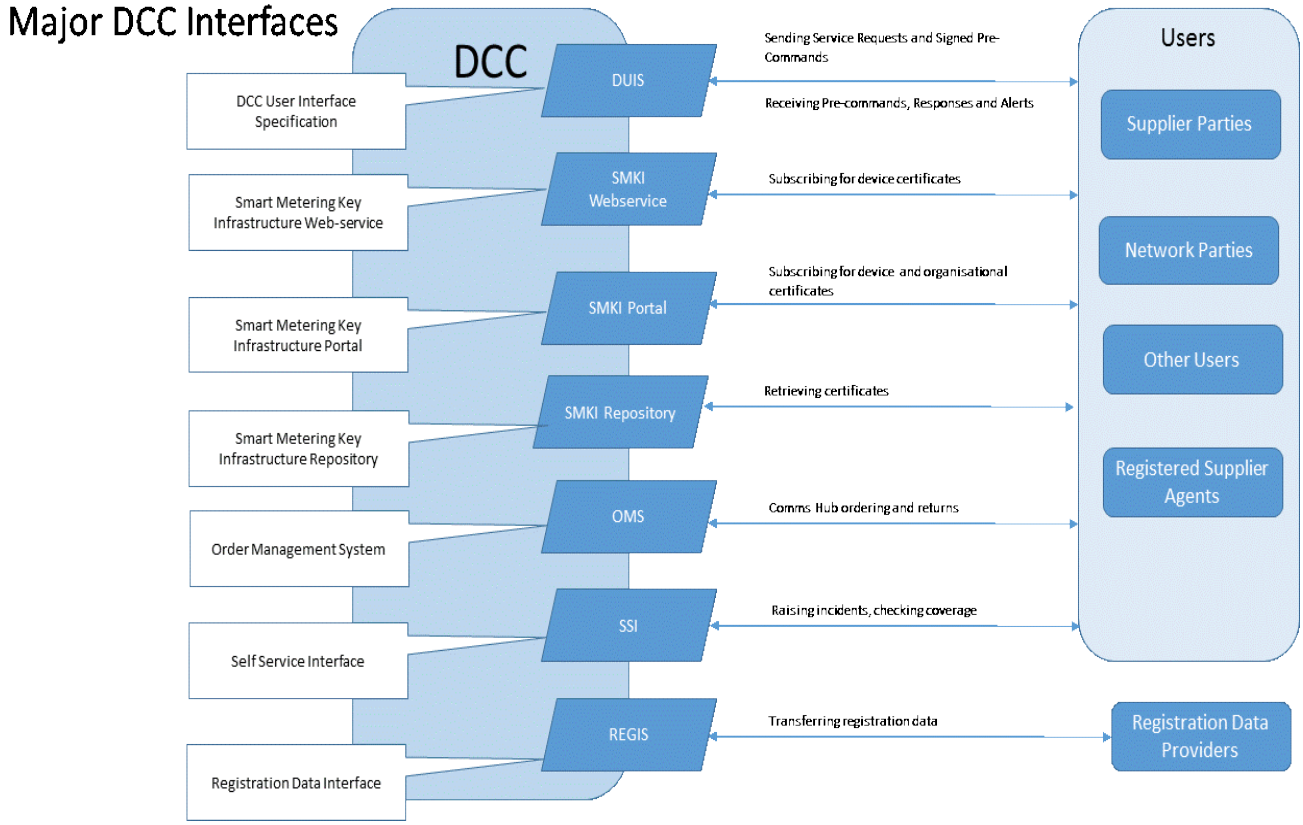
Core Communication Services are the minimum set of services that are available to Users in relation to any SMS that has been Enrolled with the DCC. They were specified by the SMIP to enable Users to operate and maintain the SMS to discharge their key business functions. Users can request Elective Communication Services from the DCC if they require additional communication services to meet their business need.

The DCC provides some of these Services via the DCC User Interface; these DCC Services are defined as DCC User Interface Services. These Services are listed in SEC Appendix E – DCC User Interface Services Schedule. To support the provision of the DCC User Interface Services, the DCC has in place certain functions such as a Service Desk and the Self-Service Interface (SSI).

4.4 Major DCC Interfaces

The DCC has established a number of interfaces to give Users access to its services.

Figure 1. Major DCC Interfaces



DCC User Interface

SEC Appendix E – DCC User Interface Services Schedule defines what Service Requests each User can request from the DCC. The construction of these Service Requests is covered in SEC Appendix AD - DCC User Interface Specification and in the DUIS XML Schema contained within it. To send (and receive the Responses from) these Service Requests, Users need to establish a gateway connection with the DCC in accordance with SEC Appendix G – DCC Gateway Connection Code of Connection and send them through the DCC User Interface.

SMKI and DCCKI Interface

To access SMKI and DCC Key Infrastructure (DCCKI) Services, which support the security of communications, Users are required to establish a gateway connection in compliance with SEC Appendix N – SMKI Code of Connection and SEC Appendix V – DCCKI Code of Connection and DCCKI Repository Code of Connection. Users can access these SMKI Services through an SMKI Interface; SEC Appendix M - SMKI Interface Design Specification provides the technical detail for the interface, including protocols and technical standards. The DCCKI Services can be accessed via the DCCKI Interface. SEC Appendix T – DCCKI Interface Design Specification describes the technical details for that interface.

SMKI and DCCKI Repository Interface

SMKI Organisational and Device Certificates are held in the SMKI Repository, and DDCKI certificates in the DCCKI Repository. To access the relevant repository, Users are required to establish a DCC Gateway Connection in compliance with SEC Appendix P – SMKI Repository Code of Connection and in compliance with SEC Appendix V – DCCKI Code of Connection and the DCCKI Repository Code of Connection. Users can access the SMKI Repository through the SMKI Repository Interface; SEC Appendix O - SMKI Repository Interface Design Specification provides the technical detail for the interface, including protocols and technical standards. The detail for the DCCKI Repository Interface is described in SEC Appendix U – DCCKI Repository Interface Design Specification.

Self-Service Interface

The DCC is required to provide a self-service portal to Users – the SSI. It allows Users, to perform a range of self-service functions including raising and monitoring the status of incidents, viewing the SMI and accessing external systems. Its technical specification is covered in SEC Appendix AH - Self-Service Interface Design Specification, while SEC Appendix AI - Self-Service Interface Code of Connection describes how to connect to it. The SSI enables Users to:

a) query the SMI – which lists all the Devices that the DCC is permitted to communicate with, and their association with each other;
b) see an audit trail of Service Requests sent;
c) raise an Incident. This is further supplemented by SEC Appendix AG – Incident Management Policy. It details the full Incident Management lifecycle including management and declaration of DCC Major Incidents, DCC Major Security Incidents, Problems and escalations;
d) order CHs via the Order Management System (OMS) (it should be noted that the OMS is also available via a public internet link); and
check DCC's planned maintenance schedule.

Registration Data Interface

The DCC uses Registration Data to check the eligibility of certain types of Users for Service Requests. The DCC receives the Registration Data from Registration Data Providers (RDPs) via the Registration Data Interface. The technical specification for this interface is described in SEC Appendix X - Registration Data Interface Specification, while how RDPs connect to the DCC is set out in SEC Appendix Y - Registration Data Interface Code of Connection.

4.5 Processes

In respect of the DCC User Interface Services set out in SEC Appendix E – DCC User Interface Services Schedule, the DCC undertakes three types of processing:

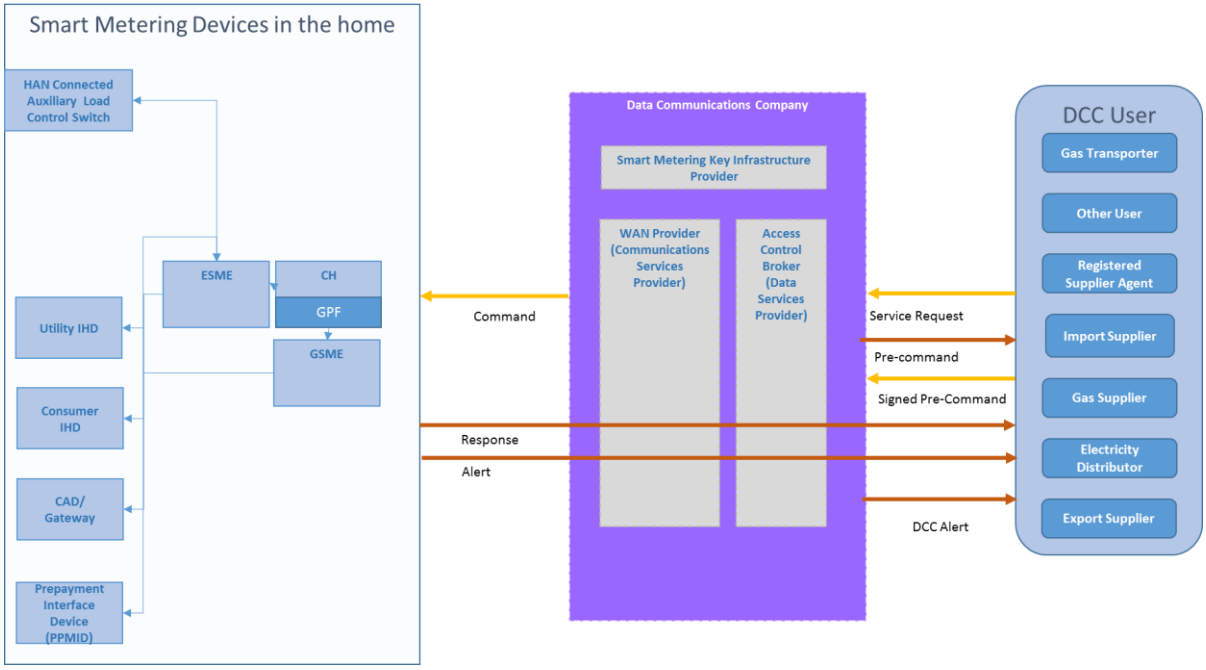
a) Critical and Non-Critical Service Request processing- if the Service Request results in a corresponding Command destined for Devices forming part of a SMS, and if that Command has a supply affecting activity if executed;

b) Non-Device Service Request processing– if the Service Request is for notifying the DCC of an activity.

The actions that the DCC must take in respect of these Service Requests are defined in SEC Appendix AB - Service Request Processing Document, SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures and SEC Sections H4 'Processing Service Requests', H5 'Smart Metering Inventory and Enrolment Services', and H6 'Decommissioning, Withdrawal and Suspension Of Devices'. Service Requests are subject to access control, and the DCC uses the Registration Data for that purpose. The eligibility for Service Requests is based on the role each User plays in achieving the programme outcomes, the role is ensuring the programme objectives are realised as well as their business need.

SEC Schedule 8 – the Great Britain Companion Specification (GBCS) describes the detailed requirements for communications between Devices and the DCC, while SEC Appendix AF - Message Mapping Catalogue sets out the mapping of content of Service Responses and Device Alerts issued in GBCS format to the DUIS XML Schema.

Figure 2. Business Process Diagram



Non-Critical Service Request Processing

The User sends a Service Request to the DCC. The DCC receives it and applies the required checks. If any of the checks fail, the DCC rejects the Service Request and informs the User. If the checks are passed, the DCC creates a corresponding Command and sends the Command to the User or the Device as specified by the Command Variant included in the Service Request. The Device receives the Command, processes and executes it, and sends a Response to the DCC. The DCC receives the Response, creates a Service Response and sends it to the User.

Critical Service Request Processing

The User sends a Service Request to the DCC. The DCC receives it and applies the required checks. If any of the checks fail, the DCC rejects the Service Request and informs the User. If the checks are passed, the DCC Transforms the Service Request into a Pre-Command, and sends the Pre-Command to the User. The User checks and Correlates the Pre-Command. Where Correlation of the Pre-Command demonstrates that it is substantively identical to the Service Request the User signs the Pre-Command, and sends the Signed Pre-Command to the DCC. The DCC receives the Signed Pre-Command, and applies further checks, including Anomaly Detection Threshold (ADT). If any of the checks (excluding the ADT) fails, the DCC rejects the Signed Pre-Command and notifies User. If the ADT fails, the DCC quarantines the Signed Pre-Command, and checks with the User (via an out of band process) whether the Signed Pre-Command is valid or not. If all the checks are passed, the DCC applies a Message Authentication Code to the Signed Pre-Command to create the Command and sends it to the User and to the Device specified in the Service Request. The Device receives the Command, processes and executes it. The Device sends a Response to the DCC. The DCC receives it, and creates a Service Response. The DCC sends the Service Response to the User.

Non-Device Service Request Processing

The User sends a Service Request to the DCC. The DCC receives it and applies the required checks. If the checks are successful, the DCC executes the activity specified in the Service Request. The DCC sends a Service Response to the User notifying it whether Service Request was successfully processed. If the checks are not successful, the DCC does not execute the activity specified in the Service Requests and sends a Service Response.

DCC Alert Processing

Alerts are unsolicited messages triggered by specific events, which means that are not generated in response to a Service Request. DCC Alerts are generated by the DCC in response to specific events, and sent to Users on the occurrence of the specified events. Specific events may also result in specific DCC behaviour, for example an SMI update by the DCC.

Device Alert Processing

Device Alerts are generated by Devices in response to specific events, and are unsolicited. They are sent to the DCC, which the DCC forwards to certain Users (Suppliers or Electricity Distributors).

4.6 Actors

DCC

The DCC has been established to provide communications between Users wishing or needing to use such communications and SMS installed in Energy Consumers' premises.

To deliver these services, the DCC has contracts in place for the following activities:

a) Provision of facilities to manage the flow of information to and from SMSs – data service provider function, which includes:

- Ordering CHs (and dealing with returned CHs);
- Maintenance of the SMI;
- Maintenance of the Registration Data;
- Provision of the SSI;
- Provision of the DCC User Interface;
- Provision of the Parse and Correlate software;
- Access Control;
- Transitional CoS;
- Provision of Service Request processing functionality including:
    - Anomaly Detection;
    - Translation;
    - Routing;
    - Signing;

- Communication management (e.g. scheduling and future dating).

b) Provision of WAN – communication service provider function, which includes:

- Provision of CH to Suppliers;
- Network management;
- Communication transport;
- Routing;
- Power outage alert management;

c) Provision of the SMKI – trusted service provider function

DCC Users

Electricity Distributor and Gas Transporter (Network Operators)

Electricity Distributors and Gas Transporters (collectively known in the BAD as Network Operators) are responsible for the gas and electricity networks that deliver energy to Energy Consumers' homes / business premises. The Network Operators also transmit, away from Energy Consumer premises, energy that is generated on those premises, for example through photovoltaic cells on roofs. Network Operators are licenced entities.

Import Supplier and Gas Supplier (Supplier)

Import Suppliers and Gas Suppliers (collectively known in the BAD as Suppliers) have the contracts with Energy Consumers for the supply of gas / electricity to their premises. An Energy Consumer may have a different Import Supplier and Gas Supplier, or they may have a single dual fuel Supplier. Import and Gas Suppliers pay the electricity generators and gas shippers for the amount of energy used by the Energy Consumers they serve. Import and Gas Suppliers are licenced entities.

Export Supplier

Where Energy Consumers have electricity generation equipment on their premises, the Electricity Smart Meter also measures how much of the generated electricity is exported from their premises. Consumers may also produce energy on their premises for export to an Export Supplier.

Registered Supplier Agent (RSA)

An Energy Consumer's Supplier is responsible for the installation and maintenance of the SMS on the Energy Consumer's premises. The Gas Supplier is responsible for the gas SMSs and the Import Supplier for the electricity SMSs. Responsibility for SMS maintenance transfers to new Supplier(s) when Consumers change Supplier(s).

Suppliers may subcontract the installation and maintenance of SMSs to specialist organisations. In the gas industry the specialists are referred to as Meter Asset Managers (MAM) and in the electricity industry, Meter Operators (MOP). The financing of Devices forming part of SMSs can be met by third party organisations known as Meter Asset Providers (MAP) who then collect rental charges from the Supplier. It should be noted that MAMs can also provide such financing for gas meters.

MAMs or MOPs may need to use some of the DCC User Interface Services to carry out their work. To do this, they must become a User in the role of Registered Supplier Agent.

Other User

Other Users are parties who may wish to engage with Energy Consumers to advise about their energy usage. Other Users have access to the DCC User Interface Services to enable them to obtain data from Smart Meters in order to provide advice to Energy Consumers. In accordance with the Data Protection Act, Other Users are required to obtain consent from the consumer before accessing their data.

Devices

There are three key documents which define the technical standards relating to smart metering equipment:

- SEC Schedule 9 - Smart Metering Equipment Technical Specifications (SMETS). SMETS covers the minimum specification for physical devices deployed in the home except the CH. There are multiple versions of the SMETS and this document reflects all changes up to Release 2.0 content, which includes the content up to SMETS2 V3.0[6].
- SEC Schedule 10 - Communications Hub Technical Specification (CHTS). CHTS covers the minimum technical specification for CHs. There are multiple versions of the CHTS and this document reflects all changes up to the Release 2.0 content, which includes CHTS v1.1
- SEC Schedule 8 - Great Britain Companion Specification (GBCS). GBCS describes the detailed requirements for communications between Devices and the DCC. There are multiple versions of GBCS and this document reflects all changes up to the Release 2.0 content, which includes GBCS v2.0. The reference term "GBCS" used in this document relates to the latest version of GBCS. where a specific version of GBCS is referenced the version number is appended to the term, i.e GBCS v1.0.

The following physical devices may form part of a SMS:

- Electricity Smart Meter;
- Gas Smart Meter;
- Communications Hub (CH);
- Prepayment Meter Interface Device (PPMID) for consumers using prepayment to ensure that they can manage supply and, as with the IHD, that the SMIP objectives are realised;
- One or more Home Area Network (HAN) Connected Auxiliary Load Control Switch (HCALCS) if supply of electricity to certain appliances needs to be managed;
- IHD to ensure that the SMIP objectives are realised;
- A consumer access device (CAD), which may be provided to assist the Energy Consumer, for example, with managing their energy use.

[6] With the exception of SMETS1 version at this time, as the delivery of SMETS1 Services by the DCC is still to be put in place and made operational. This is likely to be from Q4 2018.

As a minimum, a SMS needs to consist of: a CH, Gas or Electricity Smart Meter, and in the domestic sector an IHD or PPMID.

4.7 Regulation

The GB energy sector is regulated primarily through the Electricity Act 1989 and Gas Act 1986. These Acts prohibit a number of activities, such as the supply of electricity, except under licence. Licence holders are then required to comply with the relevant conditions contained within their licence; non-compliance with these conditions is enforceable by the Gas and Electricity Markets Authority or Ofgem. Below these licence conditions sit a number of industry codes which contain the technical and commercial obligations that govern participation in licensed activities.

Significant changes to this regulatory framework are being made to support the roll-out of Smart Meters. Powers in the Energy Act 2008 and 2011, allow the Secretary of State to make changes to legislation, licences and codes, and to introduce a new licensable activity relating to communications between Suppliers and other Parties and SMSs in Energy Consumer premises for the purposes of supporting the roll-out of Smart Meters.

To ensure that the SMIP objectives are realised and the roll-out of Smart Meters delivers the SMIP anticipated outcomes, the roll-out and operation of smart meters is underpinned by regulation.

The regulatory framework supporting the roll out and operation of Smart Meters include:

- Amendments to existing energy licences and industry codes;
- The introduction of a new licensable activity relating to communications between Suppliers and other Parties and Smart Meters in Energy Consumer premises and the appointment of the DCC to carry out this licensed activity;
- The introduction of the SEC where the rules, rights and obligations for the DCC and the Parties using the DCC are set out.

The amendments to the energy licences and codes include the mandate to roll-out of Smart Meters by energy suppliers and the requirement that domestic energy suppliers provide IHD to customers when they install SMSs. These obligations are supported by requirements relating to the operation of Smart Meters. Further obligations include the establishment of a code of practice (Smart Metering Installation Code of Practice) for the installation of Smart Meters in domestic premises, obligations in relation to consumer engagement, including the establishment of the Central Delivery Body, data access, reporting and security. Furthermore, energy suppliers are required to ensure that Smart Meters make key data available to domestic and micro-business consumers. Finally, licence obligations require energy suppliers to ensure that consumer personal data can be accessed as required by the Energy Efficiency Directive (2012/27/EU) and to support CoS.

The establishment of the DCC is covered by two statutory instruments:

- The Electricity and Gas (Smart Meters Licensable Activity) Order 2012 (SI 2012/2400) - this Order introduced a new licensable activity which relates to the provision of a service of communicating with Smart Meters on behalf of all licensed energy suppliers.

- The Electricity and Gas (Competitive Tenders for Smart Meter Communication Licences) Regulations 2012 (SI 2012/2414) (DCC Licence Application Regulations) - these set out the

competitive application process to award licences for the provision of a service of communicating with Smart Meters on behalf of all licensed energy suppliers. The process under the regulations allows for a single person to be granted licences for this activity in respect of both Electricity and Gas Smart Meters after competition and to become a monopoly provider of communication services in GB.

The SEC is a multiparty contract which sets out the terms for the provision of the DCC Services, and specifies other provisions to govern the end-to-end management of smart metering. The SEC was created to support the matters dealing with the operations of the DCC in the provision of the DCC Services to DCC Users, which are described in the above sections in more detail. Organisations involved in the roll out of smart metering are required by their licences to accede to the SEC. Non-licenced parties who wish to help deliver the SMIP outcomes need to accede to the SEC to be granted access to the DCC Services.

The SEC also contains the SMETS, CHTS, GBCS, and obligations requiring suppliers to roll out equipment compliant with these specifications. Suppliers can check whether a Device is compliant by checking the Certified Products List (CPL). SEC Appendix Z - CPL Requirements Document describes procedures for adding and removing Devices from the CPL. SEC Section F4 describes Suppliers' operational obligations relating to the roll-out of Smart Meters. Since Suppliers procure CHs from the DCC, SEC Sections F5[7], F6[8], F7[9], F8[10], F9[11] and F10[12] describe how to order CHs from the DCC, raise an Incident and return CHs to the DCC. These sections are supplemented further by SEC Appendix H – Communications Hubs Handover Support Materials and SEC Appendix I – Communications Hubs Installation and Maintenance Support Materials which provide further processes and details to facilitate the delivery, installation, maintenance and return of CHs.

The responsibility for the security of the End-to-End Smart Metering System is shared between the DCC and Users. SEC Section G describes the respective system, personnel and information security obligations. One of the systems security controls that the DCC and Users are required to have in place by virtue of SEC Section G is Threshold Anomaly Detection (TAD). SEC Appendix AA – Threshold Anomaly Detection Procedures describes the process by which the DCC and Users communicate regarding any matters relating to the TAD.

The authenticity and where required, confidentiality of communications is provided by the SMKI and DCCKI. SEC Section L describes what the DCC is required to provide (as SMKI Service Provider and SMKI Repository Service Provider) and what the DCC and Users are required to establish and put in place to support this infrastructure. To obtain relevant certificates for their organisation and Devices, the DCC and Users are required to become Subscribers. SEC Appendix D - Smart Metering Key Infrastructure Registration Authority Policies and Procedures (RAPP) and SEC Appendix W – DCCKI Registration Authority Policies and Procedures (RAPP) describe how to become a Subscriber for relevant certificates. Subscribers are required to maintain their certificates in accordance with

[7] Communications Hub Forecasts & Orders
[8] Delivery and Acceptance of Communications Hubs
[9] Installation and Maintenance of Communications Hubs
[10] Removal and Return of Communications Hubs
[11] Categories of Communications Hub Responsibility
[12] Test Communications Hubs

SEC Appendix A – Device Certificate Policy, SEC Appendix B – Organisation Certificate Policy and SEC Appendix S – DCCKI Certificate Policy. Subscribers are also subject to an assurance scheme; the detail of which is described in SEC Appendix C – SMKI Compliance Policy.

There may be instances where a Relevant Private Key Material is Compromised. SEC Appendix L - SMKI Recovery Procedure sets out the notification and resolution process that the DCC and Users need to follow in relation to any such incident.

4.8 Governance

Under the SEC, the Panel, has been established to ensure effective and efficient operation of the SEC. The SEC (Section C 'Governance') sets out the composition of the Panel, voting arrangements and the Panel's role and responsibilities. The Panel has the right to establish a number of sub-committees to help it discharge it duties.

The SEC Code Administrator and Secretariat (SECAS) plays an important role in SEC governance, undertaking day-to-day governance activities under the direction of the Panel, which include:

- Configuration control of the SEC and supporting documentation;
- Management of the Modification process;
- Accession of Parties to the SEC;
- The provision of advice and support to prospective Parties;
- Suspension, expulsion and withdrawal procedures for Parties;
- Dispute resolution between Parties;
- Reporting;
- Performing administrative duties on behalf of the Panel.

5 Tooling and Relationship to Business Architecture Model

The BAD describes the processes that the DCC and Users are required to follow to support certain business outcomes for Users. The Business Architecture Model (BAM) sits alongside the BAD. It describes in diagrammatic terms, the business processes at high level and like the BAD, relies on the obligations set out in the SEC. The BAM has been developed using the Erwin Enterprise Architecture (formerly CaseWise^{tm}) suite of modelling tools and can be accessed via an Evolve portal (hosted by SECAS). The notation used in the BAM is Business Process Model and Notation version 2.

The BAM is supported by a user guide that explains the notation in more detail as well as to provide an overview on how the BAM can be navigated.

The BAM is intended to provide a high-level view of the processes supporting User access to the DCC Services and all the actors involved in these processes. It focuses on the key interactions between the DCC, Users and Devices. The BAM also includes any relevant SEC obligations that apply to a particular process and particular actor involved in the process. As the BAD, it takes the device lifecycle approach to showing all the processes and interactions between them.

The BAM is deliberately dynamic, enabling readers to drill into more detailed information as they move down levels. At the lowest level, the BAM explains in detail how the DCC processes Service Requests. The BAM highlights the links and dependencies between processes helping readers to follow the process as well as any associated interactions from start to finish.

The BAM allows processes to be filtered by actor.

The model is intended to follow the same structure as the BAD and use the same notation to ensure ease of navigation between the two documents.

6 Change Management

The SEC obligations on which the Business Architecture (so the BAD and BAM) relies upon are subject to change. Changes to the SEC may impact on the business processes, which means that the BAD and the BAM may be subject to change.

Changes to the SEC are driven either by the Secretary of State or by industry by raising Modification Proposals.

Both processes for amending the SEC are very similar, and they will be managed in a similar way. Table 1 below describes the key stages of the change cycle and the status of that change at each stage. The BAD and BAM will be amended at these key stages of the change cycle.

Table 1. Key stages in the change cycle

#	Secretary of State led changes	Modification Proposals	Status of change
1	Secretary of State led change in consultation	Modification Proposal in Refinement	Draft
2	Secretary of State led change has concluded	Modification Proposal is approved[13]	Final
3	Secretary of State led change has been designated	Modification Proposal is released	Effective

Two aspects of the BAD and BAM will be maintained in light of changes to the SEC:

- Processes – process descriptions in the BAD and processes in the BAM
- Regulations – regulations in the BAD and regulations in the BAM

A full Modifications Register can be found at:

https://smartenergycodecompany.co.uk/modifications/

[13] If a Modification Proposal, that impacts the BAD and/or BAM, is rejected and therefore not implemented any associated changes to the BAM and/or BAM will not be applied.

The Modifications Register contains details on all Modification Proposals, including associated Modification Reports. The Modification reports for each modification will set out which areas of the BAD and BAM are impacted (if any).

This document incorporates the Secretary of State led changes to the SEC for Release 2.0 (which includes Dual Band CH). The future Release covering SMETS1 enrolment and adoption will have a further impact on the Business Architecture. The TABASC anticipate that both the BAD and the BAM will require material amendment to incorporate these changes. Apart from the aforementioned changes, we expect that the government may amend the SEC further under transitional powers and that some of these changes will have an impact on the Business Architecture.

The BAD and BAM will be maintained as part of the on-going release management cycles, with the necessary changes prepared and drafted in advance of the effective date of the relevant changes. On the effective date of the changes the updated BAD and BAM would then be published and issued.

The BAD will be kept up to date in line with the current version of the SEC. In between releases, minor changes to the SEC may be applied that do not impact the content of the BAD, however in these cases the version of the SEC referenced will be updated to be clear which version the BAD has been produced against.

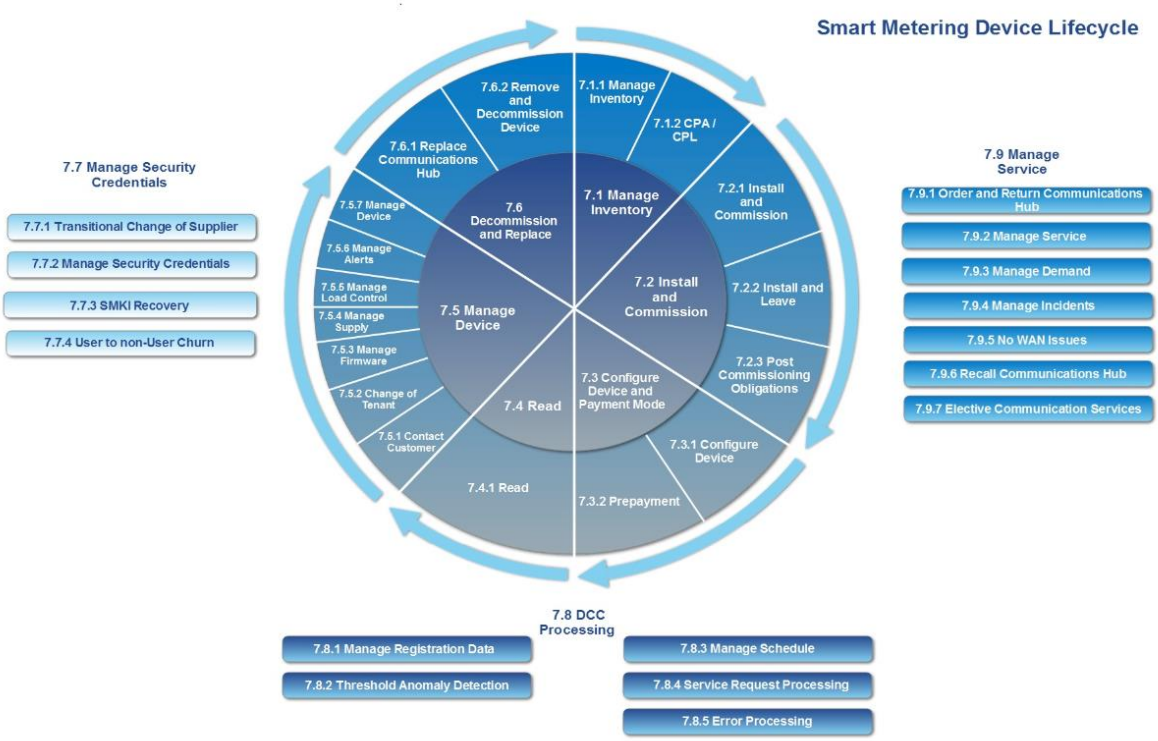
The current version of the SEC that the BAD has been based on is SEC version **[5.19, designated on 25th June 2018]**

7 Functional and Process Areas

The functional and process areas that are described in this section are arranged around the lifecycle of Devices when they are operated by the DCC. The Devices have a lifecycle that starts with their addition to the SMI through to their Commissioning, and ends when they are Decommissioned. It should be noted that some activities can occur more than once during the life of a Device, for example Manage Credentials as they can be updated on a device multiple times.

This lifecycle is illustrated as follows:

Figure 3. Smart Metering Device Lifecycle



7.1 Manage Inventory

The SMI is a central list of Devices that the DCC is permitted to communicate with. This means that it forms part of many business processes, not just for the DCC but also for Users. The DCC is responsible for maintaining the SMI, though Suppliers have a responsibility to ensure the records of Devices for which they are the Responsible Supplier are kept up to date, reflecting any changes made, and correcting any identified errors. The DCC maintains the SMI through monitoring Device status through their inventory lifecycle. The DCC also ensures that relevant Users are aware of those status changes through DCC Alerts. This section covers two process areas:

- Manage Inventory - the processes for adding Devices to the SMI, and maintaining Device related data in the SMI through its lifecycle.
- Commercial Product Assurance (CPA) / Certified Product List (CPL)– the process for ensuring that the DCC only communicates with those Devices which meet the assurance requirements.

7.1.1 Manage Inventory

7.1.1.1 Introduction

This process area describes the processes for adding to and removing Devices from the SMI, and keeping the information held in the SMI up-to-date.

The SMI plays a critical role in the operation of Smart Metering. It lists all the Devices which the DCC is permitted to communicate with and shows the Association between these Devices. This means

that the SMI forms part of many end to end business processes not just for the DCC but also for Users.

The DCC and Users are jointly responsible for making sure that the SMI is up-to-date. The DCC maintains the SMI by adding Communications Hub Function (CHF) and Gas Proxy Function (GPF) to it, monitoring and updating the SMI Status of Devices (other than Type 2 Devices) throughout their lifecycle. The DCC also ensures that certain Users are aware of those SMI Status changes through various DCC Alerts. Users, on the other hand, are responsible for adding Devices other than the CHF and GPF to the SMI. Once Devices are added to the SMI, Suppliers are then responsible for making sure that the Device SMI records are up-to-date.

Device SMI Status is critical because it directly affects the extent to which the DCC is permitted to communicate with such Devices. Device SMI Statuses (other than for Type 2 Devices, which do not have a Device status in the SMI) are:

- Pending
- Whitelisted
- Installed not Commissioned
- Commissioned
- Decommissioned
- Withdrawn
- Suspended
- Recovery
- Recovered

7.1.1.2 Scope

This process area includes:

- Device Pre-notification
- Update Inventory

This process area involves but does not specifically describe Read (Non-Device) - Read Inventory. This is described in Section 7.4.1.6.3 of the BAD.

This process area excludes DCC internal process for managing the SMI.

7.1.1.3 Inputs

- ‘Update Inventory’ Service Request (SRV 8.4)
- ‘Device Pre-Notification’ Service Request (SRV 12.2)

7.1.1.4 Actors

- User
- DCC
- CH
- Smart Meter
- Type 1 Device
- Type 2 Device

7.1.1.5 Prerequisites

The Device (except Type 2 Devices) is on the CPL and has a status of 'current'.

The Party has received the required assurance certificates for Type 2 Devices.

7.1.1.6 Process Description

This section describes how a Device (other than Type 2 Device) SMI Status changes throughout its lifecycle. It signposts to the specific processes described in this document that trigger the SMI Status change. For completeness, the specific triggers for the DCC to change a Device SMI status are captured, however more detail on the triggers and associated processes can be found in the relevant process area.

7.1.1.6.1 Device SMI Status change during its lifecycle

Table 2. Device SMI Status change during its lifecycle

Status	Process Area	Process	Trigger	Device Type
Pending	1. 7.1.1 Manage Inventory	1. 7.1.1.6.2 Device Pre-notification	1a. Successful processing by the DCC of a 'Device Pre-Notification' Service Request 1b. The DCC adding CHF and GPF to the SMI	1a. Smart Meter, Type 1 Device 1b. CHF, GPF
Whitelisted	1. 7.2.1 Install and Commission	1. 7.2.1.6.7 Update HAN Device Log – Add Device	1. Receipt by the DCC of a CCS01 Response arising from an 'Update HAN Device Log' Service Request indicating that a Device has been added to the CHF Device Log	1. Smart Meter, Type 1 Device

Installed not Commissioned	1. 7.2.1 Install and Commission 2. 7.2.2 Install and Leave	1. 7.2.1.6.7 Update HAN Device Log – Add Device 2. 7.2.2.6.5 Update Inventory – Update Device SMI Status to 'Installed no Commissioned'	1. Receipt, within the timeout period, by the DCC of a second CS14 Device Alert from the CHF, following CBKE. 2. Successful processing by the DCC of an 'Update Inventory' Service Request	1. Smart Meter, Type 1 Device 2. Smart Meter, Type 1 Device, CHF, GPF
Commissioned	1. 7.2.1 Install and Commission 2. Install and Leave	1a. 7.2.1.6.10 Commission Device 1b. 7.2.1.6.12 Join Service 1c. 7.2.1.6.4 Install Communications Hub 2. 7.2.2.6.8 Update Inventory – Update GPF SMI Status to 'Commissioned'	1a. Receipt by the DCC of a GCS28 for Gas Smart Meter or ECS70 Response for the Electricity Smart Meter arising from a 'Commission Device' Service Request indicating that the Meter has synchronised its time with the CHF time1b. Receipt by the DCC Responses from Meters and GPF arising from 'Join Device' Service Requests indicating that the Device and the Meter / GPF have completed CBKE 1c. Receipt and successful validation by the DCC of a communication from the CHF 2. Successful processing by the DCC of an 'Update Inventory' Service Request	1a. Smart Meter 1b. Type 1 Device, GPF 1c. CHF 2. GPF

Suspended	1. 7.1.1 Manage Inventory	1. 7.1.2.4.3 Suspend Device	1. Receipt by the DCC a CPL file indicating that a Device Model has been removed from the CPL	1. Smart Meter, Type 1 Device, CH
Withdrawn	Proposed to be removed subject to BEIS consultation outcome			
Recovery	1. 7.7.3 SMKI Recovery	1a. 7.7.3.4.3 Recovery of Private Keys associated with Organisation Certificates by the DCC installing ACB Certificates 1b. 7.7.3.4.4 Recovery of Private Keys associated with Organisation Certificates by the DCC installing Organisation Certificates 1c. 7.7.3.4.5 Recovery using Contingency Private Key	1. The DCC becomes aware of Device Compromise	1. Smart Meter, HCALCS, GPF, CHF
Recovered	1. 7.7.3 SMKI Recovery	1a. 7.7.3.4.3 Recovery of Private Keys associated with Organisation Certificates by the DCC installing ACB Certificates 1b. 7.7.3.4.5 Recovery using Contingency Private Key	1. Successful replacement of the affected Organisation Certificates by the DCC	1. Smart Meter, HCLACS, GPF, CHF
Decommissioned	1. 7.6.2 Remove and Decommission Device	1. 7.6.2.5.5 Decommission Device	1. Successful processing by the DCC of a 'Decommission Device' Service Request	1. Smart Meter, Type 1 Device, CH

7.1.1.6.2 Device Pre-notification

The DCC is responsible for adding the CHF and GPF to the SMI. Before delivering a CH to the Supplier, the DCC checks the CH's Device Model is on the CPL, and if it is, the DCC adds the CHF and GPF to the SMI with an SMI Status of 'Pending' and Associates the CHF and GPF. (This is an internal-to-DCC process.)

Users are responsible for adding Devices other than the CHF and GPF to the SMI. Users add such Devices to the SMI by composing and sending a 'Device Pre-Notification' Service Request (SRV 12.2) to the DCC.

The DCC receives the Service Request from the User and:

- For all Devices, undertakes Non-Device Service Request processing; and
- For Smart Meters and Type 1 Devices the DCC checks that the Device is on the CPL.

The DCC then:

- Sends a Service Response to the User (indicating success or failure); and
- For Smart Meters and Type 1 Devices, if both the checks are successful, the DCC adds the Device to the SMI with a SMI Status of 'Pending'; or
- For Type 2 Devices, if the Non-Device Service Request processing is successful, the DCC adds the Device to the SMI with no SMI Status.

Where the SMI Status of a Device (Smart Meter or Type 1 Device) has remained 'Pending' for 12 months, then the DCC removes the Device from the SMI. When the DCC removes the Device from the SMI, the DCC sends a 'Device removed from Inventory - Pending Status expired' (N8) DCC Alert to the User that sent the corresponding 'Device Pre-Notification' Service Request to add that Device to the SMI.

7.1.1.6.3 Update Inventory

SMI updates are primarily triggered by the various Service Requests and / or DCC processing steps as set out in Table 2. However, in some circumstances it may be necessary for Suppliers to change SMI records directly, using an 'Update Inventory' Service Request (SRV 8.4).

The use of the 'Update Inventory' Service Request is heavily constrained. If the Device has a status of 'Pending' only the User who added the Device to the SMI can update Device details by sending the 'Update Inventory' Service Request. If the Device has an SMI Status of other than 'Pending', only the Supplier responsible for that Device can update its details using the 'Update Inventory' Service Request.

To update Device details, a User composes the 'Update Inventory' Service Request and sends it to the DCC. The DCC completes Non-Device Service Request processing and sends a Service Response to the User indicating success or failure. If the Non-Device Service Request processing is successful, the DCC updates or deletes the SMI record as requested and, where required, sends relevant DCC Alerts to relevant Users.

For example, if the Supplier updates the Meter Point Number (MPxN) value using the 'Update Inventory' Service Request, following the successful execution of the Service Request, the DCC sends a 'Device Identity Confirmation' DCC Alert (N16) to the Network Operator.

7.1.1.6.4 Read (Non-Device) - Read Inventory

There are two ways a User can read the Data held in the SMI. One way to interrogate the SMI is to send a 'Read Inventory' Service Request to the DCC or the other is to search it via the SSI. These processes are described in more detail in Section 7.4.1.6.3 of the BAD.

7.1.1.7 Commentary

Please note that BEIS is consulting on whether to remove DCC opt out, therefore a 'withdrawn' status is not covered in this document.

7.1.1.8 Associated Process Areas

#	Process Areas
7.2.1	Install and Commission
7.2.2	Install and Leave
7.4.1	Read
7.6.1	Replace Communications Hub
7.6.2	Remove and Decommission
7.7.3	SMKI Recovery

7.1.1.9 Governance

Actor	SEC Document	Clause	Text
7.1.1.6.2 Device Pre-notification			
DCC	Smart Energy Code	Section H5.5	The DCC shall establish and maintain the Smart Metering Inventory in accordance with the Inventory, Enrolment and Withdrawal Procedures. https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.1	The DCC shall establish and maintain the Smart Metering Inventory. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.2	The DCC shall ensure that the Smart Metering Inventory reflects the most up-to-date information provided (or made available) to it from time to time in accordance with this Code (subject to Section F2.9 (Publication and Use by the DCC)). https://smartenergycodecompany.co.uk/download/2275
DCC, User	SEC Appendix AC - Inventory Enrolment and	2.3	Parties shall not seek to add Devices to the Smart Metering Inventory (and the DCC shall not add Devices to the Smart Metering Inventory) otherwise than in compliance with this Appendix.

	Withdrawal Procedures		https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.4	Prior to delivering a Communication Hub to a Party pursuant to the Communications Hub Service, the DCC shall add the Communications Hub Function and Gas Proxy Function that comprise that Communications Hub to the Smart Metering Inventory (to be identified with an SMI Status of 'pending'); provided that such Devices may only be added to the Smart Metering Inventory where the Communications Hub is of a Device Model identified in the Certified Products List. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.5	No Party shall add Communications Hub Functions to the Smart Metering Inventory without also adding the Gas Proxy Function that forms part of the same Communications Hub (and vice versa). https://smartenergycodecompany.co.uk/download/2275
User	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.6	Any User may send a Service Request requesting that the DCC adds a Device to the Smart Metering Inventory (to be identified with an SMI Status of 'pending'); provided that only Devices of a Device Model that is identified in the Certified Products List are eligible to be added to the Smart Metering Inventory. This Clause 2.6 does not apply to Type 2 Devices (which are covered in Clause 2.9). https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.7	The DCC shall not send any communication to a Device unless the Device is listed in the Smart Metering Inventory; save for communications sent for the purposes of testing under Section H14 (Testing Services) or Section T (Testing During Transition). https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.8	In the case of Communications Hub Functions and Gas Proxy Functions, only those that comprise a Communications Hub that is to be provided by the DCC pursuant to the Communications Hub Service may be added to the Smart Metering Inventory (subject to Clause 10.3) https://smartenergycodecompany.co.uk/download/2275

DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.9	Any User may send a Service Request requesting that the DCC adds a Type 2 Device to the Smart Metering Inventory. For the avoidance of doubt, a Type 2 Device shall not be identified in the Certified Products List and shall have no SMI Status. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	7.2	Where the SMI Status of a Device has remained as 'pending' for 12 months, then the DCC shall remove the Device from the Smart Metering Inventory. https://smartenergycodecompany.co.uk/download/2275
User	SEC Appendix AD - DCC User Interface Specification	3.8.113.1	A User must ensure that all Devices that are required to be displayed via the Smart Metering Inventory and/or required to be connected into the Home Area Network (HAN) must have an associated Device Pre-notification Service Request sent to the DCC. https://smartenergycodecompany.co.uk/download/2279
DCC	SEC Appendix AD - DCC User Interface Specification	3.8.113.1	The DCC shall ensure that the Communication Hub Function and Gas Proxy Function Devices are pre-notified and associated details are updated into the Smart Metering Inventory on behalf of Users. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification	3.8.113.2	Upon successful execution of a DevicePrenotification Service Request, the DCC shall update the Smart Metering Inventory and set the SMI Status of the DeviceId to ‘Pending’ where the Device Type is one that has an SMI Status recorded within the Smart Metering Inventory. https://smartenergycodecompany.co.uk/download/2279
7.1.1.6.3 Update Inventory			
User	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.10	The Responsible Supplier for each Smart Metering System shall keep under review the information recorded in the Smart Metering Inventory in respect of the Devices that comprise that Smart Metering System. Where circumstances change or the Responsible Supplier identifies an error in such information, the Responsible Supplier shall submit Service Requests requesting that the DCC updates the Smart Metering Inventory (or, where it is not possible to do so, shall raise an Incident in accordance with the Incident Management Policy). Where a correction is made in respect of the relationship between one or more Smart Meters and an MPAN and/or MPRN, then the DCC shall notify

			the Electricity Distributor and/or Gas Transporter for the affected MPANs and/or MPRNs. https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	7.1	Where the Responsible Supplier wishes to change the SMI Status of any Device (other than a Type 2 Device) from 'decommissioned', 'whitelisted' or 'withdrawn' to 'pending', then the Responsible Supplier shall send the DCC a Service Request to that effect. Provided the Device in question is of a Device Model that is identified in the Certified Products List, the DCC shall change the SMI Status to 'pending'. https://smartenergycodecompany.co.uk/download/2275
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4	When a User sends an Update Inventory Service Request to the DCC in respect of a Communications Hub, the DeviceId specified within the Service Request shall be that of the Communications Hub Function and not the Gas Proxy Function. Note that where a Device has an SMI Status of 'Recovered' the Device's SMI Status immediately prior to it having the SMI Status of 'Recovery' shall be used in validation. This Service Request can be used by Users to perform the following four functions; https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4	When a User sends an Update Inventory Service Request to the DCC in respect of a Communications Hub, the DeviceId specified within the Service Request shall be that of the Communications Hub Function and not the Gas Proxy Function. Note that where a Device has an SMI Status of 'Recovered' the Device's SMI Status immediately prior to it having the SMI Status of 'Recovery' shall be used in validation. This Service Request can be used by Users to perform the following four functions; https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1	Update Device details within the Smart Metering Inventory provided via Pre-Notification; https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC	3.8.101.4.1	Update Device details within the Smart Metering Inventory provided via Pre-Notification

	User Interface Specification v2.0		https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1a	This functionality of the Service Request is available to all the Eligible User Roles associated with this Service Request. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1a	This functionality of the Service Request is available to all the Eligible User Roles associated with this Service Request. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1b	Only the User who originally added the Device to the Smart Metering Inventory may update these device details whilst the Device has a status of 'Pending'. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1b	Only the User who originally added the Device to the Smart Metering Inventory may update these device details whilst the Device has a status of 'Pending'. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1c	For Devices that have SMI Status values, only Devices in a status of 'Pending' can be updated. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1c	For Devices that have SMI Status values, only Devices in a status of 'Pending' can be updated. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface	3.8.93.4.1d	Type 2 (IHD and CAD) Devices can be updated at any time. https://smartenergycodecompany.co.uk/download/2279

	Specification v1.1		
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1d	Type 2 (IHD and CAD) Devices can be updated at any time. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1e	Update most of the Device details that were initially provided to the DCC via Service Request 12.2 – Device Pre-notification (see clause 3.8.113) https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1e	Update most of the Device details that were initially provided to the DCC via Service Request 12.2 – Device Pre-notification (see clause 3.8.1.22) https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1f	It isn't possible to update a Device ID (including the GPF Device ID associated to a CHF). If it has been entered in error it has to be deleted via this Service Request and re-added via Service Request 12.2 – Device Pre-notification (see clause 3.8.113). https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1f	It isn't possible to update a Device ID (including the GPF Device ID associated to a CHF). If it has been entered in error it has to be deleted via this Service Request and re-added via Service Request 12.2 – Device Pre-notification (see clause 3.8.122). https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1g	It isn't possible to update a Device Type. If it has been entered in error it has to be deleted via this Service Request and re-added via Service Request 12.2 – Device Pre-notification (see clause 3.8.113) https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface	3.8.101.4.1g	It isn't possible to update a Device Type. If it has been entered in error it has to be deleted via this Service Request and re-added via Service Request 12.2 – Device Pre-notification (see clause 3.8.122).

	Specification v2.0		https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.1h	Any updates to the details shared between a CHF and a GPF will be applied to both. The Device ID in the Service Request has to be that of the CHF. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.1h	h. Any updates to the details shared between a CHF and a GPF will be applied to both. The Device ID in the Service Request has to be that of the CHF. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.2	Delete Device details from the Smart Metering Inventory provided via Pre-Notification which have not been installed. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.2	Delete Device details from the Smart Metering Inventory provided via Pre-Notification which have not been installed. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.2a	This functionality of the Service Request is available to all the Eligible User Roles associated with this Service Request. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.2a	This functionality of the Service Request is available to all the Eligible User Roles associated with this Service Request. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User	3.8.93.4.2b	Only the User who originally added the Device to the Smart Metering Inventory may delete these device details. https://smartenergycodecompany.co.uk/download/2279

	Interface Specification		
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.2b	Only the User who originally added the Device to the Smart Metering Inventory may delete these device details. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.2c	For Devices that have SMI Status values, only Devices in a status of 'Pending' can be deleted. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.2c	For Devices that have SMI Status values, only Devices in a status of 'Pending' can be deleted. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.2d	Type 2 (IHD and CAD) Devices can be deleted at any time. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.2d	Type 2 (IHD and CAD) Devices can be deleted at any time. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.2e	Deleting a CHF will also delete its associated GPF. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface	3.8.101.4.2e	e. Deleting a CHF will also delete its associated GPF. https://smartenergycodecompany.co.uk/download/4639

	Specification v2.0		
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3	Update SMI Status within the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3	Update SMI Status within the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3a	This functionality of the Service Request is ONLY available to the Eligible User Roles of Import Supplier and Gas Supplier who are the Responsible Supplier to the Device being updated. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3a	This functionality of the Service Request is ONLY available to the Eligible User Roles of Import Supplier and Gas Supplier who are the Responsible Supplier to the Device being updated. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3b	Different options exist for which device SMI Status values can be updated by DCC Service Users depending on Device type. Functionality allows, https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3b	Different options exist for which device SMI Status values can be updated by DCC Service Users depending on Device type. Functionality allows, https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface	3.8.93.4.3bi	Update the Device status for all Device Types, other than the CHF and the GPF and where the old and new status apply to the Device Type https://smartenergycodecompany.co.uk/download/2279

	Specification v1.1		
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3bi	Update the Device status for all Device Types, other than the CHF and the GPF and where the old and new status apply to the Device Type https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3bi.1	From 'Pending' to 'Installed Not Commissioned' https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3bi.1	From 'Pending' to 'Installed Not Commissioned' https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3bi.2	From 'Whitelisted' to 'Pending' https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3bi.2	From 'Whitelisted' to 'Pending' https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3c	Update the Device SMI Status for a CHF (and its associated GPF) https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface	3.8.101.4.3c	Update the Device SMI Status for a CHF (and its associated GPF) https://smartenergycodecompany.co.uk/download/4639

	Specification v2.0		
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3ci	To support the Install & Leave process and / or Install & Commission after Decommissioning or Withdrawal: https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3ci	To support the Install & Leave process and / or Install & Commission after Decommissioning or Withdrawal: https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3ci.1	From 'Pending' to 'Installed Not Commissioned' (GPF from 'Pending' to 'Installed Not Commissioned') https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3ci.1	From 'Pending' to 'Installed Not Commissioned' (GPF from 'Pending' to 'Installed Not Commissioned') https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3.ci.2	From 'Installed Not Commissioned' to 'Commissioned' (GPF no status transition) https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3.ci.2	From 'Installed Not Commissioned' to 'Commissioned' (GPF no status transition) https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3ci.3	From 'Pending' to 'Commissioned' (GPF from 'Pending' to 'Installed Not Commissioned') https://smartenergycodecompany.co.uk/download/2279

	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.93.4.3ci.3	From 'Pending' to 'Commissioned' (GPF from 'Pending' to 'Installed Not Commissioned') https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3cii	From 'Commissioned' to 'Withdrawn'. This is the equivalent of Service Request 8.5 – Service Opt Out (see clause 3.8.94) for other Device Types. On successful completion of the Service Request, the DCC Systems will: https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3cii	From 'Commissioned' to 'Withdrawn'. This is the equivalent of Service Request 8.5 – Service Opt Out (see clause 3.8.102) for other Device Types. On successful completion of the Service Request, the DCC Systems will: https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3cii.1	automatically delete all active DSP Schedules on all Devices in the CHF Whitelist. For each deleted DSP Schedule a DCC Alert N37 will be sent to the DCC Service User that owned it. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3cii.1	automatically delete all active DSP Schedules on all Devices in the CHF Whitelist. For each deleted DSP Schedule a DCC Alert N37 will be sent to the DCC Service User that owned it. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.3cii.2	automatically cancel all Future Dated (DSP) requests not yet sent to the Device for that CHF and all the Devices in its Whitelist. For each cancelled request a DCC Alert N36 will be sent to the sender of the Future Dated request. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.3cii.2	automatically cancel all Future Dated (DSP) requests not yet sent to the Device for that CHF and all the Devices in its Whitelist. For each cancelled request a DCC Alert N36 will be sent to the sender of the Future Dated request. https://smartenergycodecompany.co.uk/download/4639

DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.4	Update MPxN associated with the Device (or add a new association) within the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.4	Update MPxN associated with the Device (or add a new association) within the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.4a	This functionality of the Service Request is ONLY available to the Eligible User Roles of Import Supplier and Gas Supplier who are the Responsible Supplier for both the existing MPxN association and the requested MPxN association update. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.4a	This functionality of the Service Request is ONLY available to the Eligible User Roles of Import Supplier and Gas Supplier who are the Responsible Supplier for both the existing MPxN association and the requested MPxN association update. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.4b	The Responsible Supplier can only update the MPxN value to another which they are also the Responsible Supplier for. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.4b	The Responsible Supplier can only update the MPxN value to another which they are also the Responsible Supplier for. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.4c	The new MPxN must be consistent with the type of Device, for example if the Secondary MPAN is updated then the device must be a twin element ESME. https://smartenergycodecompany.co.uk/download/2279

	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.4c	The new MPxN must be consistent with the type of Device, for example if the Secondary MPAN is updated then the device must be a twin element ESME. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.4.4d	ONLY a single MPxN association change be changed per Service Request call https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.4d	ONLY a single MPxN association change be changed per Service Request call https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification	3.8.93.4.4e	If the MPxN is successfully updated in the Smart Metering Inventory, then a DCC Alert N16 is sent to the Meter's Registered Network Operator. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.4.4e	If the MPxN is successfully updated in the Smart Metering Inventory, then a DCC Alert N16 is sent to the Meter's Registered Network Operator. https://smartenergycodecompany.co.uk/download/4639

7.1.2 CPA / CPL

7.1.2.1 Introduction

This process area describes the processes for adding and removing Device Models from the CPL, how the DCC sets the SMI Status of a Device (other than a Type 2 Device) to 'Suspended', and the consequences of this status change for Users.

The CPL contains the Device Models for which the Panel has received all the Assurance Certificates required for the Device Type relevant to that Device Model. The Panel has the responsibility for maintaining the CPL.

Different Devices Types require different levels of certification, as described in the CHTS and SMETS:

Table 3. Device Certification

Device Type	ZigBee	DLMS	CPA
CH	Yes		Yes
Electricity Smart Meter	Yes	Yes	Yes
Gas Smart Meter	Yes		Yes
PPMID	Yes		
HCALCS	Yes		Yes
IHD	Yes		

The following Assurance Certification Bodies issue the following Assurance Certificates:

- ZigBee Certification provided by the ZigBee Alliance;
- Device Language Message Specification (DLMS) Certification provided by the DLMS User Association; and
- Commercial Product Assurance Certification provided by the National Cyber Security Centre (NCSC).

The SMI lists all the Devices with which the DCC is permitted to communicate with. The DCC is not permitted to add a new Device to the SMI unless that Device has the status of 'current' on the CPL.

If a Device is already on the SMI and that Device's Device Model is subsequently removed from the CPL, the DCC is required to set the SMI Status of that Device to 'suspended'. This means that the DCC is not permitted to communicate with that Device unless to take it out from 'suspension'.

7.1.2.2 Scope

This process area includes:

- CPL Submission
- Certificate expiry
- Suspend Device

This process area excludes:

- The Assurance or Certification processes undertaken by Assurance Certification Bodies
- Processes to take the Device out of suspension

7.1.2.3 Actors

- Supplier
- Network Operator
- Manufacturer
- DCC

- Panel
- CH
- Smart Meter
- Type 1 Device
- IHD

7.1.2.4 Process Description

7.1.2.4.1 CPL Submission

To add a Device Model (excluding Device Models for Type 2 Devices) to the CPL, SEC Appendix Z - CPL Requirements Document requires that the following information is supplied to the Panel:

- Each of the required values of attributes of the Device Type e.g. hardware version, Firmware Version); and
- The required Assurance Certificates.

The SEC does not constrain who supplies this information to the Panel: it could be the manufacturer, a Supplier, an Other User or an organisation that is not a Party. In this document, it is assumed that the organisation notifying the Panel is the manufacturer.

The manufacturer prepares the Device Model for testing:

- For all Device Types, the manufacturer submits the Device Model, Declaration of Conformity and Protocol Implementation Conformance Statement (PICS) for ZigBee testing to a ZigBee test lab. The test lab then provides test results to the ZigBee Alliance for assessment. If assessment is successful, the ZigBee Alliance issues a ZigBee Assurance Certificate for the Device Model; and
- For CH, Smart Meters and HCALCS, the manufacturer submits the Device Model for CPA testing to a CPA test lab. The test lab provides test results to the NCSC for assessment. If assessment is successful, the NCSC issues a CPA Certificate for the Device Model; or
- For Electricity Smart Meters, the manufacturer submits the Device Model and Conformance Test Information file for testing to a DLMS test lab. The test lab provides test results to the DLMS User Association for assessment. If the assessment is successful, the DLMS User Association issues a DLMS Certificate for the Device Model.

The manufacturer makes a CPL submission for Device Types (other than Type 2 Devices) to the Panel. For Type 2 Devices, the manufacturer provides the information to the Supplier who procured the Device Model. The Supplier keeps the record of it.

The Panel receives the CPL submission and checks whether each of the required values of attributes of the Device Type and all the Assurance Certificates required for the Device Type have been

provided. If the check is successful, the Panel adds the Device Model to the CPL with a status of 'current'. If the check fails, the Panel does not add the Device Model to the CPL.

Within one Working Day after being required to add or remove the Device Model from the CPL, the Panel does the following things:

- Publishes the updated CPL on the website;
- Sends a copy of the CPL to the DCC; and
- Notify the Parties that the CPL has been updated.

The DCC uses the CPL to update the SMI Status of Device Models. Within 24 hours from receiving the updated CPL, the DCC updates the SMI. Device Models with a CPL status of 'current' retain their SMI Status (provided that there is a corresponding entry in the SMI), while Devices Models with a CPL status of 'removed' have their SMI Status set to 'Suspended'.

7.1.2.4.2 Certificate Expiry

CPA Certification lasts for a period of 6 years and then expires. The Panel notifies the following Parties 12 and 6 months ahead of the expiry, to allow time for them to seek re-certification:

- The DCC for CH; and
- The Import Supplier or Gas Supplier (as applicable) responsible for Device Models of all other Physical Device Types.

If no action is taken and the CPA Certificate for a Device Model expires, the Panel sets the status of the Device Model on the CPL to 'removed'.

7.1.2.4.3 Suspend Device

If a Device Model is removed from the CPL, for example because its Certification has expired, the Panel sets the CPL status of the Device Model to 'removed'. The Panel provides a copy of the CPL to the DCC.

On receipt of the CPL extract, the DCC checks its records against the provided CPL extract and where a Device Model is marked as 'Removed' on the CPL extract, the DCC does the following things:

- Within 24 hours of receiving the CPL extract, updates the status of each Devices with the Device Model in the SMI to 'suspended' and sends a 'Device Suspended' DCC Alert (N28) to the relevant Supplier and Network Operator;
- Cancels all Schedules for the 'suspended' Device with the Device Model and sends a 'Schedule Removal because of Device Suspension' (N40) DCC Alert to each User who created a Schedule for that Device; and
- Deletes all Future Dated Service Requests for that Device with the Device Model and sends a 'Cancellation of Future Dated (DSP) requests because of Device Suspension' (N41) DCC Alert to each User that sent a Future Dated Service request for that Device.

Device Suspension has the effect of stopping all communications between Users and the Device, except to take it out of suspension.

7.1.2.4.4 Unsuspend Device

Remedial action is needed to take each Device with the Device Model out of 'suspension'. Depending upon the reason for suspension, this could be through, for example, updating the Firmware on the Device to address a vulnerability.

Once the remedial action is applied, a new entry on the CPL is created as described in the CPL submission section above. The status of the new Device Model is now set to 'current'. The DCC receives the updated CPL, updates the SMI Status of the Device to the one before 'suspension' and sends a 'Device Restored from Suspension' DCC Alert (N29) to the relevant Supplier and Network Operator.

7.1.2.5 Associated Process Area

#	Process Area
7.1.1	Manage Inventory

7.1.2.6 Governance

Actor	SEC Document	Clause	Text
7.1.2.4.1 CPL Submission			
Panel	Smart Energy Code	Section F2.1	The Panel shall establish and maintain a list of the Device Models for which the Panel has received all the Assurance Certificates required for the Physical Device Type relevant to that Device Model (the "**Certified Products List**"). https://smartenergycodecompany.co.uk/download/2476
Panel	Smart Energy Code	Section F2.2	The Panel shall ensure that the Certified Products List identifies the Data required in accordance with the CPL Requirements Document, and that the Certified Products List is updated to add and remove Device Models in accordance with the CPL Requirements Document. https://smartenergycodecompany.co.uk/download/2476
Panel	Smart Energy Code	Section F2.3	The Technical Specification relevant to the Physical Device Type sets out which Physical Device Types require Assurance Certificates from one or more of the following persons (each being an "**Assurance Certification Body**"): (a) the ZigBee Alliance; (b) the DLMS User Association; and (c) CESG. https://smartenergycodecompany.co.uk/download/2476
Panel	Smart Energy Code	Section F2.4	The following Assurance Certification Bodies issue the following certificates in respect of Device Models of the relevant Physical Device Types (each being, as further

			described in the applicable Technical Specification, an "**Assurance Certificate**"): (a) the ZigBee Alliance issues certificates which contain the ZigBee certified logo and interoperability icons; (b) the DLMS User Association issues certificates which include the conformance tested service mark ("**DLMS Certificates**"); and (c) CESG issues commercial product assurance scheme certificates ("**CPA Certificates**") https://smartenergycodecompany.co.uk/download/2476
Panel	SEC Appendix Z - CPL Requirements Document	2.1	The Panel shall ensure that the Certified Products List identifies each Device Model by Physical Device Type, and lists the following matters in respect of each Device Model: (a) Manufacturer and model; (b) hardware version; (c) firmware version; (d) the version of the SMETS or CHTS (as applicable) and (in each case) the GBCS version for which the Device Model has one or more Assurance Certificates; (e) the identification numbers for each of the Device Model's Assurance Certificates (including the version of the relevant standard against which each Assurance Certificate was issued); (f) the expiry date of the Device Model's CPA Certificate and the associated version of the Security Characteristics (as defined in the relevant Technical Specification); and (g) where there is an associated Manufacturer Image: (i) the relevant identity of the person who created the Manufacturer Image; (ii) a descriptor of the Manufacturer Image; and (iii) the Hash of the Manufacturer Image (to be provided pursuant to Clause 4). https://smartenergycodecompany.co.uk/download/2397
Panel	SEC Appendix Z - CPL Requirements Document	3.1	The Panel shall only add Device Models to the Certified Products List once the Panel has received all the Assurance Certificates required (under the Technical Specifications) to be obtained in respect of Device Models of the relevant Physical Device Type (which Assurance Certificates may be provided to the Panel by a Party or any other person). https://smartenergycodecompany.co.uk/download/2397
Supplier, DCC, Panel	SEC Appendix Z - CPL Requirements Document	5.1	An existing CPA Certificate for a Device Model may allow one or more additional Device Models to be added under that existing CPA Certificate, provided that any additional Device Model differs from the Device Model for which the CPA Certificate was originally issued only by virtue of having different versions of hardware and/or firmware that do not have a significant impact on the security functions of the

			Device Model (as set out in the CPA Assurance Maintenance Plan). Where this is the case: (a) the DCC for Communications Hubs; or (b) a Supplier Party for Device Models of all other Physical Device Types, may notify the Panel of one or more additional Device Models to be added to the CPA Certificate. https://smartenergycodecompany.co.uk/download/2397
Supplier, DCC	SEC Appendix Z - CPL Requirements Document	5.2	Where the DCC or a Supplier Party notifies the Panel of an additional Device Model pursuant to Clause 5.1, the DCC or the Supplier Party shall: (a) only do so in accordance with the terms of the relevant CPA Assurance Maintenance Plan; and (b) retain evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, such evidence to be provided to the Panel or the Authority on request. https://smartenergycodecompany.co.uk/download/2397
Panel	SEC Appendix Z - CPL Requirements Document	5.3	The Panel shall not be required to check whether the DCC or a Supplier Party (as applicable) is entitled to add a Device Model under the terms of the CPA Certificate and the CPA Assurance Maintenance Plan (as described in Clause 5.1). https://smartenergycodecompany.co.uk/download/2397
7.1.2.4.2 Certificate Expiry			
Panel	Smart Energy Code	Section F2.5	An Assurance Certificate will not be valid unless it expressly identifies the Device Model(s) and the relevant Physical Device Type to which it applies. An Assurance Certificate will not be valid if it specifies an expiry date that falls more than 6 years after its issue. https://smartenergycodecompany.co.uk/download/2476
Panel	Smart Energy Code	Section F2.6	As CPA Certificates will contain an expiry date, the following Parties shall ensure that a replacement CPA Certificate is issued in respect of Device Models for the following Physical Device Types before the expiry of such CPA Certificate (to the extent Device Models of the relevant Physical Device Type require CPA Certificates in accordance with the applicable Technical Specification): (a) the DCC for Communications Hubs; and (b) the Import Supplier and/or Gas Supplier (as applicable) for Device Models of all other Physical Device Types. https://smartenergycodecompany.co.uk/download/2476
Panel	Smart Energy Code	Section F2.7	The Panel shall notify the Parties on or around the dates occurring 12 and 6 months prior to the date on which the CPA Certificate for any Device Model is due to expire. https://smartenergycodecompany.co.uk/download/2476
7.1.2.4.3 Suspend Device			

Panel	SEC Appendix Z - CPL Requirements Document	6.1	Where an Assurance Certificate for a Device Model is withdrawn or cancelled by the Assurance Certification Body or (in the case of CPA Certificates) expires, then the Panel shall remove that Device Model from the Certified Products List. https://smartenergycodecompany.co.uk/download/2397
DCC, Supplier, Panel	SEC Appendix Z - CPL Requirements Document	6.2	The DCC and each Supplier Party shall notify the Panel of any withdrawal, expiry or cancellation of an Assurance Certificate of which the DCC or Supplier Party becomes aware. The Panel shall only remove a Device Model from the Certified Products List after the Panel has confirmed with the relevant Assurance Certification Body that the Assurance Certificate for that Device Model has expired or has been withdrawn or cancelled (and no new Assurance Certificate has been provided to the Panel under Clause 3). https://smartenergycodecompany.co.uk/download/2397
Panel	SEC Appendix Z - CPL Requirements Document	6.3	For the purposes of the Code, a Communications Hub Function or a Gas Proxy Function shall be considered to be on (or not on) the Certified Products List if the Communications Hub of which it forms part is on (or not on) the Certified Products List. https://smartenergycodecompany.co.uk/download/2397
Panel	SEC Appendix Z - CPL Requirements Document	6.4	The Panel may provide for the removal of a Device Model from the Certified Products List by marking that Device Model as 'removed'. All references in this Code to the removal of a Device Model from the Certified Products List (and similar expressions) shall be interpreted accordingly. https://smartenergycodecompany.co.uk/download/2397
DCC	Smart Energy Code	Section H6.10	Where a Device's Device Model is removed from the Certified Products List, that Device shall be Suspended and the DCC shall set the SMI Status of the Device to 'suspended'. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H6.11	Where a Communications Hub Device Model is removed from the Certified Products List, both the Communications Hub Function and the Gas Proxy Function shall be deemed to be Suspended (and Section H6.10 shall apply accordingly). https://smartenergycodecompany.co.uk/download/2483
DCC, User	Smart Energy Code	H6.12	Each User and the DCC shall each comply with the obligations set out in the Inventory, Enrolment and Decommissioning Procedures concerning Decommissioning and Suspension of Devices (and the Smart Metering Systems of which such Devices from part), including (where

			applicable) notifying other Users of such Decommissioning and Suspension. https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.12	The DCC shall not send a Command to a Smart Meter in response to a Service Request under Clause 4.11 where: (a) the Smart Meter is not listed within the Smart Metering Inventory; (b) the Smart Meter has an SMI Status of 'commissioned', 'decommissioned', 'withdrawn' or 'suspended'; and/or (c) the Communications Hub Function that is to form part of the same Smart Metering System is not listed in the Smart Metering Inventory with an SMI Status of 'commissioned'. https://smartenergycodecompany.co.uk/download/2275
User	SEC Appendix AB - Service Request Processing Document	2.1	A User shall take all reasonable steps to ensure that it does not send Service Requests in relation to Devices that have an SMI Status of 'suspended', other than where: (a) the Service Requests will (if Successfully Executed) result in the Device's Device Model becoming one that is listed on the Certified Products List; or (b) it is necessary to do so in order to update the Device Security Credentials following a change of Responsible Supplier. https://smartenergycodecompany.co.uk/download/2271
DCC, Network Operator	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	9.1	As soon as reasonably practicable following the Decommissioning, Withdrawal or Suspension of a Smart Meter, the DCC shall notify the Electricity Distributor or Gas Transporter for that Smart Meter of such Decommissioning, Withdrawal or Suspension, such notification to be made via the DCC User Interface. https://smartenergycodecompany.co.uk/download/2275
DCC, Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	9.2	As soon as reasonably practicable following the Suspension of a Device, the DCC shall notify the Responsible Supplier(s) for that Device of such Suspension, such notification to be made via the DCC User Interface. https://smartenergycodecompany.co.uk/download/2275
DCC	Smart Energy Code	Section H3.20	The DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services for which the Command has not yet been sent and which are due to be undertaken in respect of a Device after the Decommissioning or Suspension of that Device (and shall notify the relevant User of such cancellation via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2483
7.1.2.4.4 Unsuspend Device			

DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	7.3	Where a Device ceases to be Suspended (either as a result of the Device Model being added to the Certified Product List, or the Device's Device Model being modified such that it is on the Certified Product List), the DCC shall change the SMI Status of that Device to the status it held immediately prior to its Suspension. https://smartenergycodecompany.co.uk/download/2275

7.2 Install and Commission

This functional area describes how Devices added to the SMI are Enrolled into the DCC. The process of Enrolment into the DCC establishes end to end communications between SMSs and Suppliers via the DCC. Enrolling a SMS enables other Users to request Communication Services in respect of Devices forming part of that SMS, from the DCC.

The main path for Enrolment is via the Install and Commission process as laid out in Section 7.2.1 of the BAD. Where the WAN is not available at the site where a SMS is to be installed but the Supplier expected the WAN coverage to be available at that site, the Install and Leave process (described in Section 7.2.2 of the BAD) may be followed to begin the Enrolment of the SMS.

Once an SMS has been Enrolled (i.e. Smart Meters and GPF forming part of the SMS have been Commissioned), Suppliers are obligated to update Security Credentials on those Devices, which is covered by Post Commissioning Obligations (described in Section 7.2.3 of the BAD). This is to ensure the security of end-to-end communications.

7.2.1 Install and Commission

7.2.1.1 Introduction

This process area describes how Suppliers Enrol SMSs into the DCC. Once a SMS is Enrolled, other Users can request DCC Services in respect of Devices forming part of that SMS.

The processes covered in this process area apply equally to the initial installation of SMSs in new builds and replacement of conventional meters as well as replacement of individual Devices that are found to be faulty or have exceeded their effective life. This is provided that the WAN is available during the installation.

This process area describes a dual fuel Install and Commission starting with establishing an electricity SMS. The process treats each installation separately i.e. the process for installing and commissioning an electricity SMS excludes any processes for installing and commissioning a gas SMS, while the process for installing and commissioning a gas SMS excludes any processes for installing an electricity SMS. A single fuel installation of a gas SMS may require the use of a “Hot-shoe” – for more details please refer to SEC Section H12 - Intimate Communications Hub Interface Specification.

Suppliers have a licence obligation to Enrol SMSs and therefore to Commission Smart Meters and GPFs as soon as reasonably practicable. This is because Enrolment of an SMS occurs:

- in the case of electricity, on the Commissioning of the Electricity Smart Meter forming part of that SMS; or

- in the case of gas, on the Commissioning of both the Gas Smart Meter and the GPF forming part of that SMS.

7.2.1.2 Scope

This process area includes:

- Install Communications Hub
- Install Devices
- Communications Hub Status Update – Install Success
- Update HAN Device Log – Add Device
- Commission Device
- Set Device Configuration (Import MPxN)
- Join Service
- Remote CAD Pairing

This process area involves but does not specifically describe:

- Read (Non-Device) - Request WAN Matrix. This is described in Section 7.4.1.6.3 of the BAD.
- Read (Non-Device) - Read Inventory. This is described in Section 7.4.1.6.3 of the BAD.
- Device Pre-notification. This is described in Section 7.1.1.6.2 of the BAD.
- Order and Return Communications Hub. This is described in Section 7.9.1 of the BAD.
- The process for configuring a Smart Meter once installed. This is described in Section 7.3 of the BAD.
- The installation process when there is no WAN coverage. This is described in Section 7.2.2 of the BAD.
- Post Commissioning Obligations. This is described in Section 7.2.3 of the BAD.
- Update Security Credentials (KRP). This is described in Section 7.7.2.5.6 of the BAD.
- Request Handover of DCC Controlled Device. This is described in Section 7.7.2.5.5 of the BAD.

7.2.1.3 Inputs

- 'Set Device Configuration (Import MPxN)' Service Request (SRV 6.20.1)
- 'Commission Device' Service Request (SRV 8.1.1)

- ‘Join Service (Critical)’ Service Request (SRV 8.7.1)
- ‘Join Service (Non-critical)’ Service Request (SRV 8.7.2)
- ‘Update HAN Device Log’ Service Request (SRV 8.11)
- ‘Communications Hub Status Update - Install Success’ Service Request (SRV 8.14.1)

7.2.1.4 Actors

- Supplier
- Network Operator
- DCC
- CH
- Smart Meter
- Type 1 Device
- Type 2 Device
- Registered Supplier Agent
- Installer

7.2.1.5 Prerequisites

- For CHF and GPF only; Trust Anchor Cells are populated with the relevant Security Credentials by the DCC.
- For all other Devices (except for Type 2 Devices); Trust Anchor Cells are populated with the relevant Security Credentials by the Party whom has procured the Device. (See Table 4).
- As far as practicable, ensure that Devices are configured as requested by the Network Operator[14].
- The CH and any Meters or Type 1 Devices are listed on the SMI and are present on the CPL.
- Devices to be installed are pre-notified to the SMI.
- The SM WAN Coverage is available at the site.

[14] While not required by the SEC, Electricity Distributors laid out the recommended configuration for Electricity Smart Meters as those set out in Engineering Recommendation M30 Standard Electricity Network Operator electricity smart meter configurations and Engineering Recommendation M31 DNO strategy for Supplier population of ESME Network Operators’ Trust Anchor Cells.

Table 4. Security Credentials Populated in Trust Anchor Cells

Remote Party Role	Certificate
Root	the Root OCA Certificate
Recovery	the DCC Recovery Certificate
Access Control Broker	a DCC Access Control Broker Certificate
Transitional CoS	the DCC Transitional CoS Certificate
Supplier	One of the following: (a) one of the relevant Supplier Party's Organisation Certificates; (b) a DCC Access Control Broker Certificate; (c) (where the consent of that other Supplier Party has been given) another Supplier Party's Organisation Certificate.
Network Operator	One of the following: (a) one of the relevant Network Operator's Organisation Certificates; (b) one of the relevant Supplier Party's Organisation Certificates; (c) (where the consent of that other Supplier Party has been given) another Supplier Party's Organisation Certificate; (d) a DCC Access Control Broker Certificate. (NB Network Operator Certificates are required for Electricity Smart Meter and Gas Proxy Function only)
WAN Provider	A CSP WAN Provider certificate

7.2.1.6 Process Description

It is expected that prior to the installation the Supplier follows the following pre-installation steps:

7.2.1.6.1 Device Pre-notification

(Step 1) The DCC and Users pre-notified the applicable Devices to the SMI. The process for pre-notifying Devices is described in Section 7.1.1.6.2 of the BAD.

7.2.1.6.2 –Read (Non-Device) - Request WAN Matrix

(Step 2) Within 30 days before installation, the Supplier checked the WAN Matrix to ascertain whether there is SM WAN coverage at the site and the type of WAN Variant required for the site. The process for Requesting WAN Matrix is described in Section 7.4.1.6.3 of the BAD.

7.2.1.6.3 –Read (Non-Device) - Read Inventory

(Step 3) The Supplier obtained any required information from the SMI. The process for Reading Inventory is described in Section 7.4.1.6.3 of the BAD.

7.2.1.6.4 Install Communications Hub

For dual fuel and single fuel electricity only installations, once on site, the Installer physically installs the Electricity Smart Meter, and then the CH. This is to provide a power source for the CH. A single fuel gas SMS installation may require the use of a "Hot-shoe" to provide a power source for the CH. Further detail on the CH installation process can be found in SEC Appendix I - Communications Hub Installation and Maintenance Support Materials (CHIMSM).

Once the CH is installed the Installer powers it up. The CH is designed to automatically connect to the SM WAN. When it does so, it does the following:

- Synchronises its time with the Network Time; and
- Identifies itself to the DCC, which is an automatic process.

After receiving a communication from the CH, the DCC validates it and updates the SMI Status of the CHF on the SMI to 'Commissioned'. The DCC then records any information that is necessary for the DCC to communicate with the CH.

The SM WAN Indicator on the CH confirms to the Installer that the CH has established a connection to the SM WAN. The Installer notifies the Supplier of that fact, which is an out of band process. The Installer also passes the Device details, including the Device ID, and information to confirm site details, to the Supplier.

If the CH does not connect to the SM WAN, the Supplier may elect to abort the installation or continue following the Install and Leave process as set out in Section 7.2.2 of the BAD.

Dual Band Communications Hubs may require configuration of the Sub-GHz Channels. The supplier is able to set the Sub-GHz Configuration items on the CHF using Service Request 6.29, for further information see section **Error! Reference source not found.**.

The supplier may wish to read the current CHF sub-GHz configuration values, this is achieved via SR 6.30 "Read CHF Sub-GHz Configuration", see 7.4.1.6.2

7.2.1.6.5 Install Devices

The Installer physically installs additional Devices as required (Gas Smart Meter, PPMID, HCALCS, IHD). It is unusual to have both a PPMID and an IHD in the same SMS, but these are included for completeness in both the electricity SMS and gas SMS. The Installer passes the Device details,

including Device IDs, and information and site details to the Supplier, which is an out-of-band process.

7.2.1.6.6 Communications Hub Status Update – Install Success

Within 5 Working Days from receiving the confirmation from the Installer of CH connection to the SM WAN, the Supplier composes and sends a 'Communications Hub Status Update - Install Success' Service Request (SRV 8.14.1) to the DCC.

The DCC receives it and completes Non-Device Service Request processing. The DCC updates its asset management systems and sends a Service Response to the Supplier.

7.2.1.6.7 Update HAN Device Log – Add Device

The Supplier receives the Device and site details and looks up the MPxN for the site. For a Device to join a SM HAN, each Device needs to be added to the CHF Device Log. The Supplier does this by composing an 'Update HAN Device Log' Service Request (SRV 8.11) for each Device to be added. The Supplier sends the 'Update HAN Device Log' Service Request for each Device to be added to the DCC.

The DCC receives it, completes Non-Critical Service Request processing, and sends an 'Add Device to CHF Device Log' CCS01 Command to the CHF.

The CHF receives the Command, executes it by adding the Device ID to its Device Log, and sends a Response to the DCC. The DCC receives the Response and does the following things:

- For Meters and Type 1 Devices, sets the SMI Status of the Device to 'Whitelisted';
- For all Devices, Associates the Device with the CHF in the SMI;
- For Meters only, Associates the MPxN and Meter in the SMI;
- For Meters only; sends a 'Device Identity Confirmation' N16 DCC Alert to the Network Operator identified based in the Registration Data to inform them that there is a new Meter at the Meter Point in their area; and
- For all Devices, sends a Service Response (SRV 8.11) to the Supplier.

After a Device ID is added to the CHF Device Log, the CHF sends an initial CS14 'CHF Device Log Changed' (0x8F12) Device Alert to the DCC. This Device Alert is stored on the DCC Systems to support the Replace Communications Hub process area (see Section 7.6.1 of the BAD). This Device Alert is stored until a more recent CS14 Device Alert is received by the DCC. At which point, all previous CS14 Device Alerts are discarded.

The CHF sets its beacon to allow the Device to join, in a ZigBee sense, the SM HAN. The Device detects the SM HAN set by the CHF and requests to join it. The CHF Authenticates the Device to join the SM HAN using the Install Code provided in Service Request 'Update HAN Device Log' (SRV 8.11) and then undertakes CBKE with the Device. On successful completion of CBKE, the Device is then joined to the SM HAN.

Once the Device joins the SMHAN, the CHF updates its Device Log and sends a second CS14 'CHF Device Log Changed' (Alert Code:0x8F12) Device Alert containing the new Device Log to the DCC. The DCC receives it and stores this Device Alert and discards the previous one.

For Gas Smart Meter only; once the Device has successfully completed CBKE with the CHF, the Gas Smart Meter sends a request to the GPF requesting the creation of a Mirror. This Mirror is also required to be configured by the Gas Smart Meter.

For Meters only, if at least one of the Supplier's Trust Anchor Cells is populated with a Supplier's Organisation Certificate, the Meter sends a 'Device Commissioned' Device Alert (Alert Code: 0x8F69) to the DCC, which the DCC forwards to the Supplier. The Meter may also send a 'Device joined SMHAN' Device Alert (Alert Code: 0x8183) to the DCC, which the DCC forwards to the Supplier.

The DCC checks that the second CS14 'CHF Device Log Changed' Device Alert (Alert Code: 0x8F12) is received within the join timeout period specified in the Service Request. If the DCC receives this Device Alert within the join timeout period, it does the following things:

- For all Devices, sends a 'Successful Communications Hub Function Whitelist Update' (N24) DCC Alert to the Supplier; and
- For Meters and Type 1 Devices, sets the SMI status of the Device to ‘Installed not Commissioned’.

If the DCC does not receive this Device Alert within the join timeout period, the DCC, for all Devices, sends a 'Potentially Unsuccessful Communications Hub Function Whitelist Update' (N25) DCC Alert to the Supplier to confirm that the communication between the CHF and the Device may not have been established.

7.2.1.6.8 Request Handover of DCC Controlled Device

Before Commissioning a Meter, the Supplier must ensure its Organisation Certificates are on the Device. Where the DCC’s Organisation Certificates are in the Supplier’s Trust Anchor Cells, the Supplier replaces the DCC’s Organisation Certificates with its own Organisation Certificates. In this case, the Supplier uses a ‘Request Handover of DCC Controlled Device’ Service Request (SRV 6.21). For more information on the process see Section 7.7.2.5.5 of the BAD.

7.2.1.6.9 Update Security Credentials (KRP)

For operational reasons (e.g. where a Supplier has multiple Market Participant IDs (MPID) and for convenience, the Supplier may wish to insert the Organisation Certificates relating to just one MPID onto a Device at manufacture. If subsequently the Organisation Certificates need to be replaced with the Certificates relating to the relevant MPID. the Supplier will need to use a ‘Update Security Credentials (KRP)’ SRV (SRV 6.15.1). For more information on the process see Section 7.7.2.5.6 of the BAD.

7.2.1.6.10 Commission Device

To Commission a Meter, the Supplier composes a ‘Commission Device’ Service Request (SRV 8.1.1) and sends it to the DCC.

The DCC receives it, completes Critical Service Request processing, and sends a 'Set Clock' Command (ECS70) to the Electricity Smart Meter, or a 'Set Clock' (GCS28) to the Gas Smart Meter. The Smart Meter receives the 'Set Clock' Command and executes it and sends a Response to the DCC. The DCC receives the Response from the Smart Meter and does the following things:

- Sets the Meter status to 'Commissioned' in the SMI; and
- Sends a Service Response (SRV 8.1.1) to the Supplier.

7.2.1.6.11 Configure Device - Set Device Configuration (Import MPxN)

To meet the obligation to display the MPxN on the Meter as soon as practicable after Commissioning the Meter, the Supplier composes a 'Set Device Configuration (Import MPxN)' Service Request (SRV 6.20.1) and sends it to the DCC. For more information on the process see Section 7.3.1.6.3 of the BAD.

7.2.1.6.12 Join Service

After the Devices are added to the CHF Device Log, they can communicate at the network level, but they need to be joined ("paired") at the application level as well. The exact sequence will depend upon the Devices to be joined, and the preference of the Supplier. This process covers all possible Devices and treats each installation separately i.e. the process for creating an electricity SMS excludes any processes for creating a gas SMS, while the process for creating a gas SMS excludes any processes for creating an electricity SMS.

Join Electricity Smart Meter to IHD

The Import Supplier composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the IHD to be joined, addressed to the Electricity Smart Meter, and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing, and sends a 'Method B Join' (CS02B) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command and executes it by adding the IHD's Security Credentials to its Device Log, and effects the join to the IHD using the mechanisms described in the GBCS.

The Electricity Smart Meter sends a Response to the DCC. The DCC receives the Response and does the following things:

- Associates the IHD with the Electricity Smart Meter in the SMI; and
- Sends a Service Response (SRV 8.7.2) to the Import Supplier.

The Electricity Smart Meter and the IHD are now joined.

Join PPMID and Electricity Smart Meter

The Import Supplier composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the Electricity Smart Meter to be joined, addressed to the PPMID, and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method A Join (non-Meter)' (CS03A2) Command to the PPMID.

The PPMID receives the Command, executes it by adding the Electricity Smart Meter's Security Credentials to its Device Log, and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 8.7.2) to the Import Supplier.

The Import Supplier receives the Service Response and composes a 'Join Service (Critical)' Service Request (SRV 8.7.1), identifying the PPMID to be joined, addressed to the Electricity Smart Meter, and sends it to the DCC.

The DCC receives it, completes Critical Service Request processing and sends a 'Method A Join (Meter)' (CS03A1) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command and executes it by adding the PPMID's Security Credentials of to its Device Log. The Electricity Smart Meter undertakes CBKE with the PPMID, which enables communication between the two.

The Electricity Smart Meter sends a Response to the DCC. The DCC receives the Response and does the following things:

- Associates the PPMID with the Electricity Smart Meter in the SMI;
- Sets the PPMID's SMI Status to 'Commissioned' if the Electricity Smart Meter is 'Commissioned', or 'Installed not Commissioned' if the Electricity Smart Meter is 'Installed not Commissioned; and
- Sends a Service Response (SRV 8.7.1) to the Import Supplier.

The Electricity Smart Meter and the PPMID are now joined.

Join HCALCS and Electricity Smart Meter

The Import Supplier composes a 'Join Service (Critical)' Service Request (Service Request Variant 8.7.1), identifying the Electricity Smart Meter to be joined, addressed to the HCALCS, and sends it to the DCC.

The DCC receives it, completes Critical Service Request processing and sends a 'Method A Join (non-Meter) CS03A2' Command to the HCALCS.

The HCALCS receives the Command, executes it by adding the Electricity Smart Meter's Security Unique Identifier to its Device Log, and sends a CS03A2 Response to the DCC.

The DCC receives the Response and sends a Service Response (Service Reverence Variant 8.7.1) to the Import Supplier.

The Import Supplier receives the Service Response and composes a 'Join Service (Critical)' Service Request (SRV 8.7.1), identifying the HCALCS to be joined, addressed to the Electricity Smart Meter, and sends it to the DCC.

The DCC receives it, completes Critical Service Request processing and sends a 'Method A Join (Meter) (CS03A1)' Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command, executes it by adding the HCALCS' Security Credentials to its Device Log, and effects the join between the two Devices using the mechanisms described in the GBCS.

The Electricity Smart Meter sends a Response to the DCC. The DCC receives the Response from the Electricity Smart Meter, and does the following things:

- Associates the HCALCS with the Electricity Smart Meter in the SMI;
- Sets the HCALCS SMI Status to 'Commissioned' if the Electricity Smart Meter is 'Commissioned', or 'Installed not Commissioned' if the Electricity Smart Meter is 'Installed not Commissioned'; and
- Sends a Service Response (SRV 8.7.1) to the Import Supplier.

The Electricity Smart Meter and the HCALCS are now joined.

For a single fuel electricity only installation, the process stops here. For a dual fuel installation or for a single fuel gas only installation the Supplier joins the following Devices:

Join Gas Smart Meter to GPF

The Supplier composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the GPF to be joined, addressed to the Gas Smart Meter, and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method B Join (CS03B)' Command to the Gas Smart Meter.

The Gas Smart Meter receives the Command and executes it by adding the GPF's Security Credentials to its Device Log. The Gas Smart Meter effects the join between the two Devices using the mechanisms described in the GBCS.

The Gas Smart Meter sends a Response to the DCC. The DCC receives the Response, and does the following things:

- Associates the Gas Smart Meter with the GPF in the SMI;
- Sets the GPFs SMI Status to 'Commissioned' if the Gas Smart Meter is 'Commissioned', or if the Gas Smart Meter is 'Installed not Commissioned, sets the GPF SMI Status to 'Installed not Commissioned'; and
- Sends a Service Response (SRV 8.7.2) to the Supplier.

Join Gas Smart Meter and GPF to PPMID

The Gas Supplier composes a 'Join Service (Non-Critical)' Service Request (SRV 8.7.2), identifying the PPMID to be joined, addressed to the GPF, and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method B Join (CS03B)' Command the GPF.

The GPF receives the Command and executes it by adding the PPMID's Security Credentials to its Device Log, and effects the join between the two Devices using the mechanisms described in the GBCS.

The GPF sends a Response to the DCC. The DCC receives the Response and does the following things:

- Associates the PPMID and the GPF in the SMI;
- Updates the SMI Status of the PPMID to 'Commissioned' if the GPF is 'Commissioned'. If the GPF is 'Installed not Commissioned', the DCC sets the PPMID SMI Status to 'Installed not Commissioned'; and
- Sends a Service Response (SRV 8.7.2) to the Gas Supplier.

The GPF sends an GCS62 Alert to the DCC containing the contents of the GPF device log, the data is stored for use during the Communications Hub replacement process (as described in section 7.6.1) to restore the GPF device Log (Service Request 8.12.2).

The Gas Supplier receives the Service Response (SRV 8.7.2) and composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the Gas Smart Meter to be joined, addressed to the PPMID, and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method C Join (CS03C)' Command to the PPMID.

The PPMID receives the Command and executes it by adding the Gas Smart Meter's Security Credentials to its Device Log and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 8.7.2) to the Gas Supplier. The Gas Supplier receives the Service Response and composes a 'Join Service' (Critical) Service Request (SRV 8.7.1), identifying the PPMID to be joined, addressed to the Gas Smart Meter, and sends it to the DCC.

The DCC receives it, completes Critical Service Request processing and sends a 'Method C Join (CS03C)' Command to the Gas Smart Meter.

The Gas Smart Meter receives the Command and executes it by adding the PPMID's Security Credentials to its Device Log, and effects the join between the two Devices using the mechanisms described in the GBCS.

The Gas Smart Meter sends a Response to the DCC. The DCC receives the Response and does the following things:

- Associates the PPMID and Gas Smart Meter in the SMI;
- Updates the SMI Status of the PPMID to 'Commissioned' if the Gas Smart Meter is 'Commissioned', or 'Installed not Commissioned' if the Gas Smart Meter is 'Installed not Commissioned; and
- Sends a Service Response (SRV 8.7.1) to the Gas Supplier.

Join GPF to IHD

The Gas Supplier composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the IHD to be joined, addressed to the GPF, and sends this to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method B Join (CS03B)' Command to the GPF.

The GPF receives the Command and executes it by adding the IHD's Security Credentials to its Device Log, and effects the join between the two Devices using the mechanisms described in the GBCS.

The GPF sends a Response to the DCC. The DCC receives the Response and does the following things:

- Associates the IHD with the GPF in the SMI; and
- Sends a Service Response (SRV 8.7.2) to the Gas Supplier.

The GPF sends an GCS62 Alert to the DCC containing the contents of the GPF device log, the data is stored for use during the Communications Hub replacement process (as described in section 7.6.1) to restore the GPF device Log (Service Request 8.12.2).

7.2.1.6.13 Configure Device

The Install and Commission process is now complete. The Supplier may now carry out Configuration activities for the SMS. For more information on the Configuration process, please see Section 7.3 of the BAD.

7.2.1.6.14 Remote CAD Pairing

For a CAD to join a SM HAN, a User needs to add it to the CHF Device Log. (The CAD is the only Device that an Other User can join to the SM HAN.) The User does this by composing an 'Update HAN Device Log' Service Request (SRV 8.11). This process is described in detail in Section 7.2.1.6.7 of the BAD.

After the CAD is added to the CHF Device Log, it needs to be joined ("paired") at the application level as well to the Electricity Smart Meter and/or GPF. To join the CAD to the Electricity Smart Meter, the User composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the CAD to be joined, addressed to the Electricity Smart Meter, and sends it to the DCC. To join a CAD to the GPF, the User composes a 'Join Service' (Non-Critical) Service Request (SRV 8.7.2), identifying the CAD to be joined, addressed to the GPF, and sends it to the DCC. The process for joining CADs is the same as for joining any other Device, and it is described in Section 7.2.1.6.12 of the BAD.

7.2.1.7 Associated Process Areas

#	Process Areas
7.1.1	Manage Inventory
7.2.2	Install and Leave
7.2.3	Post Commissioning Obligations
7.3	Configure Device and Payment Mode
7.4.1	Read
7.7.2	Manage Security Credentials
7.9.1	Order and Return Communications Hub

7.2.1.8 Governance

Actor	SEC Document	Clause	Text
7.2.1.6.4 Install Communications Hub			
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	4.1	When attempting the initial installation of a Communications Hub, a Supplier Party shall ensure that it uses the WAN Variant that was identified as being required for the Installation Location on the Coverage Database when the Supplier Party checked the Coverage Database, provided that this check was performed at any time within the period 30 days prior to the Installation Date. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	4.3	When installing a Communications Hub or Communications Hub Auxiliary Equipment, as set out in the Annex E of this document, a Supplier Party shall ensure that all appropriate tolls and equipment are used. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	4.4	A Supplier Party shall ensure that a Communications Hub is fitted according to the procedure set out in Annex A of this document. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.1	Subject to Clause 4.2, where the DCC receives a communication originating from a Communications Hub Function which does not have an SMI Status of 'commissioned' confirming that it has connected to the SM WAN, the DCC shall update the SMI Status of that Communications Hub Function to 'commissioned'. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC	4.2	Before taking the step set out in Clause 4.1, the DCC shall confirm whether the communication originates from the

	- Inventory Enrolment and Withdrawal Procedures		Communications Hub Function that is identified within the communication. The DCC shall not take the step set out in Clause 4.1 in respect of a Communications Hub Function where: (a) the Communications Hub Function is not listed within the Smart Metering Inventory; (b) the Communications Hub Function is not identified in the Smart Metering Inventory as having an SMI Status of 'pending' or 'installed not commissioned'; and/or (c) the communication may have changed in transit or does not originate from the Communications Hub Function that is identified within the communication. https://smartenergycodecompany.co.uk/download/2275
7.2.1.6.5 Install Devices			
DCC, Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	3.1	Before: (a) a Responsible Supplier sends a Service Request which may result in the sending of a Command to a Smart Meter, Gas Proxy Function or Type 1 Device; or (b) the DCC delivers a Communications Hub (comprising a Communications Hub Function and a Gas Proxy Function) to a Party in accordance with the Communications Hub Service, the Responsible Supplier or DCC (as the case may be) shall ensure that each Trust Anchor Cell on that Device which is required by the GB Companion Specification to be populated with credentials is populated with credentials in accordance with the requirements of Clause 3.2. https://smartenergycodecompany.co.uk/download/2275
DCC, Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	3.2	The requirements of this Clause 3.2 are that: (a) each Trust Anchor Cell with the Remote Party Role listed in the table immediately below shall be populated with the Security Credentials from the Certificate (or, as indicated, one of the Certificates) identified in relation to that Remote Party Role in the second column of that table; and (b) in each case the relevant Certificate shall have a keyUsage value which is the same as that of the Trust Anchor Cell it populates. Where 'DCC Recovery Certificate', 'DCC Transitional CoS Certificate', 'DCC Access Control Broker Certificate' and 'DCC WAN Provider Certificate' are each Organisation Certificates created by the DCC for the purposes of occupying the relevant Trust Anchor Cells on Devices in accordance with the above table and used by those DCC Systems described in (respectively) sub-paragraphs (f), (c), (a) and (a) of the definition of DCC Live Systems. https://smartenergycodecompany.co.uk/download/2275

Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	3.3	Where and to the extent that the Electricity Distributor or Gas Transporter for a Device has notified the Responsible Supplier for the Device of the values for the 'NP Configurable Data Items' that the Electricity Distributor or Gas Transporter (as applicable) wishes to have configured on the Device at the time of its Commissioning, the Responsible Supplier shall take all reasonable steps to ensure that those data items are so configured on the Device at the time of its Commissioning. In this Clause 3.3, 'NP Configurable Data Items' means those data items held on Devices that are capable of being configured via Services Requests for which the User Role of 'Electricity Distributors' or 'Gas Transporter' (as applicable) is an Eligible User Role. https://smartenergycodecompany.co.uk/download/2275
7.2.1.6.6 Communications Hub Status Update – Install Success			
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	4.6	Where, during the installation process, the Supplier Party suspects that a fault has occurred with the Communications Hub, the relevant Supplier Party shall follow the procedures set out in clauses 8.1 to 8.13 of this document. https://smartenergycodecompany.co.uk/download/2336
7.2.1.6.7 Update HAN Device Log – Add Device			
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.3 (a)	update the Smart Metering Inventory to Associate the Device with the applicable Communications Hub Function; https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.3(b)	in the case of Smart Meters only, record the MPAN(s) or MPRN (as applicable) provided within the Service Request against that Smart Meter and notify the Electricity Distributor or Gas Transporter (as applicable) of the MPAN(s) and/or MPRN and of the Smart Meter's Device ID and Device Type; and https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.101.4(b)	Where the Device ID to be added to HAN Device Log is an Electricity Smart Meter or a Gas Smart Meter, the association between the Device ID and its MPxN(s) is recorded in the Smart Metering Inventory and DCC Alert N16 is sent to the Electricity Distributor or Gas Transporter (as applicable) https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD	3.8.109.4(b)	Where the Device ID to be added to HAN Device Log is an Electricity Smart Meter or a Gas Smart Meter, the

	- DCC User Interface Specification v2.0		association between the Device ID and its MPxN(s) is recorded in the Smart Metering Inventory and DCC Alert N16 is sent to the Electricity Distributor or Gas Transporter (as applicable) https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.3(c)	other than in the case of a Type 2 Device, set the SMI Status of the Device to 'whitelisted'. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.101.4(a)	Upon receipt of a successful Response resulting from the Update HAN Device Log Service Request to Add a Device, the DCC shall, for the specified Device ID identified within the Service Request, perform the following action. a) Update the Smart Metering Inventory and set the Device status of the Device ID to 'Whitelisted' https://smartenergycodecompany.co.uk/download/2275
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.109.4(a)	Upon receipt of a successful Response resulting from the Update HAN Device Log Service Request to Add a Device, the DCC shall, for the specified Device ID identified within the Service Request, perform the following action. a) Update the Smart Metering Inventory and set the Device status of the Device ID to 'Whitelisted' https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.3(b)	in the case of Smart Meters only, record the MPAN(s) or MPRN (as applicable) provided within the Service Request against that Smart Meter and notify the Electricity Distributor or Gas Transporter (as applicable) of the MPAN(s) and/or MPRN and of the Smart Meter's Device ID and Device Type; and https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	8.1	The DCC shall monitor Alerts and Responses sent from each Communications Hub Function and Gas Proxy Function in order to establish and maintain an up-to-date electronic record of the most recent information stored in the Device Log of each such Device. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.101.4(b)	Where the Device ID to be added to HAN Device Log is an Electricity Smart Meter or a Gas Smart Meter, the association between the Device ID and its MPxN(s) is recorded in the Smart Metering Inventory and DCC Alert N16 is sent to the Electricity Distributor or Gas Transporter (as applicable)

			https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.109.4(b)	Where the Device ID to be added to HAN Device Log is an Electricity Smart Meter or a Gas Smart Meter, the association between the Device ID and its MPxN(s) is recorded in the Smart Metering Inventory and DCC Alert N16 is sent to the Electricity Distributor or Gas Transporter (as applicable) https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.101.4	The DCC Systems shall wait for a timeout period to receive the updated Device Log from the CHF following the successful execution of an Update HAN Device Log Service Request to Add a Device. The timeout period that the DCC Systems shall wait for the Device Alert is defined as "Join Time Period" as specified within the Service Request plus a configurable network transmission time to allow delivery of the Device Alert over the SM WAN. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.109.4	The DCC Systems shall wait for a timeout period to receive the updated Device Log from the CHF following the successful execution of an Update HAN Device Log Service Request to Add a Device. The timeout period that the DCC Systems shall wait for the Device Alert is defined as "Join Time Period" as specified within the Service Request plus a configurable network transmission time to allow delivery of the Device Alert over the SM WAN. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.101.4	If a copy of the CHF Device Log confirming communications have been established with the Device specified in the Service Request is received within the timeout period, then the DCC Systems shall notify the Responsible Supplier for the specified Device via a DCC Alert N24, and for i. ESME GSME, HCALCS and PPMID, the Device Status is set to 'InstalledNotCommissioned' in the Smart Metering Inventory. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.109.4(a)	If the CHF Device Log confirming communications have been established with the Device specified in the Service Request is received within the timeout period, then the DCC Systems shall notify the Responsible Supplier for the specified Device via a DCC Alert N24, and; i. For ESME, GSME, HCALCS and PPMID the Device Status is set to 'InstalledNotCommissioned' in the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/4639

DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.4	Following the receipt of an Alert from a Communications Hub Function informing the DCC that the Communications Hub Function is able to communicate over the HAN with a Device, the DCC shall (other than in the case of a Type 2 Device, or where the relevant Device already has an SMI Status of 'commissioned') set the SMI Status of the Device to 'installed not commissioned'. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.101.4	If a copy of the CHF Device Log confirming communications have been established with the Device specified in the Service Request is not received within the timeout period, then the DCC Data Systems informs the DCC Service User via a DCC Alert N25. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.109.4(b)	If the CHF Device Log confirming communications have been established with the Device specified in the Service Request is not received within the timeout period, then the DCC Systems informs the User via a DCC Alert N25. https://smartenergycodecompany.co.uk/download/4639
7.2.1.6.10 Commission Device			
Supplier	Smart Energy Code	Section H5.1	Enrolment of a Smart Metering System occurs: (a) in the case of electricity, on the Commissioning of the Electricity Smart Meter forming part of that Smart Metering System; or (b) in the case of gas, on the Commissioning of both the Gas Smart Meter and the Gas Proxy Function forming part of that Smart Metering System. https://smartenergycodecompany.co.uk/download/2483
DCC, Supplier	Smart Energy Code	Section H5.2	No Device that is to form part of a Smart Metering System (other than the Communications Hub Function) can be Commissioned before the Communications Hub Function that is to form part of that Smart Metering System has been Commissioned. https://smartenergycodecompany.co.uk/download/2483
DCC, Supplier	Smart Energy Code	Section H5.3	No Device can be Commissioned unless it is: (a) listed on the Smart Metering Inventory; and (b) other than for Type 2 Devices, listed with an SMI Status which is not 'withdrawn' or 'decommissioned'. https://smartenergycodecompany.co.uk/download/2483
Supplier	SEC Appendix AC - Inventory Enrolment and	4.11	Were a Responsible Supplier wishes to Commission a Smart Meter, the Responsible Supplier shall send the DCC a 'Commission Device' Service Request in respect of that Smart Meter.

	Withdrawal Procedures		https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.12	The DCC shall not send a Command to a Smart Meter in response to a Service Request under Clause 4.11 where: (a) the Smart Meter is not listed within the Smart Metering Inventory; (b) the Smart Meter has an SMI Status of 'commissioned', 'decommissioned', 'withdrawn' or 'suspended'; and/or (c) the Communications Hub Function that is to form part of the same Smart Metering System is not listed in the Smart Metering Inventory with an SMI Status of 'commissioned'. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.13	Following the receipt of a Response over the SM WAN that indicates the Successful Execution of a 'Commission Device' Service Request in accordance with Clauses 4.11 and 4.12 in respect of a Smart Meter, the DCC shall update the SMI Status of the Smart Meter to 'Commissioned'. https://smartenergycodecompany.co.uk/download/2275
7.2.1.6.11 Set Device Configuration (Import MPxN)			
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.14	As soon as reasonably practicable after the Successful Execution of a 'Commission Device' Service Request, the Responsible Supplier shall send a 'Set Device Configuration (Import MPxN)' Service Request to ensure that the relevant MPAN or MPRN (as applicable) is available for display upon the Smart Meter. https://smartenergycodecompany.co.uk/download/2275
7.2.1.6.12 Join Service			
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.5	Where a Responsible Supplier wishes to join any Device (other than a Communications Hub Function or Type 2 Device) to a Smart Meter or a Gas Proxy Function, the Responsible Supplier shall send the DCC a 'Join Service' Service Request to add the relevant Device to the Device Log of the relevant Smart Meter or Gas Proxy Function. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.6	The DCC shall not send a Command to join a Device to a Smart Meter or Gas Proxy Function in response to a Service Request under Clause 4.5 where: (a) the Device is not listed within the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'; (b) the Communications Hub Function that is to form part of the same Smart Metering System is not listed in the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'; and/or (c) the Smart Meter or Gas Proxy Function with which the Device is to be joined is not listed in the Smart Metering

			Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.8 (b)	In respect of Type 2 Devices: (b) the DCC shall not send a Command to join a Type 2 Device to a Smart Meter or Gas Proxy Function in response to a Service Request under Clause 4.8(a) where the Electricity Smart Meter or Gas Proxy Function with which the Type 2 Device is to be Associated is not listed in the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'; and https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.7	On the Successful Execution of a 'Join Service' Service Request to add a Device to the Device Log of a Smart Meter or Gas Proxy Function in accordance with Clauses 4.5 and 4.6, the DCC shall Associate that Device with the applicable Smart Meter or Gas Proxy Function (as applicable), and either: (a) where the Smart Meter or Gas Proxy Function (as applicable) has an SMI Status of 'installed not commissioned', set the SMI Status of the Device to 'installed not commissioned'; or (b) where the Smart Meter or Gas Proxy Function (as applicable) has an SMI Status of 'commissioned', set the SMI Status of the Device to 'commissioned'. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.8 (c)	In respect of Type 2 Devices: (c) on the Successful Execution of a 'Join Service' Service Request to add a Type 2 Device to the Device Log of a Smart Meter or Gas Proxy Function in accordance with (a) and (b) above, the DCC shall Associate that Device with the applicable Smart Meter or Gas Proxy Function (as applicable). https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.9	Where a Responsible Supplier wishes to Commission a Type 1 Device, it shall send (under Clause 4.5) a 'Join Service' Service Request to add the Type 1 Device to the Device Log of a Commissioned Electricity Smart Meter or a Commissioned Gas Proxy Function (as applicable). https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC - Inventory Enrolment and	4.10	Where a Responsible Supplier wishes to Commission a Gas Proxy Function, it shall send (under Clause 4.5) a 'Join Service' Service Request to add the Gas Proxy Function to the Device Log of a Commissioned Gas Smart Meter. https://smartenergycodecompany.co.uk/download/2275

	Withdrawal Procedures		
7.2.1.6.14 Remote CAD Pairing			
Other User	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	4.8 (a)	In respect of Type 2 Devices: (a) where the Responsible Supplier or an Other User wishes to add a Type 2 Device to the Device Log of an Electricity Smart Meter or a Gas Proxy Function, it shall send a 'Join Service' Service Request in order to do so; https://smartenergycodecompany.co.uk/download/2275
Other User	Smart Energy Code	Section I1.3	Each User undertakes that it will not send either a 'Join Service' or 'Unjoin Service' Service Request (respectively to join a Type 2 Device to, or unjoin it from, any Smart Meter or Device Associated with a Smart Meter) unless: (a) the User is the Responsible Supplier for the Smart Meter or Associated Device to which the Service Request is sent, and sends that Service Request for the purpose of complying with an obligation under its Energy Supply Licence; or (b) the Energy Consumer at the premises at which the Smart Meter is located has given the User Unambiguous Consent, which has not been withdrawn, to (as the case may be): (i) join that Type 2 Device to the Smart Meter or Associated Device, and the User has clearly informed the Energy Consumer before obtaining such Unambiguous Consent that a consequence of joining the Type 2 Device may be that Data relating to the Energy Consumer will be shared with third parties; or (ii) unjoin it from the Smart Meter or Associated Device, save that the Responsible Supplier for a Smart Metering System at the premises need not obtain such Unambiguous Consent where it has reasonable grounds to believe that the Type 2 Device has Compromised or is likely to Compromise any Device forming part of that Smart Metering System (and the Responsible Supplier shall, where it unjoins a Type 2 Device in such circumstances, take all reasonable steps to inform the Energy Consumer that it has done so). https://smartenergycodecompany.co.uk/download/2486

7.2.2 Install and Leave

7.2.2.1 Introduction

This process area describes how to install a SMS when the WAN is not available.

There are two types of Install and Leave depending on whether the WAN coverage is expected to be available at the site (i.e. the WAN Matrix reported that there is WAN coverage for the site):

- Reactive; the WAN is expected to be in place but is it not available during the installation. The Installer established the HAN and left the installation with the working HAN. This process description focuses on such reactive Install and Leave. While the establishment of the HAN is not an absolute requirement, Suppliers will not be able to count such installation towards their roll out obligations unless: the HAN is established; for domestic installations only, the customer has been offered an IHD and had its function explained; and energy efficiency advice has been provided in line with Smart Metering Installation Code of Practice requirements at the time of installation. As such, this document does not cover a scenario where the Installer installs Devices but leaves them without the working HAN. While this process allows for the establishment of the HAN, Meters and the GPF forming part of the SMS need to be Commissioned after the CH connects to the WAN to be Enrolled.

- Proactive; the Supplier knew there was no WAN available at the site but decided to proceed with the installation. Proactive Install and Leave is only permissible in the case of new connections, where the WAN is expected to be in place by the end of 2020, or where a meter requires replacement for safety or compliance reasons. In such cases, Suppliers are not permitted to establish the HAN until the WAN becomes available. In the former case, the establishment of the HAN will follow the process described in Section 7.2.1 of the BAD once the WAN becomes available.

The process described in this section replicates many of the steps in the standard Install and Commission process as set out in Section 7.2.1 of the BAD. The main difference is the use of a Hand Held Terminal (HHT) to simulate WAN connectivity and allow processing of Commands as if the WAN were in place.

For the process to work, the HHT must either:

- Be able to make contact with the Supplier's systems in real time; or

- Be preloaded with necessary Commands to enable installation.

A wide range of Commands may be sent using the HHT; this process focuses solely on those needed to establish the HAN. Suppliers are welcome to use additional Commands to meet their specific business needs, but it should be noted that Devices which have not been 'Commissioned' may not have valid time set, and this may constrain which Commands Suppliers may send to Devices. Also, certain Commands cannot be delivered locally (for example a Command resulting from a 'Commission Device' Service Request (SRV 8.1.1)).

7.2.2.2 Scope

This process area includes:

- Communications Hub Status Update – Install No SM WAN

- Obtain Commands for Local Delivery

- Send Commands Locally

- Local Command Response

- Establish WAN Connection

This process area involves but does not specifically describe:

- Read (non-Device) - Request WAN Matrix. This is described in Section 7.4.1.6.3 of the BAD.
- Read (non-Device) - Read Inventory. This is described in Section 7.4.1.6.3 of the BAD.
- Device Pre-notification. This is described in Section 7.1.1.6.2 of the BAD.
- Install Communications Hub. This is described in Section 7.2.1.6.4 of the BAD.
- Update Inventory - Update Device SMI Status to 'Installed not Commissioned'. This is described in Section 7.1.1.6.3 of the BAD.
- Update Inventory – Update the GPF SMI Status to 'Commissioned'. This is described in Section 7.1.1.6.3 of the BAD.
- Commission Device. This is described in Section 7.2.1.6.10 of the BAD.
- Set Device Configuration (Import MPxN). This is described in Section 7.2.1.6.11 of the BAD.

7.2.2.3 Inputs

- 'Update Security Credentials' Service Request (SRV 6.15)
- 'Request Handover of DCC Controlled Device' Service Request (SRV 6.21)
- 'Update Inventory' Service Request (SRV 8.4)
- 'Join Service (Critical)' Service Request (SRV 8.7.1)
- 'Join Service (Non-Critical)' Service Request (SRV 8.7.2)
- 'Update HAN Device Log' Service Request (SRV 8.11)
- 'Local Command Response' Service Request (SRV 8.13)
- 'Communications Hub Status Update - Install No SM WAN' Service Request (SRV 8.14.2)

7.2.2.4 Actors

- Supplier
- DCC
- CHF
- GPF
- Smart Meter
- Type 1 Device

- IHD
- Installer

7.2.2.5 Prerequisites

- See Section 7.2.1.5 of the BAD.
- The SM WAN Coverage is available at the site (but it is not available on the day).

7.2.2.6 Process Description

The installation process follows the same steps as in Sections 7.2.1.6.1 – 7.2.1.6.4. The Supplier completed the three pre-installation steps and CH installation has taken place.

The CH fails to connect to the WAN. The Supplier, in consultation with the Installer, decides whether to abort the installation or Install and Leave.

7.2.2.6.1 Communications Hub Status Update – Install No SM WAN

Within 3 Working Days of the installation, the Supplier notifies the DCC that there was no SM WAN at the premises. To do that, the Supplier composes a 'Communications Hub Status Update Install No SM WAN' Service Request (SRV 8.14.2) and sends it to the DCC. The DCC receives it and completes Non-Device Service Request processing, and does the following things:

- Sends a Service Response to the Supplier; and
- Creates an Incident and includes within the Incident details of any Network Enhancement Plan affecting the Installation Location (See Section 7.9.4of the BAD).

The DCC investigates and advises the Supplier of the steps to take to establish connection to the WAN at the premises. The steps may include the installation of a mesh CH, or special aerials.

7.2.2.6.2 Obtain Commands for Local Delivery

The Installer either uses a HHT onsite to add Devices to the CHF Device Log, join them as required, update Security Credentials if required and perform other activities. This process may have been completed prior to the installation (e.g. in a lab), using a HHT or similar Device. If that is the case, this step is not required.

The Installer provides the Supplier with Device IDs, Installation Code and other necessary information for all the Devices to be installed, and the HHT used onsite. The communication between the Supplier and Installer is via an out-of-band process.

The Supplier determines the Commands required for installation. This depends upon the specific Devices to form the SMS.

For a Device to join a HAN, each Device needs to be added to the CHF Device Log. The Supplier needs an 'Update HAN Device Log' Service Request (SRV 8.11) for each Device to be added. This Service Request is also needed to add the HHT to the CHF Device Log so the total number of

corresponding CCS01 Commands needs to be equal to the number of Devices to be added to the CHF Device Log plus one for the HHT.

The Supplier needs to ensure its Organisation Certificates are on the Devices. This applies to Smart Meters, HCALCS and GPF. Where the DCC's Organisation Certificates are populated in the Supplier's Trust Anchor Cells, the Supplier will have to replace the DCC's Organisation Certificates with their own Organisation Certificates. In this case, the Supplier uses a 'Request Handover of DCC Controlled Device' Service Request (SRV 6.21).

Where the Supplier's group Organisation Certificate is populated in the Supplier's Trust Anchor Cells, the Supplier may use an 'Update Security Credentials (KRP)' Service Request (SRV 6.15.1) to replace the Supplier's group Organisation Certificate with the Supplier's Organisation Certificate.

The total number of corresponding CS02b Commands depends on the number of Organisation Certificates to be replaced, and the number of Devices.

The Supplier needs a number of 'Join Service' (Critical) Service Requests (SRV 8.7.1) and 'Join Service' (Non-Critical) Service Requests (SRV 8.7.2) so Devices can communicate at the application level. The number of corresponding Commands depends on the set up of the SMS, as shown below.

Table 5. Commands Corresponding to Device Join

SRV	8.7.1 (Critical)	8.7.2 (Non-Critical)
Join Electricity Smart Meter to IHD		CS03B (ESME)
PPMID to Electricity Smart Meter	CS03A2 (PPMID)	
Electricity Smart Meter to PPMID	CS03A1 (ESME)	
HCALCS to Electricity Smart Meter	CS03A2 (HCALCS)	
Electricity Smart Meter to HCALCS	CS03A1 (ESME)	
Gas Smart Meter to PPMID	CS03C (GSME)	
PPMID to Gas Smart Meter	CS03C (PPMID)	
GPF to PPMID		CS03B (GPF)
Gas Smart Meter to GPF	CS03C (GSME)	
GPF to IHD		CS03B (GPF)

The Supplier may also choose to complete basic configuration of Meters. See Section 7.3.1 of the BAD.

The Supplier may wish to complete other activities. This is subject to their installation policies and business needs so this is not covered here.

The process for requesting these Service Requests for local delivery is the same as for requesting Service Requests for delivery over the WAN. The only difference is instead of sending the corresponding Commands to Devices and to the Supplier, the DCC only sends them to the Supplier.

The process is as follows: the Supplier composes the Service Request specifying that the corresponding Command is for local delivery. The DCC receives the Service Request and completes either Critical or Non-Critical Service Request processing (depending on the Service Request). The DCC returns the corresponding Command to the Supplier. The DCC does not send it to the Device.

7.2.2.6.3 Send Commands Locally

The Supplier receives the Commands and makes them available to the Installer to download to their HHT.

To send these Commands to Devices using the HHT, the Installer establishes an Inter-PAN between the HHT and the CHF. The CH opens the Inter-PAN connection for 60 minutes after powering on. The HHT detects any CHF in the range, and the Installer selects the right CHF, (either through manual data entry or scanning the CHF barcode). Both Devices complete CBKE over inter-PAN. The Installer then sends a 'Add Device to CHF Device Log' (CCS01) Command to the CHF to add the HHT to the CHF Device Log – this Command needs to be sent first. The CHF receives the Command and processes it by adding the Security Credentials of the HHT to the CHF Device Log. This process establishes the communication between the two Devices. The CHF sends a Response to the HHT.

At this point the HHT has successfully whitelisted itself in the Communications Hub Device Log, the Communications Hub will permit joining for the period identified in the HHT CCS01 command received over the inter-PAN connection. The HHT then joins the Communications Hub in the same manner as any other device, including performing CBKE, and opens a tunnel to the Communications Hub.

The Installer uses the HHT to send the remaining CCS01 Commands for each Device to be added to the CHF Device Log. The process for adding Devices is very similar to that described in Section 7.2.1.6.7 of the BAD:

- The Installer sends the CCS01 Command, to add a Device to the CHF Device Log, to the CHF;
- The CHF receives the Command, and processes it by adding the Security Credentials of the Device to the CHF Device Log;
- The CHF sends a CCS01 Response to the HHT;
- The CHF then sends a 'Device Addition to / Removal from HAN Whitelist' (CS14) (Alert Code:0x8F12) Device Alert containing the changed Device Log to the HHT;
- The CHF sets its beacon to allow the Device to join the HAN. Device detects the HAN and requests that it joins. The CHF and Device undertake CBKE;
- Once the process is complete the CHF updates its Device Log and sends a 'Device Addition To / Removal From HAN Whitelist' (CS14) (Alert Code: 0x8F12) Device Alert containing the changed Device Log to the HHT. This Alert confirms the Device has joined the HAN; and
- For Smart Meters only; if the Meter has successfully joined the HAN, the Meter may send two Device Alerts to the HHT:
    - A 'Device Commissioned' (Alert Code 0x8F69) Device Alert; and
    - A 'Device joined SMHAN' (Alert Code 0x8183) Device Alert.

If relevant, CS02b Commands supporting credential management are on the HHT, the Installer now completes the credential management for the Smart Meter, HCALCS and GPF, as required:

- The Installer sends a CS02b Command, per Organisation Certificate to be replaced, to each Device;
- The Device receives the CS02b Command, processes it by carrying out checks of the Certificate to be replaced. This process is described in Section 7.7.2.5.5 and 7.7.2.5.6 of the BAD;
- If the checks are successful, the Organisation Certificate is replaced. If the checks fail, the Organisation Certificate is not replaced; and
- The Device sends a CS02b Response to the HHT.

The Devices can now communicate at the network level, but they need to be joined ("paired") at the application level as well. The exact sequence will depend upon the Devices to be joined, and the preference of the Installer. The Installer should have a number of CS03A1, CS03A2, CS03A3 CS03B, CS03C Commands on the HHT, as determined by the Supplier. The process for joining Devices is very similar to that described in Section 7.2.1.6.12 of the BAD:

- The Installer sends each of the Commands to the relevant Device;
- The Device receives the Command, processes it by adding the Device to be joined Security Credentials to its Device Log, and effects the join between the two Devices using the mechanisms described in the GBCS. These processes are described in Section 7.2.1.6.12 of the BAD; and
- The Device sends the Response to the HHT.

If the GPF device log has been updated the GPF will send a GCS62 Alert to the HHT containing the contents of the GPF device log.

After the joining process, the Installer may send other Commands to the Devices, as required by the Supplier. However, since this step is Supplier specific, we do not cover it here.

The HHT stores all Device Alerts and Responses received from the CHF. Note: the CHF also maintains a buffer of all Device Alerts and Responses whilst the WAN is unavailable. These will be sent to the DCC when the CH connects to the WAN.

7.2.2.6.4 Return Local Command Response

Once the Installer receives all the required Responses and Device Alerts, the Installer connects the HHT to the Supplier's System to download all the Responses and Device Alerts. This communication is via an out-of-band process.

Once all the Responses and Device Alerts are downloaded to the Supplier's system, the Supplier composes a 'Return Local Command Response' Service Request (SRV 8.13) for each of the following Device Alerts and Responses and sends it to the DCC:

Responses

8.7.1 - Join Service (Critical)
8.7.2 - Join Service (Non-Critical)
8.8.1 - Unjoin Service (Critical)
8.8.2 - Unjoin Service (Non-Critical)
8.11 – Update HAN Device Log

Device Alerts
• Device Addition To / Removal From HAN Whitelist Device Alerts (Alert Code: 0x8F12) • Backup GPF Device Log Alert (GCS62)

The DCC receives the Service Request, undertakes Non-Device Service Request processing, and does the following things:

- Sends a Service Response to the Supplier; and
- Updates the SMI as follows:
    - For Smart Meters only, Associates the Smart Meter with the MPxN;
    - For all Devices, Associates each Device with the CHF and as indicated by how they are joined.

7.2.2.6.5 Update Inventory – Update Device SMI Status to 'Installed not Commissioned'

The Supplier may wish to update the SMI Status of the CHF, GPF, Meters and Type 1 Devices to 'Installed not Commissioned'. To do this the Supplier composes and sends an 'Update Inventory' Service Request (SRV 8.4) to the DCC.

This process is described in Section 7.1.1.6.3 of the BAD.

7.2.2.6.6 Establish WAN Connection

Once the CH connects to the WAN, the CH sends all the Responses and Device Alerts it has held in its buffer to the DCC. The DCC receives them and sends Service Responses and Device Alerts to the Supplier. As the CH connects to the WAN, the DCC changes the SMI Status of the CHF to 'Commissioned'. This process is described in Section 7.2.1.6.4 of the BAD.

7.2.2.6.7 Commission Device

The Supplier may now 'Commission' the Meter. To do that the Supplier composes a 'Commission Device' Service Request (SRV 8.1.1).

This process is described in detail in Section 7.2.1.6.10 of the BAD.

7.2.2.6.8 Update Inventory – Update GPF SMI Status to 'Commissioned'

For the gas SMS to be Enrolled, the Gas Smart Meter as well as the GPF must be 'Commissioned'. To 'Commission' the GPF, the Supplier composes and sends an 'Update Inventory' Service Request (SRV 8.4) to the DCC.

This process is described in more detail in Section 7.1.1.6.3 of the BAD.

7.2.2.6.9 Configure Device - Set Device Configuration (Import MPxN)

The Supplier is required to make the MPxN available on the Smart Meter's User Interface. To do so, the Supplier composes a 'Set Device Configuration (Import MPxN)' Service Request (SRV 6.20.1) and sends it to the DCC.

This process is described in more detail in Section 7.2.1.6.11 of the BAD.

The Install and Commission process is now complete. The Supplier may now carry out other activities.

7.2.2.7 Commentary

Type 1 Devices stay 'Installed not Commissioned', as there is currently no mechanism to change the SMI Status of these Devices to 'Commissioned' once the Meter is 'Commissioned'.

7.2.2.8 Associated Process Areas

#	Process Areas
7.1.1	Manage Inventory
7.2.1	Install and Commission
7.2.3	Post Commissioning Obligations
7.3.1	Configure Device
7.4.1	Read
7.7.2	Manage Security Credentials
7.9.1	Order and Return Communications Hub

7.2.2.9 Governance

Actor	SEC Document	Clause	Text
7.2.2.6.1 Communications Hub Status Update – Install No SM WAN			
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	4.8	Where, following the fitting and activation procedure, a Supplier Party wishes to leave a Communications Hub installed without establishing a connection to the SM WAN, the Supplier Party shall: (a) ensure that the power supply to the Communications Hub is capable of being maintained following fitting and activation; (b) verify that the CH Status Information does not indicate any fault other than failure to connect to the SM WAN; (c) ensure that the Communications Hub is fitted with a security seal; and

			(d) the relevant Supplier Party shall notify the DCC by submitting a Service Request 8.14.2 (Communications Hub Status Update Install No SM WAN) in accordance with the DUIS, within three (3) Working Days. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	4.9	Pursuant to 0 a Supplier Party submitting an 8.14.2 Service Request shall indicate whether each of the following conditions exists: (a) a Significant Metallic Obstruction exists at the Installation Point with respect to any of the following surfaces; (i) the front surface of the Communications Hub; (ii) the top surface of the Communications Hub; (iii) the left-side surface of the Communications Hub; or (iv) the right-side surface of the Communications Hub. (b) (without detailed or expert assessment), the Installation Point appears to have Substantial Stone Walls; or (c) the Installation Point is in a shared or communal area, outside the individual premises.
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	4.10	Following receipt of a Service Request 8.14.2 (Communications Hub Status Update Install No SM WAN), the DCC shall create an Incident and shall include within the Incident details of any Network Enhancement Plan affecting the Installation Location. https://smartenergycodecompany.co.uk/download/2336
7.2.2.6.4 Return Local Command Response			
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	2.11	Where a User receives a Response or Alert other than via the SM WAN, the User shall, where the Response or Alert is listed in the DCC User Interface Specification as one that is required to be returned to the DCC, send a 'Return Local Command Response' Service Request containing the Response or Alert to the DCC. https://smartenergycodecompany.co.uk/download/2275

7.2.3 Post Commissioning Obligations

7.2.3.1 Introduction

This process area explains obligations after Commissioning certain Devices.

For the CHF only, the key obligation is that within 7 days of Commissioning the CHF, the DCC ensures that:

- The CHF re-generates its Private Keys (Digital Signing and Key Agreement) and the Device Certificates containing the Associated new Public Keys which are stored on the CHF; and
- The DCC replaces at least one of the Organisation Certificates (KRP) which comprise the CHF's Device Security Credentials. For the purposes of this exercise, the Organisation Certificate may be replaced by the same Organisation Certificate.

For Meters and GPF; the key obligation is that within 7 days of Commissioning a Smart Meter or GPF, the Supplier shall, in relation to each such Device, ensure that:

- The Device re-generates its Private Key (Digital Signing and Key Agreement) and the Device Certificates containing the Associated new Public Keys on the Smart Meter and GPF;
- The Device Security Credentials for the Network Party are those of the Electricity Distributor or Gas Transporter; and
- For Smart Meters only, replace at least one of the Organisation Certificates (KRP) which comprise the Smart Meter's Device Security Credentials. For the purposes of this exercise, the Organisation Certificate may be replaced by the same Organisation Certificate.

7.2.3.2 Scope

The process includes

Post Commissioning Management and Reporting.

The process involves but does not specifically describe:

- Read (Device) - Retrieve Device Security Credentials (Device). This process is described in Section 7.4.1.6.2 of the BAD.
- Issue Security Credentials. This process is described in Section 7.7.2.5.7 of the BAD.
- Obtain Device Certificate. This process is described in Section 7.7.2.5.3 of the BAD.
- Update Security Credentials (Device). This process is described in Section 7.7.2.5.8 of the BAD.
- Request Handover of DCC Controlled Device – Update Network Operator Certificate. This process is described in Section 7.7.2.5.5 of the BAD.
- Update Security Credentials (KRP) – Update Network Operator Certificate. This process is described in Section 7.7.2.5.6 of the BAD.
- Update Security Credentials (KRP) – Replace Organisation Certificate. This process is described in Section 7.7.2.5.6 of the BAD.

7.2.3.3 Actors

- Supplier

- Network Operator
- DCC
- Smart Meter
- CHF
- GPF

7.2.3.4 Prerequisites

The CHF, Smart Meter and GPF have the SMI Status of 'Commissioned'.

7.2.3.5 Process Description

This section of the BAD describes the processes that Suppliers follow to replace Device Security Credentials. While this process area also applies to the DCC, the processes that the DCC follows to replace Device Security Credentials are internal to the DCC, and are not described here.

7.2.3.5.1 Read (Device) - Retrieve Device Security Credentials

A Supplier may wish to retrieve the current Device Security Credentials. To do so they use a 'Retrieve Device Security Credentials (Device)' Service Request (SRV 6.24.2).

This process is described in Section 7.4.1.6.2 of the BAD.

7.2.3.5.2 Issue Security Credentials

To comply with the obligation to ensure that the Device regenerates its Private Keys the Supplier needs to ensure that Device re-generates new Public-Private Key Pair using 'Issue Security Credentials' Service Request (SRV 6.17).

This process is described in detail in Section 7.7.2.5.7 of the BAD.

7.2.3.5.3 Obtain Device Certificate

To comply with the obligation to ensure that the Device Certificates containing the associated new Public Keys are stored on the Device, the Supplier needs to create a Device CSR and submit it to the DCC.

This process is described in detail in Section 7.7.2.5.3 of the BAD.

7.2.3.5.4 Update Security Credentials (Device)

The Supplier then needs to use 'Update Security Credentials (Device)' Service Request (SRV 6.15.2) to store the Device Certificate on the Device.

This process is described in detail in Section 7.7.2.5.8 of the BAD.

7.2.3.5.5 Update Security Credentials (KRP) or Request Handover of DCC Controlled Device – Update Network Operator Certificate

If the relevant Network Operator Certificates (Key Agreement and Digital Signing) are not on the Device (Smart Meter and GPF) at the point of 'Commissioning', to comply with the obligation to ensure that within 7 days of the Smart Meter or GPF being 'Commissioned', the Device Security Credentials for the Network Operator are those of the relevant Electricity Distributor and Gas Transporter, the Supplier sends an 'Update Security Credentials (KRP)' (SRV 6.15.1) or 'Request Handover of DCC Controlled Device' (SRV 6.21) to the DCC. Which Service Request to use depends on whose Organisation Certificate is in the Network Operator's Trust Anchor Cell.

This process is described in detail in Section 7.7.2.5.5 and 7.7.2.5.6 of the BAD.

7.2.3.5.6 Update Security Credentials (KRP) – Replace Organisation Certificate

The Supplier's final post commissioning obligation, for a Meter, is that one of the Organisation Certificates are replaced. This has the effect of validating the authenticity of Root Security Credentials on the Device. Note that an Organisation Certificate can be replaced with the same Organisation Certificate.

To do so, the Supplier composes an 'Update Device Security Credentials' Service Request (SRV 6.15.1), including an Organisation Certificate to be replaced (this could be the Digital Signing Certificate, Key Agreement Certificate or Prepayment Top Up Key Agreement Certificate) and sends it to the DCC.

This process is described in detail in Section 7.7.2.5.6 of the BAD.

7.2.3.5.7 Post Commissioning Management and Reporting

Where the Supplier has not met its Post Commissioning Obligations and the Device has not been interrogated within 14 days of Commissioning, the Supplier is not permitted to send any Service Requests destined for that Device other than for the purposes of: (i) completing the Post Commissioning steps; (ii) replacing the Device Security Credentials held on the Device in response to a change of supplier; or (iii) maintaining an energy supply to the relevant premises.

Where, the Supplier responsible for a GPF or Smart Meter becomes aware that the Smart Meter or GPF does not have a Recovery Trust Anchor Cell populated with a DCC Recovery Certificate, the Supplier is required to replace the Smart Meter or CH.

Following the removal of the CH, the Supplier notifies the DCC of its removal by sending a 'Communications Hub Status Update – Fault Return' (SRV 8.14.3) Service Request to the DCC within 5 Working Days from the removal. The Supplier indicates in the Service Request 'CH Defect' as a failure type and uses the OMS to arrange the return of the CH. This process is discussed in more details in 7.9.1.6.2 of the BAD.

Within 7 days of Commissioning of a CHF, GPF or a Meter, the DCC is required to interrogate the Device to ascertain whether the Device's Recovery Trust Anchor Cell is populated with a DCC Recovery Certificate.

The DCC keeps a daily record of Devices which are at risk of not having the Recovery Trust Anchor Cell populated with the DCC Recovery Certificate. Each month, the DCC provides a report to the Panel, Security Sub-Committee and Authority of the number of Devices at risk of not having the Recovery Trust Anchor Cell populated with the DCC Recovery Certificate.

The DCC also compiles a daily report for each Supplier (and makes it available for 30 days) of the Devices that the Supplier is responsible that are at risk of not having the Recovery Trust Anchor Cell populated with the DCC Recovery Certificate. The DCC makes this report available to the Panel and the Authority on request.

Where the DCC has not met its Post Commissioning Obligations and has not interrogated the CHF, GPF or a Smart Meter, or the DCC has successfully interrogated the CHF, GPF or a Smart Meter but identified that the Device does not have the DCC Recovery Certificate in the Recovery Trust Anchor Cell, the DCC raises an Incident.

7.2.3.6 Associated Process Areas

#	Process Areas
7.2.1	Install and Commission
7.4.1	Read
7.6.1	Replace Communications Hub
7.7.2	Manage Security Credentials
7.9.4	Manage Incidents

7.2.3.7 Governance

Actor	SEC Document	Clause	Text
7.2.3 Post Commissioning Obligations			
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.1	As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, the DCC shall ensure that: (a) the Communications Hub Function re-generates its Private Keys, and that Device Certificates containing the associated new Public Keys are stored on the Device; and (b) the information from at least one of the Organisation Certificates that comprise the Communications Hub Function's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate). https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC -	5.2	As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Smart

	Inventory Enrolment and Withdrawal Procedures		Meter or a Gas Proxy Function, the Responsible Supplier shall, in relation to each such Device, ensure that: (a) the Device Security Credentials which pertain to the Network Party are those of the Electricity Distributor or Gas Transporter (as applicable); (b) the Device re-generates its Private Keys, and that the Device Certificates containing the associated new Public Keys are stored on the Device; and (c) in the case of a Smart Meter only, information from at least one of the Organisation Certificates that comprise the Smart Meter's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate). https://smartenergycodecompany.co.uk/download/2275
7.2.3.5.7 Post Commissioning Management and Reporting			
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.3	As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, Gas Proxy Function or a Smart Meter, the DCC shall interrogate the Device to ascertain whether the Device's recovery Trust Anchor Cell is populated with Device Security Credentials that pertain to a DCC Recovery Certificate. For Devices Commissioned before Service Release 1.3 (or such later date as may be directed by the SofS for the purposes of this Clause 5.3), the reference to the period of 7 days following Commissioning shall apply as 7 days following Service Release 1.3 (or 7 days following any later date directed by the SofS). https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.4	The DCC shall monitor Commands sent to Devices and the associated Responses from Devices and, based on the information available to it, record the information set out in Clause 5.7 in relation to each Device identified in Clause 5.6 (the “Post Commissioning Information”). https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.5	The DCC shall ensure that the Post Commissioning Information is updated on a daily basis to reflect the most accurate and up-to-date information available to the DCC at the time of the update https://smartenergycodecompany.co.uk/download/2275

DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.6	For the purposes of Clause 5.4, the relevant Devices include any Communications Hub Function, Gas Proxy Function or Smart Meter which has an SMI Status of 'commissioned', has been Commissioned for a period of 7 days or more, and in relation to which one or more of the following applies: (a) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.3; (b) the DCC has successfully carried out the interrogation of the Device pursuant to Clause 5.3 and has identified that the Device's recovery Trust Anchor Cell is not populated with Device Security Credentials that pertain to a DCC Recovery Certificate; and/or (c) the Device has not sent Responses indicating that Commands associated with each of the following Service Requests have been Successfully Executed on the Device (provided that, for the purposes of this paragraph (c), where the Device sends, before Service Release 1.3 (or such later date as may be specified by the Secretary of State for the purposes of this Clause 5.6(c)), a Response to any such Command, the DCC may treat such Command as having been Successfully Executed, without further analysis of the Response): (i) at least two 'Issue Security Credentials' Service Requests; (ii) at least two 'Update Security Credentials (Device)' Services Requests; and (iii) in relation to Communications Hub Functions and Smart Meters only, at least one 'Update Security Credentials (KRP)' Service Request. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.7	For the purposes of Clause 5.4, the Post Commissioning Information to be recorded in relation to each relevant Device shall include: (a) the Device ID and Device Type; (b) the date upon which the Device was Commissioned; (c) which of Clauses 5.6 (a), (b), (c)(i), (c)(ii) and/or (c)(iii) applies; (d) other than in the case of Communications Hub Functions, the Responsible Supplier at the time the Post Commissioning Information for the Device was most recently updated; (e) other than in the case of Communications Hub Functions, the Supplier Party that sent the Service Request that resulted in the Commissioning of the Device; and (f) the date on which the Post Commissioning Information for the Device was most recently updated.

			https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.8	As soon as reasonable practicable following the end of each month, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that month, compile and provide (in an electronic format) to the Panel, the Security Sub-Committee and the Authority a report which includes the following information: (a) the month to which the report relates; (b) for each Party that is the Responsible Supplier for any Smart Meter or Gas Proxy Function that is listed in the Post Commissioning Information for that month (or was listed in the information for the previous month): (i) the total number of Devices of each Device Type listed in the Post Commissioning Information for that month for which that Party is the Responsible Supplier; (ii) the number of such Devices of each Device Type that have been added since the last monthly report; (iii) the number of such Devices of each Device Type that have been removed since the last monthly report; (iv) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates; (v) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and (vi) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates; and (c) in respect of Communications Hub Functions: (i) the total number of Communications Hub Functions listed in the Post Commissioning Information; (ii) the number of Communications Hub Functions that have been added since the last monthly report; (iii) the number of Communications Hub Functions that have been removed since the last monthly report; (iv) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates; (v) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and

			(vi) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.9	As soon as reasonable practicable following the end of each day, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that day, compile and make available to each Supplier Party (via a secure electronic means for a period of at least 30 days following the day to which the report relates) a report which includes the following information in relation to Devices (other than Communications Hub Functions) listed in the Post Commissioning Information for which that Supplier Party was the Responsible Supplier on that day: (a) the Device ID and Device Type of each such Device; (b) the date on which the Post Commissioning Information for each such Device was most recently updated; (c) the date upon which each such Device was Commissioned; and (d) which of Clause 5.6 (a), (b), (c)(i), (c)(ii) and/or (c)(iii) applies in relation to each such Device. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.10	Where requested by the Panel or the Authority, the DCC shall, as soon as reasonably practicable following any such request, provide to the Panel and/or the Authority (in an electronic format) copies of the reports referred to in Clause 5.9. Where requested by the Panel or the Authority, DCC shall additionally include in any such report the information referred to in Clause 5.7(e) in relation to each Device included in any such report. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.11	The DCC shall ensure that each report provided under Clause 5.8, 5.9 or 5.10 is clearly marked as being "confidential". https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC -	5.12	Where the DCC is aware that: (a) either or both of the steps in Clauses 5.1 (a) and/or (b) have not been carried out within 7 days following

	Inventory Enrolment and Withdrawal Procedures		the Commissioning of a Communications Hub Function; and/or (b) either of Clause 5.6(a) or (b) applies in relation to a Communications Hub Function, then the DCC shall raise an Incident in accordance with the Incident Management Policy https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.13	Where, in relation to a Gas Proxy Function or a Smart Meter, a Supplier Party is aware that: (a) either or both of the steps in Clauses 5.2 (b) and/or (in the case of Smart Meters only) 5.2(c) have not been carried out within 7 days following the Commissioning of the Device; and/or (b) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.3, and the Supplier has (within a period of 14 days following the Commissioning of the Device) also failed to successfully carry out the relevant interrogation, then the Supplier Party shall not send Service Requests requesting that the DCC sends communications to that Device other than for the purposes of: (i) completing those steps; (ii) replacing the Device Security Credentials held on the Device in response to a change of supplier; or (iii) maintaining an energy supply to the relevant premises. https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.14	Where, the Responsible Supplier for a Gas Proxy Function or Smart Meter becomes aware that a Smart Meter or a Gas Proxy Function does not have a recovery Trust Anchor Cell that is populated with Device Security Credentials that pertain to a DCC Recovery Certificate, then that Responsible Supplier shall (subject to Clause 5.16), as soon as reasonably practicable thereafter: in the case of a Smart Meter, replace the Device; or, in the case of a Gas Proxy Function, replace the Communications Hub of which that Gas Proxy Function forms part. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and	5.15	Where a Communications Hub is returned to the DCC: (a) following its replacement pursuant to Clause 5.12 or 5.14; or (b) a Communications Hub is returned following replacement because it was not possible to interrogate the Gas Proxy Function pursuant to Clause 5.13(b),

	Withdrawal Procedures		then the Supplier Party returning the Communications Hub may (under and subject to Section F9 (Categories of Communications Hub Responsibility)) specify the reason for return as being a CH Defect. https://smartenergycodecompany.co.uk/download/2275
Supplier	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	5.16	A Responsible Supplier shall not replace a Smart Meter or Communications Hub under Clause 5.14 where the reason that the relevant steps cannot be completed is an inability to communicate with a Device as a result of the SM WAN being unavailable. https://smartenergycodecompany.co.uk/download/2275

7.3 Configure Device and Payment Mode

Suppliers, Export Suppliers and Network Operators can configure Meters to support own business processes. For example, Suppliers are expected to configure Meters to enable the Energy Consumer to have access to their current tariff information.

This section covers two process areas:

- Configure Device- describes who can and how to configure a Smart Meter operating in Credit Mode.
- Prepayment – describes how Suppliers can configure and operate a Smart Meter in Prepayment Mode. This includes: setting payment mode to Prepayment, and configuring and operating a Smart Meter in Prepayment Mode.

7.3.1 Configure Device

7.3.1.1 Introduction

This process area describes how Suppliers, Export Suppliers and Electricity Distributors configure Smart Meters operating in Credit Mode via the DCC.

Smart Meters are configured at manufacture, and it is expected that if Suppliers are approached by Network Operators to place certain configuration settings on Smart Meters before they are Commissioned, Suppliers procuring Meters will take steps to ensure that the Smart Meters are so configured. For Electricity Distributor recommended configuration see Section 7.2.1.5 of the BAD.

Configuration is not a SEC defined term, but in this context, means providing settings to the Smart Meter which then control:

- Tariffs;
- Billing;

- Alert management;
- Supply management; and
- Energy Consumer experience.

Meters can use either Time of Use (TOU) pricing, or TOU with Block Pricing. TOU pricing is used when the Energy Consumer is paying for energy on a Price-per-kWh basis. Block Pricing allows for more complex pricing, where the price varies according to time of day, and / or quantity of energy consumed.

The SMETS describes in detail how the Smart Meter uses the Data to determine the Active Tariff Price, but from a configuration perspective, the Supplier would need to set the following:

- Tariff TOU Register Matrix (a matrix for storing Tariff Registers for TOU Pricing);
- Tariff Switching Table (a set of up to 200 rules for allocating consumption to a Tariff register);
- Tariff TOU Price Matrix (a matrix containing prices for TOU Pricing);
- Tariff Threshold Matrix (a matrix capable of holding thresholds in kWh for controlling Block Pricing);
- Tariff Block Price matrix (a matrix containing prices for Block Pricing); and
- Tariff Block Counter Matrix (a matrix for storing Block Counters for Block Pricing).

Configuration is most commonly used:

- Once a Meter has been Enrolled;
- After a change of tenancy, or CoS; and
- To implement changes to tariffs or other conditions between an Energy Customer and Supplier.

7.3.1.2 Scope

This process area includes Configure Device.

This process area involves but does not specifically describe:

- Update Payment Mode. This is described in Section 7.3.2.5.1 of the BAD.
- Update Device Configuration (Billing Calendar). This is described in Section 7.4.1.6.1 of the BAD.

This process area excludes any configuration at manufacture.

7.3.1.3 Inputs

- See Table 6 and 7 below

7.3.1.4 Actors

- Supplier
- Export Supplier
- Electricity Distributor
- DCC
- Smart Meter

7.3.1.5 Prerequisites

- SMS has been Enrolled
- Electricity Distributor has received a 'Security Credentials updated on the device' (N42) DCC Alert in relation to the Smart Meter to be configured

7.3.1.6 Process Description

7.3.1.6.1 Update Payment Mode

Smart Meters are configured at manufacture to operate in either Credit or Prepayment Mode. Payment mode can subsequently be changed from credit to prepayment and vice versa. To set payment mode, a Supplier composes an 'Update Payment Mode' Service Request (SRV 1.6) and sends it to the DCC. The process is described in more detail in Section 7.3.2.5.1 of the BAD.

7.3.1.6.2 Update Device Configuration (Billing Calendar)

Suppliers can configure the automated retrieval of billing Data by configuring a Billing Calendar. To configure the Billing Calendar, a Supplier composes an 'Update Device Configuration (Billing Calendar)' Service Request (SRV 6.8) and sends it to the DCC.

This process is described in more detail in Section 7.4.1.6.1 of the BAD.

7.3.1.6.3 Configure Device

The below tables list critical and non-critical configuration Service Requests. It also describes who is eligible to send each of the Service Requests, and how the Device can be configured.

The process for sending these Service Requests includes the relevant User composing the Service Request and sending it to the DCC. The DCC undertakes Critical / Non-Critical Service Request processing, and sending a Command to the Device. The Device receives the Command, executes it and sends a Response. The DCC receives the Response and sends a Service Response to the relevant User.

Table 6. Non-Critical Configuration Service Requests

SRV	Name	When and how used?	Actors	Device	Command
6.12	UpdateDeviceConfiguration(InstantaneousPowerThreshold)	This SRV allows the Import Supplier to set the Low / Medium and Medium / High power thresholds on the Electricity Smart Meter such that High, Medium or Low ambient energy usage is displayed via the IHD accordingly	Import Supplier	Electricity Smart Meter	ECS34
6.18.1	SetMaximumDemandConfigurableTimePeri	This SRV allows the Electricity Distributor to set the Maximum Demand Configurable Time Period on the Electricity Smart Meter. Once this has been set to a new value, the Electricity Distributor may reset the Maximum Demand registers (via Use Case ECS57 (Reset Maximum Demand Registers)).	Electricity Distributor	Electricity Smart Meter	ECS37
6.18.2	ResetMaximumDemandRegisters	This SRV allows the Electricity Distributor to reset the Maximum Demand Registers on the Electricity Smart Meter	Electricity Distributor	Electricity Smart Meter	ECS57
6.20.1	SetDeviceConfiguration(ImportMPxN)	This SRV allows the Import Supplier to set the Import MPAN value for display on the Electricity Smart Meter, and MPRN for Gas Smart Meter	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter	ECS39a GCS41
6.20.2	SetDeviceConfiguration(ImportMPxN)	This SRV allows the Export Supplier to set the Export MPAN value for display on the Electricity Smart Meter	Export Supplier	Electricity Smart Meter	ECS39b
6.22	ConfigureAlertBehaviour	This SRV allows Import Supplier or the Electricity Distributor to enable or disable each Meter Alert	Import Supplier, Gas Supplier, Electricity Distributor	Electricity Smart Meter Gas Smart Meter	ECS25a ECS25b GCS20

6.22	ConfigureAlertBehaviour	This SRV allows the Import Supplier or the Gas Supplier to enable or disable HAN Alerts and Audible Alarms	Import Supplier, Gas Supplier	GBCS v1.0 GBCS v1.1 Gas Smart Meter GBCS v2.0 Electricity Smart Meter	**GBCS v1.0** **GBCS v1.1** GCS20 **GBCS v2.0** ECS25a1 ECS25a2
6.22	ConfigureAlertBehaviour	This SRV allows the Import Supplier or the Gas Supplier or the Electricity Distributor to enable or disable logging events	Import Supplier, Gas Supplier, Electricity Distributor	GBCS v1.0 GBCS v1.1 Gas Smart Meter GBCS v2.0 Electricity Smart Meter	**GBCS v1.0** **GBCSv1.1** GCS20 **GBCS v2.0** ECS25a3 ECS25b3
6.27	UpdateDeviceConfiguration(RMSVoltageCounterReset)	This SRV allows the Electricity Distributor to reset the over- and under voltage counters on an Electricity Smart Meter and 3-phase Electricity Smart Meter	Electricity Distributor	Electricity Smart Meter	**GBCS v2.0** ECS29e ECS29f
6.28	SetCHFSubGHzConfiguration	This SRV allows the import Supplier or Gas Supplier to configure the DB CHF Sub-GHz Parameters	Import Supplier (IS) Gas Supplier (GS)	CHF – Dual Band Only	**GBCS v2.0** DBCH04
6.4.2	UpdateDeviceConfiguration(LoadLimitingCounterReset)	This SRV allows the Import Supplier to set the Load Limit Counter (to zero) on the Electricity Smart Meter.	Import Supplier	Electricity Smart Meter	ECS28b
6.5	UpdateDeviceConfiguration(Voltage)	This SRV allows the Electricity Distributor to configure the voltage thresholds and reset the counters on an Electricity Smart Meter and 3-phase Electricity Smart Meter	Electricity Distributor	Electricity Smart Meter	**GBCS v1.0** **GBCS v1.1** ECS29a ECS29b **GBCS v2.0** ECS29c ECS29d

Table 7. Critical configuration Service Requests

SRV	Name	When and how used?	Actors	Device	Command
1.1.1	UpdateImportTariff(PrimaryElement)	This SRV allows the Import Supplier or Gas Supplier to set the Tariff	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter	ECS01a GCS01a
1.1.2	UpdateImportTariff(SecondaryElement)	This SRV allows the Import Supplier to set the Tariff on the second element of twin element Meters	Import Supplier	Electricity Smart Meter	ECS01c
1.2.1	UpdatePriceTariff(PrimaryElement)	This SRV allows the Import Supplier or Gas Supplier to i set the price on single element Devices or on twin element Devices setting the Tariff for the primary element.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter	ECS01b GCS01b
1.2.2	UpdatePriceSecondaryElement	This SRV allows the Import Supplier to set the Price on the Second element of twin element Devices	Import Supplier	Electricity Smart Meter	ECS01d
1.7	ResetTariffBlockCounterMatrix	This SRV allows the Import Supplier to reset the Energy Consumer's BlockConsumption back to zero, such that their consumption will go back to being charged at the first block rate.	Import Supplier	Electricity Smart Meter	ECS05
6.25	SetElectricitySupplyTamperState	This SRV allows the Import Supplier to set the Electricity Smart Meter to respond to a tamper event by stopping Supply (or not).	Import Supplier	Electricity Smart Meter	ECS81
6.4.1	UpdateDeviceConfiguration(LoadLimitingGeneralSettings)	This SRV allows the Import Supplier to set the Load Limit general configurations on the Electricity Smart Meter.	Import Supplier	Electricity Smart Meter	ECS28a
6.6	UpdateDeviceConfiguration(GasConversion)	This SRV allows the Gas Supplier to set the Calorific Value and Conversion Factor on a Gas Smart Meter.	Gas Supplier	Gas Smart Meter	GCS23

SRV	Name	When and how used?	Actors	Device	Command
6.7	UpdateDeviceConfiguration(GasFlow)	This SRV allows the Gas Supplier to set a number of configurable items, including response to tamper.	Gas Supplier	Gas Smart Meter	GCS24
6.8	UpdateDeviceConfiguration(BillingCalendar)	This SRV allows the Import Supplier or Gas Supplier to set / configure the Billing Calendar. In addition, the Use Case covers the setting up of the billing period push object(s) to allow the billing Data Log to be sent as a periodic Alert from the Smart Meter to the Supplier.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter	**GBCS v1.0** **GBCS V1.1** ECS30 GCS25 **GBCSv2.0** ECS30a GCS25a
6.26	Update Device Configuration (Daily resetting of Tariff Block Counter Matrix)	This SRV enables daily resetting of the Tariff Block Counter Matrix.	Import Supplier	Electricity Smart Meter	**GBCSv2.0** ECS48
7.12	SetRandomisedOffsetLimit	This SRV allows the Import Supplier to set the Randomised Offset Limit on the Electricity Smart Meter[15].	Import Supplier	Electricity Smart Meter	ECS38

7.3.1.7 Associated Process Areas

#	Process Areas
7.3.2	Prepayment
7.4.1	Read
7.8.4	Service Request Processing

7.3.1.8 Governance

Actor	SEC Document	Clause	Text
7.3.1.6.3 Configure Device			
Supplier	SEC Appendix AC - Inventory Enrolment	3.3	Where and to the extent that the Electricity Distributor or Gas Transporter for a Device has notified the Responsible Supplier for the Device of the values for the 'NP Configurable Data Items' that the Electricity Distributor or Gas Transporter (as applicable) wishes to

[15]The Distribution Connection and Use of System Agreement (DCUSA) requires Suppliers to set the Randomised Offset Limit with a minimum value of 600 seconds.

	and Withdrawal Procedures		have configured on the Device at the time of its Commissioning, the Responsible Supplier shall take all reasonable steps to ensure that those data items are so configured on the Device at the time of its Commissioning. In this Clause 3.3, 'NP Configurable Data Items' means those data items held on Devices that are capable of being configured via Services Requests for which the User Role of 'Electricity Distributors' or 'Gas Transporter' (as applicable) is an Eligible User Role. https://smartenergycodecompany.co.uk/download/2275

7.3.2 Prepayment

7.3.2.1 Introduction

This process area describes how Suppliers can configure and operate a Smart Meter in Prepayment Mode. It also covers the process for updating Payment Mode on Smart Meters.

7.3.2.2 Scope

This process area includes:

- Update Payment Mode
- Update Prepay Configuration
- Prepayment Alerts
- Activate Emergency Credit
- Top Up Device
- Update Debt
- Update Meter Balance

This process area involves but does not specifically describe Read (Device) - Read Payment Mode and Read Prepayment Configuration. This is described in Section 7.4.1.6.2 of the BAD.

This process area excludes:

- The processes for Energy Consumers to purchase top ups; and
- The Suppliers own credit and debt management processes.

7.3.2.3 Inputs

- 'Update Meter Balance' Service Request (SRV 1.5)

- ‘Update Payment Mode’ Service Request (SRV 1.6)
- ‘Update Prepay Configuration’ Service Request (SRV 2.1)
- ‘Top up Device’ Service Request (SRV 2.2)
- ‘Update Debt’ Service Request (SRV 2.3)
- ‘Activate Emergency Credit’ Service Request (SRV 2.5)

7.3.2.4 Actors

- Supplier
- Energy Consumer
- DCC
- Smart Meter
- PPMID

7.3.2.5 Process Description

7.3.2.5.1 Update Payment Mode

To update Payment Mode, the Supplier composes an ‘Update Payment Mode’ Service Request (SRV 1.6) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends an ‘Set Payment Mode to Prepayment’ (ECS03) Command to the Electricity Smart Meter or a ‘Set Payment Mode to Prepayment’ (GCS03) Command to the Gas Smart Meter.

The Smart Meter receives the Command, executes it by setting the mode to Prepayment, and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 1.6) to the Supplier.

To return the meter to credit mode the Supplier composes and an ‘Update Payment Mode’ Service Request (SRV 1.6) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends an ‘Set Payment Mode to Credit’ (ECS02) Command to the Electricity Smart Meter or a ‘Set Payment Mode to Credit’ (GCS02) Command to the Gas Smart Meter.

The Smart Meter receives the Command, executes it by setting the mode to Credit and sends a Response to the DCC.

7.3.2.5.2 Update Prepay Configuration

To configure a Meter in Prepayment Mode, the Supplier composes an ‘Update Prepay Configuration’ Service Request (SRV 2.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing, and sends an 'Update Prepayment Configuration' (GBCS v1.0/GBCSv1.1): ECS08; GBCS v2.0: ECS08a) Command to the Electricity Smart Meter or a 'Update Prepayment Configuration' (GCS05) Command to the Gas Smart Meter.

The Meter receives the Command, executes it by configuring the Smart Meter as specified in the Service Request. The Prepayment configuration includes:

- Setting the DebtRecoveryRateCap (maximum amount to be recovered per unit time)
- Setting the EmergencyCreditLimit (amount of Emergency Credit to be available when Emergency Credit is activated)
- Setting the EmergencyCreditThreshold (thresholds beyond which Emergency Credit can be activated)
- Setting the LowCreditThreshold (threshold that activates low credit Device Alert)
- Setting the NonDisablementCalendar (time when electricity supply will not be disabled)
- Setting the MaximumMeterBalance (threshold above which credit cannot be added)
- Setting the MaximumCreditThreshold (maximum credit that can be added)

The Smart Meter sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 2.1) to the Supplier.

7.3.2.5.3 Prepayment Alerts

Prepayment allows Energy Consumers to pay for energy on demand, rather than in arrears. The Smart Meter maintains a balance of credit available for consumption. This balance is determined by previous payments, the rate of energy consumption and the Tariff, plus any Time-Based Debt Recovery, Payment Based Debt Recovery or Standing Charges.

The Smart Meter monitors the current balance, which is the combined credit of the Meter Balance and Emergency Credit.

If the balance goes below the Low Credit Threshold, the Smart Meter:

- Notifies the Energy Consumer through its User Interface or the PPMID; and
- Sends a 'Credit Below Low Credit Limit' (Alert Code: 0x810D) Device Alert to the DCC, which the DCC forwards to the Supplier.

The Energy Consumer may then 'top up' the Meter Balance. If no action is taken by the Energy Consumer, the Smart Meter balance will drop below the Emergency Credit Threshold. The Meter notifies the Energy Consumer through its User Interface or the PPMID of that fact and displays the availability of the Emergency Credit. This scenario assumes that Emergency Credit is available and is activated.

If the combined credit of the Smart **Error! Reference source not found.** and **Error! Reference source not found.** falls below the **Error! Reference source not found.**, the Smart Meter:

- Disables the supply;
- Displays an Alert to that effect on its User Interface; and
- Sends a 'Credit Below Disablement Threshold' (Alert Code: 0x8F0F) Device Alert to the DCC, which the DCC forwards to the Supplier.

In periods defined by the Non-Disablement Calendar and any Special Days the Smart Meter suspends the disabling of the supply and

- Displays an Alert to that effect on its User Interface; and
- Sends a 'Disablement of Supply due to insufficient credit has been suspended' (Alert Code: 0x8F83) to the DCC, which the DCC forwards to the Supplier.

7.3.2.5.4 Activate Emergency Credit

If available, Emergency Credit is typically activated via the User Interface on the Smart Meter, or the PPMID. Upon the activation of the Emergency Credit by the Energy Consumer, the Smart Meter sends an 'Emergency Credit Available' (Alert Code: 0x8119) Device Alert to the DCC, which the DCC forwards to the Supplier.

However, the Energy Consumer may ask the Supplier to activate the Emergency Credit. The Energy Consumer contacts the Supplier.

To activate the Emergency Credit, the Supplier composes an 'Activate Emergency Credit' Service Request (SRV 2.5) and sends it to the DCC. The DCC receives the Service Request, completes Critical Service Request processing, and sends an 'Activate Emergency Credit Remotely' (ECS09) Command to the Electricity Smart Meter or an 'Activate Emergency Credit Remotely' (GCS06) Command to the Gas Smart Meter.

The Smart Meter receives the Command, executes it by activating Emergency Credit, and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 2.5) to the Supplier.

7.3.2.5.5 Top Up Device

The Energy Consumer makes a top-up purchase (through a retail outlet or via the Supplier's online facility). The Supplier generates a Unique Transaction Reference Number (UTRN) which is a 20-digit numeric cryptographic expression of the top-up. The UTRN is provided to the Energy Consumer at the point of sale. The Smart Meter can have the UTRN applied in three ways:

- By the Supplier sending a Service Request
- By the Energy Consumer via the Smart Meter
- By the Energy Consumer via the PPMID

By the Supplier sending a Service Request

The Supplier composes a 'Top Up Device' Service Request (SRV 2.2) containing the UTRN, and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing, and sends an 'Apply Prepayment Top Up' (CS01a) Command to the Electricity Smart Meter or an 'Apply Prepayment Top Up' (CS01b) Command to the Gas Smart Meter.

The Smart Meter receives the Command and executes it. In addition to the normal checks that the Smart Meter applies to Commands, the Smart Meter also:

- Verifies against the maximum credit values;
- Verifies the Originator Counter (as a protection against replay attacks – so a previously used UTRN cannot be re-used); and
- Validates the PTUT (Prepayment Top Up Token) Supplier MAC (Message Authentication Code) (i.e. that the Command is from the Supplier who has purported to send it).

If the checks are successful, the Smart Meter increases the Meter Balance by the value determined by the UTRN. If the checks fail, the Smart Meter does not increase the Meter Balance.

The Smart Meter sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 2.2) to the Supplier.

By the Energy Consumer via the Meter

The Energy Consumer inputs the UTRN through the Meter's User Interface.

The Smart Meter receives and executes this Command. In addition to the normal checks that the Meter applies to Commands, the Smart Meter also:

- Verifies the UTRN Check Digit;
- Uses the PPTD (Prepayment Token Decimal) to calculate the PTUT;
- Verifies the PTUT subclass category;
- Verifies against the maximum credit values;
- Derives the Originator Counter;
- Verifies the Originator Counter;
- Derives the Message Identifier; and
- Validates the PTUT Supplier MAC.

If the checks are successful, the Smart Meter:

- Increases the Meter Balance by the value determined by the UTRN and sends a CS01a / CS01b Response to the DCC. The DCC creates a DCC Alert containing the Response and sends it to the Supplier; and

- Sends a 'Credit Added Locally' (Alert Code: 0x810E) Device Alert to the DCC, containing the UTC date and time of the last update, which the DCC forwards to the Supplier.

If any of the checks fails, the Smart Meter does not increase the balance and sends a CS01a / CS01b Response to the DCC. The DCC creates a DCC Alert containing the Response and sends it to the Supplier.

By the Energy Consumer via the PPMID

The Energy Consumer inputs the UTRN through the PPMID's User Interface. (Where the PPMID is added to the Smart Meter's Device Log, the PPMID offers the Energy Consumer the choice to top up via the PPMID.) The PPMID may verify the UTRN Check Digit. It then composes and sends a Command to the Smart Meter:

- For a Gas Smart Meter, the PPMID constructs the Command according to the requirements of Use Case PCS01.

- For an Electricity Smart Meter, the PPMID constructs a ZSE Consumer Top Up Command.

The Smart Meter receives the Command from the PPMID and validates that it has the PPMID in its Device Log. If these checks fail, no further processing takes place. If successful, the Smart Meter applies a series of checks:

- The Electricity Smart Meter uses ZSE Cryptographic Processes to authenticate the Command.

- The Gas Smart Meter uses Command Authenticity and Integrity Verification to authenticate the Command.

The Smart Meter then carries out the additional processing described in the Consumer input of UTRN via the Smart Meter process.

If the checks are successful, the Smart Meter increases the Meter Balance by the value determined by the UTRN, and:

- Sends a CS01a (Electricity Smart Meter) / CS01b (Gas Smart Meter) Response to the DCC. The DCC creates a DCC Alert containing the Response and sends it to the Supplier.

- Sends a 'Credit Added Locally' (Alert Code: 0x810E) Device Alert to the DCC, containing the UTC date and time of the last update, which the DCC forwards to the Supplier.

If any of the checks fails, the Meter does not increase the balance, and sends a CS01a (Electricity Smart Meter) / CS01b (Gas Smart Meter) Response to the DCC. The DCC creates a DCC Alert containing the Response and sends it to the Supplier.

The Smart Meter will also have a Maximum Meter Balance and Maximum Credit Threshold set; top-ups which are greater than the Maximum Credit Threshold, or which would cause the Meter to exceed its Maximum Meter Balance Threshold will be rejected.

7.3.2.5.6 Update Debt

Where debt exists, it can be recovered through top-ups made. To set a means of debt recovery, the Supplier creates an 'Update Debt' Service Request (SRV 2.3) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends a 'Debt Management' (ECS07) Command to the Electricity Smart Meter or a 'Debt Management' (GCS04) Command to the Gas Smart Meter.

The Smart Meter receives the Command and executes it (as specified in the Service Request) by:

- Setting the TimeDebtRegisters (Register 1 and Register 2);
- Setting the PaymentDebtRegister;
- Setting the DebtRecoveryPerPayment;
- Setting the ElecDebtRecovery (Register 1 & Register 2); or
- Setting the GasDebtRecovery (Register 1 & Register 2).

The Smart Meter sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 2.3) to the Supplier.

7.3.2.5.7 Update Meter Balance

The Supplier may decide to increase or decrease the Meter Balance directly. To do that the Supplier composes an 'Update Meter Balance' Service Request (SRV 1.5) and sends it to the DCC. The DCC receives the Service Request, completes Critical Service Request processing, and sends an 'Adjust Meter Balance' (ECS04a) Command to the Electricity Smart Meter or an 'Adjust Prepayment Mode Meter Balance' (GCS40a) Command to the Gas Smart Meter when in prepayment mode, or GCS40c 'Adjust Credit Mode Meter Balance' if in credit mode.

The Smart Meter receives the Command, executes it by updating the Meter Balance, and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 1.5) to the Supplier.

The supplier may wish to reset the Meter balance, to achieve this they would composes an 'Update Meter Balance' Service Request (SRV 1.5) and send it to the DCC. The DCC sends a 'Reset Meter Balance' (ECS04b) Command to the Electricity Smart Meter or an 'Reset Prepayment Mode Meter Balance' (GCS40b) Command to the Gas Smart Meter when in prepayment mode, or GCS40d if the GSME is in credit mode.

The Smart Meter receives the Command, executes it by updating the Meter Balance, and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 1.5) to the Supplier.

7.3.2.5.8 Read (Device) - Read Payment Mode and Read Prepayment Configuration Data

The Supplier may read Prepayment Configuration Data and Payment Mode. To do that the Supplier composes a relevant Service Request and sends it to the DCC. The process as well as the available Service Requests are described in Section 7.4.1.6.2 of the BAD.

7.3.2.6 Associated Process Areas

#	Process Areas
7.3.1	Configure Device
7.4.1	Read
7.5.4	Manage Supply

7.4 Read

7.4.1 Read

7.4.1.1 Introduction

This functional area describes how Users can read information held on Smart Meters as well as certain information held by the DCC. This includes:

- When and how such Service Requests are used;
- Who can use them;
- What pre-conditions or validation apply; and
- Whether the Response contains sensitive Data.

The Service Requests either read or retrieve Data and cover the ability to read the following:

- Consumption Data - this includes reading anything related to Consumption (e.g. Instantaneous Import Registers, Active / Reactive Profile Data):)
  - 'Block Register' refers to a Tariff Register for recording Consumption for the purposes of combined TOU and Block Pricing.
  - 'Block Counters' refer to the Storage for recording Consumption for the purposes of combined TOU and Block Pricing.
- Export Registers Data - this includes Export values and maximum demands;
- Prepayment Data - this includes the reading of registers, the daily read log and configuration Data;
- Maximum Demand Import / Export Registers;
- Voltage Data;

- Operational Data;
- Tariff configuration and any billing related Data; and
- Any other Device related 'read' Data e.g. Device Log, Event/Security Log, Firmware Version and Supply Status.

Some read Service Requests will return data which the Information Commissioner may consider to be 'personal'; for example, Data relating to levels of debt, or consumption. The Devices must Encrypt such information, which means there will be an additional processing step by Users when they receive such Service Response.

7.4.1.2 Scope

This process area includes:

- Update Device Configuration (Billing Calendar)
- Read (Device)
- Read (Non-Device)

7.4.1.3 Inputs

- 'Update Device Configuration (Billing Calendar)' Service Request (SRV 6.8)
- See the Read (Device) and Read (non-Device) Service Request tables below

7.4.1.4 Actors

- Supplier
- Export Supplier
- Network Operator
- Registered Supplier Agent
- Other User
- DCC
- CH
- Smart Meter
- Type 1 Device
- IHD

7.4.1.5 Prerequisites

Other Users wishing to request information that is considered 'personal', have obtained their Key Agreement Organisation Certificates by submitting an Organisation Certificate Signing Request. For more detail, see Section 7.7.2.5.2 of the BAD.

7.4.1.6 Process Description

7.4.1.6.1 Update Device Configuration (Billing Calendar)

Billing Calendars allow Suppliers to automate the retrieval of billing Data by setting the billing period start date / time and a specified frequency (either daily / weekly / monthly in GBCS v1.0/GBCS v1.1 or daily / weekly / monthly / quarterly / six monthly / yearly in GBCS v2.0) with which the billing data log is to be received.

The process for setting up and operating Billing Calendars is described here, as this is likely to be a frequently used method for obtaining billing data.

To create a Billing Calendar, the Supplier composes an 'Update Device Configuration (Billing Calendar)' Service Request (SRV 6.8) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends a 'Set Billing Calendar on the Electricity Smart Meter' (ECS30 for GBCS v1.0/GBCS v1.1, and ECS30a for GBCS v2.0) Command to the Electricity Smart Meter or a 'Set Billing Calendar on the Gas Smart Meter' (GCS25 for GBCS v1.0/GBCS v1.1 and GCS25a for GBCS v2.0) Command to the Gas Smart Meter.

The Smart Meter receives the Command, executes it by creating the Billing Calendar, and sends a Response. The DCC receives the Response and sends a Service Response (SRV 6.8) to the Supplier.

At the time specified in the Billing Calendar, the Meter or GPF takes snapshots of the Billing Data Log. The following information is included in the Device Alert for either Credit or Prepayment Mode:

- The Tariff TOU Register Matrix
- The Tariff Block Counter Register Matrix
- The Consumption Register

When in Prepayment Mode, the following information is included in the Device Alert:

- The Meter Balance
- The Emergency Credit Balance
- The Payment Debt Register
- The Time Debt Registers
- The Accumulated Debt Register

The Meter or GPF sends a 'Billing Log Updated' (Alert Code: 0x8F0A) Device Alert to the DCC. The DCC forwards the Device Alert to the Supplier.

At any time, the Supplier or Registered Supplier Agent can check the current Billing Calendar using a 'Read Device Configuration (Billing Calendar)' Service Request (SRV 6.2.3).

The Supplier can choose to retrieve the Billing Data Log from the Meter or GPF using one of the Service Requests "Retrieve Billing Calendar Data Log" (SRV 4.4.2, 4.4.3, 4.4.4, 4.4.5) as described in section 7.4.1.6.2.

In Meters designed to be compliant with GBCSv1.0/GBCSv1.1 the resetting of the Tariff Block Counter Matrix is aligned with the Billing Calendar periodicity. GBCS v2.0 allows the Tariff Block Counter Matrix to be reset daily, independently of the Billing Calendar. A supplier can enable this functionality using the "Update Device Configuration (daily resetting of the Tariff Block Counter Matrix)" Service request (SR 6.26)

7.4.1.6.2 Read (Device)

To read an attribute of a Device, the User composes a Service Request and sends it to the DCC. Where the Service Response is sensitive, to construct a valid Service Request, an Other User is required to include its Key Agreement Organisation Certificate in the Service Request. Suppliers and Network Operators are not required to do so as their Key Agreement Organisation Certificates are on Devices that they can read. That specific Key Agreement Organisation Certificate (whether provided in the Service Request or in the Supplier's Trust Anchor Cell on the Device) will be used by the Device to Encrypt the Response before sending it to the User.

The list of Read (Device) Service Requests is below. Those with sensitive Responses are in bold.

Table 8. Read (Device) Service Request

SRV	Name (Bold = sensitive Data)	When and how used?	Actors	Target Device	Command
4.1.1	Read Instantaneous Import Registers	This SRV is for reading the Electricity Smart Meter Import Registers / Gas Smart Meter Consumption Registers.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	Electricity Smart Meter Gas Smart Meter GPF	ECS17b GCS13a
4.1.2	Read Instantaneous Import TOU Matrices	This SRV is for reading the Electricity Smart Meter Import / Gas Smart Meter TOU Register Matrix.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	Electricity Smart Meter Gas Smart Meter GPF	ECS17d GCS13c
4.1.3	Read Instantaneous Import TOU With Blocks Matrices	This SRV is for reading the Electricity Smart Meter Import TOU with Block Register Matrix.	Import Supplier, Electricity Distributor	Electricity Smart Meter	ECS17e

4.1.4	Read Instantaneous Import Block Counters	This SRV is for reading the Gas Smart Meter Block Counters.	Gas Supplier	Gas Smart Meter GPF	GCS13b
4.2	Read Instantaneous Export Registers	This SRV is for reading Electricity Smart Meter Export Registers.	Export Supplier, Electricity Distributor	Electricity Smart Meter	ECS17a
4.3	Read Instantaneous Prepay Values	This SRV is for reading the Smart Meter Prepayment Registers.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS19 GCS14
4.4.2	Retrieve Change of Mode/Tariff Triggered Billing Data Log	This SRV allows the Supplier to obtain a Tariff related Data set stored in the Billing Data Log on the Device on an ad-hoc basis for a specified date range.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS20b GCS15b
4.4.3	Retrieve Billing Calendar Triggered Billing Data Log	This SRV allows the Supplier to obtain a regular Consumption Data set stored in the Billing Data Log on the Device on an ad-hoc basis for a specified date range. It returns all log entries between the two dates specified.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS20c GCS15c
4.4.4	Retrieve Billing Data Log (Payment Based Debt Payments)	This SRV allows the Supplier to obtain a payment based Debt related Data set stored in the Billing Data Log for the Device on an ad-hoc basis for a specified date range.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS20a GCS15d
4.4.5	Retrieve Billing Data Log (Prepayment Credits)	This SRV allows the Supplier to obtain a Top Up Data set stored in the Billing Data Log for the Device on an ad-hoc basis for a specified date range.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS20d GCS15e
4.8.1	Read Active Import Profile Data	This SRV is for reading the Electricity Smart Meter Import / Gas Smart Meter half hourly 'active' Consumption Data.	Import Supplier, Gas Supplier ,Electricity Distributor Gas, Transporter, Other User	Electricity Smart Meter Gas Smart Meter GPF	ECS22b GCS17

4.8.2	Read Reactive Import Profile Data	This SRV is for reading the Electricity Smart Meter half hourly 'reactive' Consumption data.	Import Supplier, Electricity Distributor, Other User	Electricity Smart Meter	ECS22c
4.8.3	Read Export Profile Data	This SRV is for reading the half hourly Export values.	Export Supplier, Electricity Distributor, Other User	Electricity Smart Meter	ECS22a
4.10	Read Network Data	This SRV is for reading the voltage operational data on the Electricity Smart Meter, the voltage operational data on 3 phase Electricity Smart Meter or the gas network sampling Data Log.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	Electricity Smart Meter Gas Smart Meter	ECS23 ECS23b GCS18
4.11.1	Read Tariff (Primary Element)	This SRV is for reading the tariff configuration and operational data.	Import Supplier, Gas Supplier, Other User	Electricity Smart Meter Gas Smart Meter GPF	ECS24 GCS21f
4.11.2	Read Tariff (Secondary Element)	This SRV is for reading the Electricity Smart Meter second element tariff configuration.	Import Supplier, Other User	Electricity Smart Meter	ECS24b
4.12.1	Read Maximum Demand Import Registers	This SRV is for reading the Maximum Demand Import Registers on the Electricity Smart Meter.	Import Supplier, Electricity Distributor	Electricity Smart Meter	ECS18b
4.12.2	Read Maximum Demand Export Registers	This SRV is for reading the Maximum Demand Export Registers on the Electricity Smart Meter.	Export Supplier, Electricity Distributor	Electricity Smart Meter	ECS18a
4.13	Read Prepayment Configuration	This SRV is for reading Prepayment Configuration Data.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS26a GCS21b
4.14	Read Prepayment Daily Read Log	This SRV is for reading the (Prepayment) daily read log on the Smart Meter. The read request relates to retrieving Data from a PPMID.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS21b GCS16b
4.15	Read Load Limit Data	This SRV is for reading the Load Limit configuration	Import Supplier,	Electricity Smart Meter	ECS27

		and operational Data on the Electricity Smart Meter.	Electricity Distributor		
4.16	Read Active Power Import	This SRV is for reading the Import Power registers on the Electricity Smart Meter.	Import Supplier, Electricity Distributor	Electricity Smart Meter	ECS17c
4.17	Retrieve Daily Consumption Log	This SRV is for reading the Daily Consumption Log.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Other User	Electricity Smart Meter GPF	ECS66 GCS61
4.18	Read Meter Balance	This SRV is for reading the Meter balance(s).	Import Supplier Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS82 GCS60
4.6.1	Retrieve Import Daily Read Log	This SRV is for reading the import daily read log on the Smart Meter.	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	ECS21a GCS26a
4.6.2	Retrieve Export Daily Read Log	This SRV is for reading the daily read log on the Electricity Smart Meter for export.	Export Supplier	Electricity Smart Meter	ECS21c
6.2.1	Read Device Configuration (Voltage)	This SRV is for reading the Voltage Configuration Data on the Electricity Smart Meter.	Import Supplier, Electricity Distributor, Registered Supplier Agent	Electricity Smart Meter	ECS26b ECS26k
6.2.2	Read Device Configuration (Randomisation)	This SRV is for reading the load switching time Configuration Data on the Electricity Smart Meter.	Import Supplier, Electricity Distributor, Registered Supplier Agent	Electricity Smart Meter	ECS26c
6.2.3	Read Device Configuration (Billing Calendar)	This SRV is for reading the Billing Calendar configuration.	Import Supplier, Electricity Distributor, Registered Supplier Agent	Electricity Smart Meter Gas Smart Meter GPF	**GBCS v1.0** **GBCS v1.1** ECS26d GCS21d **GBCS2.0** ECS26l

					GCS21k
6.2.4	Read Device Configuration (Identity Exc MPxN)	This SRV is for reading Device identity Configuration Data. When the GBZ Target = "GPF", then the Service Request shall return the GPF Device Identifier rather than the Gas Smart Meter Device Identifier.	Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent, Other User	Electricity Smart Meter Gas Smart Meter GPF CHF	**GBCS v1.0** **GBCSv1.1** ECS26e GCS21e ECS26i **GBCS v2.0** ECS26m ECS26n GCS21m
6.2.5	Read Device Configuration (Instantaneous Power Thresholds)	This SRV is for reading the configured instantaneous power thresholds on the Electricity Smart Meter.	Import Supplier, Registered Supplier Agent	Electricity Smart Meter	ECS26f
6.2.7	Read Device Configuration (MPxN)	This SRV is for reading the MPAN / MPRN value of the Smart Meter.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User	Electricity Smart Meter Gas Smart Meter GPF	ECS40 GCS46
6.2.8	Read Device Configuration (Gas)	This SRV is for reading general Configuration Data on the Gas Smart Meter.	Gas Supplier, Gas Transporter, Registered Supplier Agent	Gas Smart Meter	GCS21a
6.2.9	Read Device Configuration (Payment Mode)	This SRV is for reading the payment mode configuration.	Import Supplier, Gas Supplier, Registered Supplier Agent	Electricity Smart Meter Gas Smart Meter GPF	ECS26j GCS21j
6.2.10	Read Device Configuration (Event and Alert Behaviours)	This SRV is for reading the event and alert behaviour configuration	Import Supplier, Gas Supplier, Electricity Distributor	Electricity Smart Meter Gas Smart Meter	**GBCS v2.0** ECS25r1 ECS25r2 GCS20r

6.13	Read Event Or Security Log	This SRV is for reading the Event or Security Log on the Device.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent	Electricity Smart Meter Gas Smart Meter GPF CHF	ECS35a ECS35b ECS35c ECS35d ECS35e ECS35f CS10a CS10b
6.24.1	Retrieve Device Security Credentials (KRP)	This SRV is for retrieving Public Security Credentials of the KPR.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	Electricity Smart Meter Gas Smart Meter GPF HCALCS	CS02a
6.24.2	Retrieve Device Security Credentials (Device)	This SRV is for retrieving the Device Security Credentials	Import Supplier, Gas Supplier	Electricity Smart Meter Gas Smart Meter GPF	CS02e
6.30	Read CHF Sub-GHz Configuration	This SRV reads the Sub-GHz configuration values from the CHF on a Dual Band CH	Import Supplier, Gas Supplier, Registered Supplier Agent	CHF – Dual Band Only	GBCS v2.0 DBCH03
6.31	Read CHF Sub-GHz Channel	This SRV reads the Sub GHz Channel the Dual Band CH is currently operating on	Import Supplier, Gas Supplier, Registered Supplier Agent	CHF – Dual Band Only	GBCS v2.0 DBCH01
6.32	Read CHF Sub-GHz Channel Log	This SRV reads the Sub GHz Channel Log from the Dual Band CH.	Import Supplier, Gas Supplier, Registered Supplier Agent	CHF – Dual Band Only	GBCSv2.0 DBCH02
7.4	Read Supply Status	This SRV is for reading the status of the Load Switch/Valve in the Smart Meter.	Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered	Electricity Smart Meter Gas Smart Meter GPF	ECS45 GCS33

			Supplier Agent		
7.7	Read Auxiliary Load Switch Data	This SRV is for reading the HCALCS and ALCS Data from the Electricity Smart Meter,	Import Supplier, Other User	Electricity Smart Meter	ECS61a
7.11	Read Boost Button Details	This SRV is for reading the boost button Data from the Electricity Smart Meter.	Import Supplier, Other User	Electricity Smart Meter	ECS61c
8.9	Read Device Log	This SRV provides details of the Devices currently in the Devices' Device Log. It also provides the date-time at which each Device was last communicated with by the Communications Hub.	Import Supplier, Gas Supplier, Other User	Electricity Smart Meter Gas Smart Meter GPF CHF HCALCS PPMID	CCS05 CCS04 CS07
11.2	Read Firmware Version	This SRV is for reading the Firmware Version on the Device.	Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent, Other User	Electricity Smart Meter Gas Smart Meter GPF CHF	ECS52 GCS38

The DCC receives the Service Request, completes standard Critical[16] / Non-Critical Service Request processing, and sends a Command to the Device. The Device receives the Command, executes it and if required Encrypts the data, and sends a Response to the DCC.

On receipt of the Service Response, the User detects the Encryption, and decrypts the Response, using its Agreement Key Private Key.

7.4.1.6.3 Read (Non-Device)

A User may wish to read certain information held in the DCC Systems. There are two ways of reading such information:

- Via the SSI
- Via Service Requests

[16] Only one Service Request, which is designed to read information on a Device, is Critical. This is 'Retrieve Device Security Credentials (Device)' Service Request (SRV 6.24.2).

To use the Service Request route, the User composes a Service Request and sends it to the DCC. The list of Read (non-Device) Service Requests is below.

Table 9. Read (non-Device) Service Requests

SRV	Name	When and how used?	Actors
5.2	Read Schedule	This SRV is for reading either all Schedules that has been created for a specified Device, or just a single Schedule.	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Other User, Export Supplier
8.2	Read Inventory	This SRV is for reading the SMI	Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent, Other User
12.1	Request WAN Matrix	This SRV is for checking the WAN coverage availability.	Import Supplier, Export Suppler, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent, Other User

The DCC receives the Service Request and undertakes non-Device Service Request processing. The DCC sends a Service Response containing the information requested by the User.

Read Inventory via the SSI

To read information held in the SMI, on the SSI the User can filter through the SMI by providing one or more of the following:

- MPxN;
- Device ID;
- Full postcode and property filter (inclusive of property name / number); and / or
- UPRN.

The User then uses the SMI search to find a specific Device, and follows the Device ID link, to request the detailed view for the selected Device (and Associated Devices). The following information is then provided:

- Device ID;
- Manufacturer;
- Device Model;
- Device Type;
- For Electricity Smart Meter only, the applicable Electricity Smart Meter Variant;
- SMETS Version;
- For CH only, the WAN Technology Type;
- Firmware Version;
- For CH only, the CSP region in which the Device is or has been installed;
- MPxN;
- For all Devices that are not Type 2 Devices, SMI Status (including Status history);
- First line of the address;
- UPRN;
- Full postcode;
- Associated Devices and Devices with which that Device is Associated;
- SMI Status; and
- Description of Device.

7.4.1.7 Associated Process Areas

#	Process Areas
7.1.1	Manage Inventory
7.2.1	Install and Commission
7.2.2	Install and Leave
7.2.3	Post Commissioning Obligations
7.3.1	Configure Device
7.3.2	Prepayment
5.7.3	Manage Firmware
7.6.1	Replace Communications Hub
7.6.1	Remove and Decommission Devices
7.7.1	Transitional Change of Supplier
7.7.2	Manage Security Credentials
7.8.3	Manage Schedule
7.8.4	Service Request Processing
7.9.5	No WAN Issues

7.5 Manage Device

This functional area describes how Devices can be managed via the DCC. Typically, the processes for managing Devices are triggered by certain events such as Change of Supplier or Change of Tenancy. This functional area focuses on the specific processes Suppliers will follow to manage Devices.

7.5.1 Contact Customer

7.5.1.1 Introduction

This process area refers to the ability of Users to interact with Energy Consumers via Meters and PPMIDs / IHDs.

The circumstances under which this may take place are:

- When a Supplier wishes to display a message for the Energy Consumer on the Meter's User Interface and IHD / PPMID. The message could be for marketing purposes, or to provide latest pricing information or customer service updates.
- When a Supplier wishes to update its name and contact details following a CoS Event or an internal organisational change.
- When a Supplier is asked to reset its Energy Consumer's Privacy PIN.
- When an Other User wishes to obtain evidence that the Energy Consumer has given them permission to access information that is considered as 'personal'. Other Users need to retain such evidence to demonstrate compliance with the Data Protection Act.

7.5.1.2 Scope

This process areas includes:

- Display Message
- Update Supplier Name
- Disable Privacy PIN
- Request Customer Identification Number

This process area excludes:

- Any means of communications between the Supplier and Energy Consumer, such as telephone contact, emails, webforms, letters, meetings, site visits etc; and
- Any internal Supplier policies governing their behaviour when responding to Energy Consumers' requests.

7.5.1.3 Inputs

- 'Display Message' Service Request (SRV 3.1)

- ‘Update Supplier Name’ Service Request (SRV 3.4)
- ‘Disable Privacy PIN’ Service Request (SRV 3.5)
- ‘Request Customer Identification Number’ Service Request (SRV 9.1)

7.5.1.4 Actors

- Supplier
- Other User
- Energy Consumer
- DCC
- Smart Meter
- IHD

7.5.1.5 Process Description

7.5.1.5.1 Display Message

To display a message for the Energy Consumers on the Meter’s User Interface and IHD / PPMID (if present), the Supplier composes a ‘Display Message’ Service Request (SRV 3.1), and sends it to the DCC. This Service Request includes the text to be displayed.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a ‘Send message to Electricity Smart Meter’ (ECS10) Command to the Electricity Smart Meter or a ‘Send message to Gas Smart Meter’ (GCS07) Command to the Gas Smart Meter.

The Smart Meter receives the Command and executes it by displaying the text on the Smart Meter’s User Interface. If an IHD / PPMID forms part of the SMS, the Smart Meter sends a Command to the IHD / PPMID. The IHD / PPMID receives and executes it by displaying the text on the IHD / PPMID.

The Smart Meter sends a Response to the DCC. The DCC receives it and sends a Service Response (SRV 3.1) to the Supplier.

7.5.1.5.2 Update Supplier Name

Following a CoS event, the Supplier may wish to update their name and telephone number on the Smart Meter’s User Interface. To do that, the Supplier composes an ‘Update Supplier Name’ Service Request (SRV 3.4) and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a ‘Write Supplier Contact Details on Electricity Smart Meter’ (ECS16) Command to the Electricity Smart Meter or a ‘Write Contact Details on Gas Smart Meter’ (GCS44) Command to the Gas Smart Meter.

The Smart Meter receives the Command, executes it by updating the Supplier's name and telephone number on the Meter's User Interface and sends a Response to the DCC. The DCC receives it and sends a Service Response (SRV 3.4) to the Supplier.

7.5.1.5.3 Disable Privacy PIN

Privacy PIN is a four-digit number set and used by the Energy Consumer to enable temporary access to a specified set of display items. It also enables the Smart Meter to execute certain Commands via the Smart Meter's User Interface.

If the Privacy PIN has been set by the Energy Consumer, the display items that relate to the Smart Meter balance and the level of debt will not be displayed on the Smart Meter's User Interface. These items will only be displayed if the Energy Consumer has entered the Privacy PIN.

Equally, unless the Energy Consumer has entered the Privacy PIN, the Smart Meter will not activate Emergency Credit (if in Prepayment Mode), will not disable the Privacy PIN and will not set a new Privacy PIN.

If the Privacy PIN has been set, and the Energy Consumer wishes to disable it but does not know what the Privacy PIN is, the only way to disable the Privacy PIN is for the Energy Consumer to contact the Supplier. The Supplier can disable the Privacy PIN remotely.

The Energy Consumer contacts the Supplier to disable the current Privacy PIN. The Supplier follows an internal policy to ascertain whether the Privacy PIN can be disabled. The communication between the Supplier and Energy Consumer is via an out-of-band process.

If the Supplier is satisfied that the Privacy PIN can be disabled, the Supplier composes a 'Disable Privacy PIN' Service Request (SRV 3.5) and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Disable Privacy PIN on Electricity Smart Meter' (ECS14) Command to the Electricity Smart Meter or a 'Disable Privacy PIN to Gas Smart Meter' (GCS11) Command to the Gas Smart Meter.

The Smart Meter receives the Command, executes it by disabling the Privacy PIN and sends a Response to the DCC. The DCC receives it and sends a Service Response (SRV 3.5) to the Supplier.

The Supplier informs the Energy Consumer that the Privacy PIN has been disabled. This communication is via an out-of-band process. The Energy Consumer is now free to create a new Privacy PIN, if they wish to do so. If the Energy Consumer wishes to create a new Privacy PIN, they use the Smart Meter's User Interface to create the new Privacy PIN.

7.5.1.5.4 Request Customer Identification Number

If an Other User wishes to access the Energy Consumer's Consumption Data, it must obtain consent from the Energy Consumer for the purpose of demonstrating compliance with the Data Protection Act. This process describes how the Other User could go about collecting such evidence.

The Other User composes a 'Request Customer Identification Number' Service Request (SRV 9.1) and sends it to the DCC. The Service Request includes a 4 digit CIN that has been issued by the Other User.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Send CIN to Electricity Smart Meter' (ECS50) Command to the Electricity Smart Meter or 'Send CIN to Gas Smart Meter' (GCS36) Command to the Gas Smart Meter.

The Smart Meter receives the Command and executes it by displaying the 4 digit CIN issued by the Other User on the Smart Meter's User Interface. If an IHD / PPMID forms part of the SMS, the Smart Meter sends a Command to the IHD / PPMID to display the CIN. The IHD / PPMID receives the Command and executes it by displaying the 4 digit CIN.

The Smart Meter sends a Response to the DCC. The DCC receives it sends a Service Response (SRV 9.1) to the Other User. If the Command has been Successfully Executed, the Response and therefore Service Response will include the 4 digit CIN.

The Other User asks the Energy Consumer to provide the CIN back. This is an out-of-band process, for example over the telephone between the Energy Consumer and Other User or the Energy Consumer enters the CIN onto the Other User's webpage. It should be noted that if the Privacy PIN has been set by the Energy Consumer, the Energy Consumer would need to enter their Privacy PIN to retrieve the CIN from the Smart Meter's User Interface. The Other User would keep record of the Energy Consumer confirmation of the CIN to evidence compliance with the Data Protection Act.

7.5.1.6 Associated Process Areas

#	Process
7.7.1	Transitional Change of Supplier
7.8.4	Service Request Processing

7.5.1.7 Governance

Actor	SEC Document	Clause	Text
7.5.1.5.4 Request Customer Identification Number			
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.5.6	The DCC shall return Responses from the Device to the User via a Service Response in this format. The DCC shall when sending a Service Response that contains a response from a Device (other than a response to Service Request 9.1 - Request Customer Identification Number or to a DCC scheduled request) conform to the GBCSPayload format using the Response XML element of the DUIS XML Schema. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.5.6	The DCC shall return Responses from the Device to the User via a Service Response in this format. The DCC shall when sending a Service Response that contains a response from a Device (other than a response to Service Request 9.1 - Request Customer Identification Number or to a DCC scheduled request) conform to the GBCSPayload format using the Response XML element of the DUIS XML Schema. https://smartenergycodecompany.co.uk/download/4639

Actor	SEC Document	Clause	Text
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.5.7	The DCC shall, for successful requests by the DCC Access Control Broker to send a CIN to a Device, return the CINMessage format. This message combines the GBCSPayload received from the Device with the Customer Identification Number generated by the DCC. The DCC shall, when sending a Service Response that contains a response from a Device to a Service Request 9.1 - Request Customer Identification Number, conform to the CINMessage format using the Response XML element of the DUIS XML Schema. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.5.7	The DCC shall, for successful requests by the DCC Access Control Broker to send a CIN to a Device, return the CINMessage format. This message combines the GBCSPayload received from the Device with the Customer Identification Number generated by the DCC. The DCC shall, when sending a Service Response that contains a response from a Device to a Service Request 9.1 - Request Customer Identification Number, conform to the CINMessage format using the Response XML element of the DUIS XML Schema. https://smartenergycodecompany.co.uk/download/4639

7.5.2 Change of Tenant

7.5.2.1 Introduction

This process area covers the process for restricting access to Data stored on the Electricity Smart Meter, GPF and Associated Gas Smart Meter after a change of occupancy at the premises. This process supports Suppliers in discharging their responsibilities under the Data Protection Act, by preventing the new occupant from accessing the previous occupant's personal Data, and by preventing Other Users who had permission from the previous occupant to assess their Data from accessing the new occupant's Data.

The date from which the data access restriction applies may be in the future or in the past. Once set, the date is used by the Electricity Smart Meter or GPF to restrict access to the following information:

- Profile Data log
- Cumulative and Historical Value Store
- Daily Read Log
- Prepayment Daily Read Log
- Billing Data Log

- Daily Consumption Log

The previous occupant may wish to make historic information on the Electricity Smart Meter or GPF available to be viewed by informing the Supplier. The way in which they inform the Supplier of this is via an out-of-band process.

7.5.2.2 Scope

This process area includes Restricting Access for Change of Tenancy.

This process area excludes business processes and financial reconciliation at the changeover between previous and new occupants and the Supplier.

7.5.2.3 Inputs

- 'Restrict Access for Change of Tenancy' Service Request (SRV 3.2)

7.5.2.4 Actors

- Supplier
- Other Users
- DCC
- Electricity Smart Meter
- GPF

7.5.2.5 Process Description

7.5.2.5.1 Restrict Access for Change of Tenancy

The occupant notifies the Supplier of a change of occupancy at a premises. This notification may be before or after the change of occupancy.

The Supplier composes a 'Restrict Access for Change of Tenancy' Service Request (SRV 3.2) and sends it to DCC. This Service Request includes the Restriction Date Time as notified by the occupant.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Set Change of Tenancy date' (ECS12) Command to the Electricity Smart Meter or a 'Set Change of Tenancy date' (GCS09) Command to the GPF.

The Device receives the Command, and either executes it immediately or stores it and executes it on the Execution Date Time, and sends a Response to the DCC.

The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 3.2) to the Supplier;
- If the Response indicates success, on the Restriction Date Time deletes any active Schedules for the Electricity Smart Meter or GPF and the Associated Gas Smart Meter created by Other

Users, and sends a 'Schedule removal because of CoT' (N4) DCC Alert to each Other User to inform them of the deletion; and

- If the Response indicates success, on the Restriction Date Time deletes any Future Dated Service Requests for the Electricity Smart Meter or GPF and the Associated Gas Smart Meter created by Other Users, and sends a 'Cancellation of Future Dated Response Pattern (DSP) requests because of CoT' (N3) DCC Alert to each Other User to inform them of the cancellation.

7.5.2.6 Associated Process Areas

#	Process Area
7.8.4	Service Request Processing

7.5.2.7 Governance

Actor	SEC Document	Clause	Text
7.5.1.5.4 Restrict Access for Change of Tenancy			
Supplier	Smart Energy Code	Section H3.17	As soon as reasonably practicable after a Responsible Supplier for an Enrolled Smart Metering System relating to a premises becomes aware of a change of occupancy at that premises, that Responsible Supplier shall send a 'Restrict Access for Change of Tenancy' Service Request to the DCC in relation to the Smart Meter and any Gas Proxy Function forming part of that Smart Metering System (except where the outgoing Energy Consumer has indicated that they wish historic information on the Smart Metering System to remain available to be viewed). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H3.18	As soon as reasonably practicable after receipt by the DCC of a Service Response from a Smart Metering System in respect of a 'Restrict Access for Change of Tenancy' Service Request, the DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services in respect of any Device forming part of that Smart Metering System for which the Command has not yet been sent and which are being processed on behalf of an Other User (and shall notify the relevant User of such cancellation via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.13.4	Upon successful execution of a RestrictAccessForChangeOfTenancy Service Request, the DCC shall, for the specified Device ID (for a Gas Proxy Function, Schedules on the associated Gas Smart Meter will also be deleted) identified within the Service Request, perform the following actions.

Actor	SEC Document	Clause	Text
			a) Delete all active DCC Schedules created by Other Users that are held within the DCC Systems and send a DCC Alert to the Schedule owner to inform them of their deletion. b) Delete all Future Dated (DSP) requests created by Other Users with future dated execution dates that have not been sent to the Device and send a DCC Alert to the original sender of the request https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.13.4	Upon successful execution of a RestrictAccessForChangeOfTenancy Service Request, the DCC shall, for the specified Device ID (for a Gas Proxy Function, Schedules on the associated Gas Smart Meter will also be deleted) identified within the Service Request, perform the following actions. a) Delete all active DCC Schedules created by Other Users that are held within the DCC Systems and send a DCC Alert to the Schedule owner to inform them of their deletion. b) Delete all Future Dated (DSP) requests created by Other Users with future dated execution dates that have not been sent to the Device and send a DCC Alert to the original sender of the request https://smartenergycodecompany.co.uk/download/4639

7.5.3 Manage Firmware

7.5.3.1 Introduction

This process area describes the process for distributing and activating the Firmware on Smart Meters via the DCC. It also describes the specific obligations on the DCC with regards to distributing and activating the Firmware on a CH.

All Devices contain Firmware, which has a unique Firmware version. Firmware on Smart Meters and CHs can be upgraded without physically removing or replacing the Device.

Firmware is likely to be upgraded in the following cases:

- Elective: A Supplier wishes to upgrade some of its Meters or the DCC needs to upgrade some of its CHs. For example, to introduce additional functionality on the Devices;
- Mandated through the SEC: To support a SEC change, Devices may require a Firmware upgrade. An example of such a potential requirement is in the recent BEIS consultation on

local CAD pairing[17]. For such SEC changes, the obligation would be on Suppliers / the DCC to ensure the required Firmware Images are developed, then distributed and activated on Devices;

- Operational issues which can be resolved by a Firmware upgrade: To bring an affected Device back from 'suspension' (for more detail see Section 7.1.2.4.3 of the BAD), a Firmware upgrade would need to be distributed and activated on such Devices.

7.5.3.2 Scope

This process area includes:

- Check Firmware Image Hash
- Update Firmware
- Activate Firmware
- Update CH Firmware

This process area involves but does not specifically describe:

- Read (Device) – Read Firmware Version. This process is described in Section 7.4.1.6.2 of the BAD.
- Suspend Device. This process is described in Section 7.1.2.4.3 of the BAD.

This process area excludes installing the initial version of Firmware on a Device, which is carried out at manufacture.

7.5.3.3 Inputs

- 'Update Firmware' Service Request (SRV 11.1)
- 'Activate Firmware' Service Request (SRV 11.3)

7.5.3.4 Actors

- Supplier
- DCC
- Smart Meter
- CH

7.5.3.5 Prerequisites

The new Device Model, and a hash of the Manufacturer Image, has been added to the CPL.

[17] https://www.gov.uk/government/consultations/consultation-on-implementing-home-area-network-han-solutions-and-changes-to-technical-sub-committee-tsc

For Meters, the Supplier's Trust Anchor Cell is populated with the Supplier's Organisation Certificate.

7.5.3.6 Process Description

Images less than 750kB in size

7.5.3.6.1 Check Firmware Image Hash

This section details the steps taken to remotely upgrade the Firmware on a Smart Meter.

The Smart Meter manufacturer produces the new Manufacturer Image and submits the following information to the Panel for the purpose of creating a new CPL entry:

- The 'Hash of a Manufacturer Image';
- The identity of the organisation that created the image. For the purposes of this illustration, this is assumed to be the manufacturer; and
- A Digital Signature created by the image creator across the communication containing the CPL entry details.

On receipt of the file, the Panel validates it. If validation is successful, the Panel creates a new CPL entry. This process is described in detail in Section 7.1.2. of the BAD.

The manufacturer provides the Firmware Image, Release Notes and other related information to the Supplier.

The Supplier obtains the following information:

- A copy of the Manufacturer Image;
- An OTA Header, which includes the following:
    - Manufacturer ID;
    - Model to which it can be applied;
    - Firmware Version contained in the image; and
    - Minimum and maximum hardware version to which it can be applied.
- A Digital Signature across the concatenation of the OTA Header and the Manufacturer Image created by the 'person' who created the Firmware Image; and
- A Hash value calculated across the Manufacturer Image by the sender of the Firmware Image.

The Supplier checks the following:

- The Digital Signature across the OTA Header and Manufacturer Image concatenation is valid, and is that of the manufacturer;

- The Hash the Supplier has calculated over the Manufacturer Image is the same as that provided to it;
- There is at least one CPL entry with the Hash; and
- At least one of the CPL entries corresponds to the OTA Header (i.e. that the OTA Header Manufacturer ID, model and Firmware Version fields match identically with the CPL entry); and
- The hardware version in that CPL entry is between OTA Header minimum and maximum hardware version, inclusively.

If any of the checks fail, the process stops here.

7.5.3.6.2 Update Firmware

If the checks are successful, the Supplier composes an 'Update Firmware' Service Request (SRV 11.1), including:

- The Firmware Image;
- Firmware Version; and
- A list of up to 50,000 Device IDs to which the Supplier wishes to send the Manufacturer Image.

The Supplier sends the Service Request to the DCC. The DCC receives the Service Request, completes Non-Critical Service Request processing and applies the following additional checks:

- Checks the image is not over the 750KB per image size limit;
- Calculates the Hash over the Manufacturer Image part of the Firmware Image supplied in the Service Request;
- Identifies the entry (or entries) in the CPL that contain this Hash (or rather the calculated Hash represented in hexadecimal format);
- Ensures that the Firmware Version in the Service Request equates to the Firmware Version in one of the CPL entries. This identifies the specific Device Model to which the image is to be applied; and
- For each of the Device IDs in the Service Request:
    - Checks that the Supplier is the Responsible Supplier for that Device ID and the Device is a Smart Meter;
    - Checks that the Device has a SMI Status of 'commissioned' or 'suspended'; and
    - Identifies its current Device Model, and ensures that the Manufacturer ID, model and hardware version for that current Device Model match to the entry.

The DCC sends a Service Response (SRV 11.1) to the Supplier. If any of Device IDs failed the check, the DCC lists the Device IDs that failed, and a reason for failure in the Service Response.

In addition, the DCC sends any of the following DCC Alerts if the following checks fail:

- a 'Firmware Version / Hash mismatch' (N18) DCC Alert if the Hash of the Manufacturer Image calculated by the DCC does not match the Hash held on the CPL and if the Firmware Version in one of the CPL entries does not match the Firmware Version in the Service Request;
- A 'Firmware Distribution Device ID identification failure' (N19) DCC Alert if the DCC cannot identify the Device Model to which the image should be applied;
- A 'Firmware image provided is too large' (N20) DCC Alert if the Firmware Image is greater than 750kB;
- An 'Unknown Firmware Version' (N21) DCC Alert if the Firmware Version in one of the CPL entries does not match the Firmware Version in the Service Request;

The DCC distributes the Firmware Image to each CH Associated with each Device which passed the checks. The DCC receives an acknowledgment that the CH has received the Firmware Image. If the DCC has not received such acknowledgement, it sends a 'Failure to deliver Update Firmware Command to CSP' (N22) DCC Alert to the Supplier.

The CH buffers the image and notifies the Smart Meter that the image is available to download. The Smart Meter asks the CH if there is an image that may be suitable in accordance with the Zigbee OTA specification. If that is the case, the Smart Meter requests details of the image.

The Smart Meter then downloads the image from the CH. When the download is complete, the CH sends a Response to the DCC. If the DCC does not receive the Response, it sends a 'Failure to receive Update Firmware Command Validation response from CSP' (N23) DCC Alert to the Supplier.

Once the image is downloaded, the Smart Meter checks the Supplier's Digital Signature within it[18] and stores it for subsequent activation. It then sends a 'Firmware Distribution Receipt' Device Alert detailing whether the signature check was successful (0x8F72 for success and 0x8F1C for failure) to the DCC, which the DCC forwards to the Supplier.

7.5.3.6.3 Activate Firmware

The Supplier receives the Device Alert. If the Device Alert indicates success, the Supplier may now compose and send an 'Activate Firmware' Service Request (SRV 11.3) to the DCC. The Service Request includes:

- The Hash of the Manufacturer Image (as checked at the start of the process by the Supplier); and
- (Optionally) an execution date-time, at which the Meter is to attempt activation.

The DCC applies Critical Service Request processing, and sends a 'Activate Firmware' (CS06) Command to the Smart Meter. (Note that Smart Meters cannot activate a new Manufacturer Image without a valid CS06 Command).

[18] GBCS Section 11.2.5

The Smart Meters receives and processes the CS06 Command.

If the CS06 Command is future dated, the Smart Meter:

- Undertakes the standard checks on a Critical Command;
- Stores the details for the future dated execution date-time and sends a CS06 Response to confirm validation and storage to the DCC, which the DCC forwards to the Supplier;
- At the execution date-time, the Smart Meter undertakes steps below; and
- Sends a 'Future Dated Firmware Activation' Device Alert (message code 0x00CA) to the DCC, which the DCC forwards to the Supplier. The Device Alert indicates success or failure.

If the CS06 Command is not future dated, the Smart Meter:

- Undertakes the standard checks on a Critical Command;
- Confirms it holds a Firmware Image;
- Confirms the Hash in the CS06 Command matches the Hash the Smart Meter calculates over the Manufacturer Image;
- Activates the Firmware Image. If successful, the Smart Meter also updates the value its holds for 'Firmware Version'. If unsuccessful, the Firmware Version remains unchanged; and
- The Smart Meter sends a Response, which contains a code detailing success or failure and a field containing the resulting Firmware Version.

The DCC receives the Response and does the following things:

- Sends a Service Response to the Supplier;
- If the Response / Alert indicates success, updates the Device's Firmware Version (and so Device Model) in the SMI; and
- If the Device's SMI Status is 'Suspended', changes the SMI Status of that Device to the status prior to suspension.

Images equal to or greater than 750kB in size

7.5.3.6.4 Update and Activate Firmware -

This section details the steps taken to remotely upgrade the Firmware on a Smart Meter where the Image is equal to or greater than 750kB in size.

The process of activating and upgrading is essentially the same is described above, but with the following key distinctions:

The Manufacturer has split the upgrade into multiple* images. (*For simplicity, this example uses two images 0x15 and 0x20, but there is no limit on the number of images which may be required.)

Two entries are created on the CPL, one for each Firmware Version 0x15 and 0x20.

As before, the manufacturer provides the Manufacturer Images, Release Notes and other related information to the Supplier. The Supplier receives the information and composes an 'Update Firmware' Service Request (Service Reference Variant 11.1) with Image 0x15.

On receipt of each successful Firmware Distribution Receipt Device Alert, the Supplier sends an immediate 'Activate Firmware' Service Request (Service Request Variant 11.3). Following the receipt of a CS06 Response indicating success, repeat the process for Image 0x20.

If CS06 Responses have not been received, the Supplier may check whether Image 0x15 has been activated by sending a 'Read Firmware Version' Service Request (SRV 11.2) to the DCC. The process is described in Section 7.5.3.6.6 of the BAD.

7.5.3.6.5 Update CH Firmware

This section describes the process used by the DCC to upgrade the Firmware on CHs. This broadly follows that same approach as with Smart Meters, but the requirements are less prescriptive.

The DCC is not constrained in the way it distributes Firmware Images to CHs.

The DCC is not required to use the ZigBee OTA Header format to hold information about the images.

The DCC is not constrained in the mechanisms it uses to notify delivery of an image to a CH.

The DCC creates Commands, and does not need to use a Service Request.

The specific differences are laid out in the following sections.

The DCC must perform the same checks in relation to a CH's image as Suppliers undertake for a Smart Meter image, except that:

- There is no requirement to receive an OTA Header (and therefore the signature received by the DCC from the creator of the image is only across the Firmware Images);
- There is an additional requirement that the DCC has received sufficient information about the Firmware Images to check whether there is a corresponding entry on the CPL. This is an equivalent to the OTA Header requirement except that the format of this information is not prescribed and there is no requirement for a signature across it;
- There is no requirement to receive the Firmware Image Hash from the Manufacturer; and
- The Hash of the image must be calculated by the DCC for validation against the CPL, but there is no obligation to validate this against a hash supplied together with the Firmware Images. There is also no requirement to provide an OTA header, although the fields required to validate the image against the CPL must be provided in some form. For clarity, these fields are:
    - Manufacturer ID ('Manufacturer code');
    - Model to which it can be applied ('Image type');

- Firmware Version contained in the image ('File version'); and
- Minimum and maximum hardware version to which it can be applied ('Minimum / Maximum hardware version').

Unless the activation of the replacement Firmware Images is required for urgent security related reasons, the DCC is required to inform relevant Users of its intention to update CH firmware seven days before this takes place. This notification may take place during or after firmware delivery to the CH, as this step is separate to the activation of the image. If the upgrade is security related, this notification process may be later and should not delay the delivery and activation processes.

The DCC is not constrained by the SEC in how it delivers the new image to the CH. However, it is understood that the DCC uses the CS06 Command to activate the Firmware (the Command has a MAC applied by the DSP and is Digitally Signed by the WAN Provider). The CH follows the same processing steps as the Smart Meter. On receipt of a CS06 Response from the CH, the DCC updates the Device's Firmware Version (and so Device Model) in the SMI. If the Device's SMI Status is 'Suspended', the DCC changes the SMI Status of that Device to the SMI Status prior to suspension.

The DCC is not bound by a size limit on Firmware Images so it may be possible for the WAN Provider to distribute images of over 750KB and perform large upgrades in a single step. However, there may still be occasions when a WAN Provider wishes to perform an upgrade in multiple steps.

The image may be split as desired by the manufacturer, as long as each of the resulting Firmware Images are included on the CPL.

As with other upgrades, the manufacturer is responsible for deciding whether re-certification is required for each combination, and the DCC is responsible for notifying the Panel where Assurance Certificates are reused.

7.5.3.6.6 Read (Device) – Read Firmware Version

The Supplier may use a 'Read Firmware Version' Service Request (SRV 11.2) to verify the current Firmware Version and hence confirm whether the activation was successful or not. Users in other User Roles are also eligible to send this Service Request if they wish to check the Firmware Version on Meters and CHs.

This process is described in Section 7.4.1.6.2 of the BAD.

The Response resulting from the 'Read Firmware Version' Service Request is not used by the DCC to update the Device's details on the SMI, and so the SMI may not have an accurate record of the Device's Device Model in this circumstance. If User discovers an inconsistency between the Firmware Version read from the Device and the SMI record the User may wish to raise an issue through the DCC's Service Management mechanisms.

7.5.3.7 Associated Process Areas

#	Process
7.1.1	Manage Inventory
7.1.2	CPA / CPL

7.4.1	Read
7.8.4	Service Request Processing

7.5.3.8 Governance

Actor	SEC Document	Clause	Text
7.5.3.6.1 Check Firmware Image Hash			
User	SEC Appendix AB - Service Request Processing Document	2.2	A User shall only send an 'Update Firmware' Service Request in respect of a Device if: (a) the User has received the following information: (i) the OTA Header and the associated replacement Manufacturer Image; (ii) a Digital Signature, created by the person who created the Manufacturer Image, across the concatenation of the OTA Header and the associated replacement Manufacturer Image; and (iii) the Hash of the replacement Manufacturer Image; (b) the User has successfully confirmed that the Digital Signature across the concatenation is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party); (c) the User has generated its own Hash from the replacement Manufacturer Image, and confirmed that the Hash that the User has generated is the same as the Hash provided; and (d) the User has confirmed that a Device Model associated with the replacement Manufacturer Image (as determined by the Hash and the information in the OTA Header) is currently on the Certified Product List. https://smartenergycodecompany.co.uk/download/2271
7.5.3.6.5 Upgrade CH Firmware			
DCC	SEC Appendix AB - Service Request Processing Document	5.1	The DCC shall only send a communication to distribute different firmware to a Communications Hub if: (a) the DCC has received the replacement Manufacturer Image and a Digital Signature, created by the person who created the Manufacturer Image, across that Manufacturer Image; (b) the DCC has received information about the Manufacturer Image sufficient to determine whether it is on the Certified Products List; (c) the DCC has successfully confirmed that the Digital Signature across the replacement Manufacturer Image is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party); and (d) a Device Model associated with the replacement Manufacturer Image is currently on the Certified Product List, as determined by: (i) the Hash the DCC calculates over the Manufacturer Image; and (ii) the information about the Manufacturer Image provided pursuant to Clause 5.1(b).

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	5.2	The DCC shall notify relevant Users of its intention to activate replacement Manufacturer Images in relation to Communications Hubs at least 7 days in advance of doing so; provided that DCC need not notify Users in advance if the activation of the replacement Manufacturer Images is required for urgent security related reasons (and in such circumstances the DCC shall take reasonable steps to notify Users in advance of activating replacement Manufacturer Images or, where it has not notified them in advance, shall notify them of having done so as soon as is reasonably practicable after the event) https://smartenergycodecompany.co.uk/download/2271

7.5.4 Manage Supply

7.5.4.1 Introduction

This process area describes how Suppliers manage the supply of energy to premises via the DCC.

Suppliers have the ability to remotely disconnect supply and then enable it. Supply may also be disabled by the Smart Meter itself, if the Smart Meter has been configured as such. Supply may be disabled for a variety of reasons, for example if a Smart Meter has been tampered with.

7.5.4.2 Scope

This process area includes:

- Arm Supply
- Enable Supply
- Disable Supply
- Disable Supply Device Alerts

This process area involves but does not specifically describe Prepayment logic leading the Meter to Disable and Arm supply when the Meter Balance falls below the Disablement Threshold. This is described in more detail in Section 7.3.2.5.3 of the BAD.

This process area excludes communications, contractual or legal proceedings between the Supplier and Energy Consumer once the supply is disabled.

7.5.4.3 Inputs

- ‘Enable Supply’ Service Request (SRV 7.1)
- ‘Disable Supply’ Service Request (SRV 7.2)

- ‘Arm Supply’ Service Request (SRV 7.3)

7.5.4.4 Actors

- Supplier
- Energy Consumer
- DCC
- Smart Meter

7.5.4.5 Prerequisites

For specific steps described in this process:

- The Supplier configured Supply Tamper State such that a subsequent attempted Unauthorised Physical Access through the Device’s Secure Perimeter causes the Smart Meter to establish a Locked state.
- The Gas Supplier configured the Supply Depletion State such that a subsequent loss (or impending loss) of Gas Smart Meter power causes the Gas Smart Meter to establish a Locked state.

7.5.4.6 Process Description

7.5.4.6.1 Arm Supply

There is only one way to Enable the Gas Smart Meter, which is locally by the Energy Consumer. For the Gas Smart Meter to be Enabled locally, it must first be Armed.

The Electricity Smart Meter can be locally Enabled in two ways:

- Locally, by the Consumer using the Electricity Smart Meter;
- Locally, by the Consumer using a PPMID forming part of the Electricity SMS.

To Arm the Smart Meter, the Supplier composes an 'Arm Supply ' Service Request (SRV 7.3) and sends it to the DCC.

The DCC receives it, completes Critical Service Request processing and sends an ‘Arm Load Switch/ Valve’ (ECS44) Commands to the Electricity Smart Meter or ‘Arm Load Switch / Valve’ (GCS39) to the Gas Smart Meter.

The Gas Smart Meter receives the Command and executes it first by checking the current Supply State.

If the state of the supply is Enabled or Armed, the Smart Meter:

- Arms the supply;

- Sets the Supply State to Armed;
- Sends a 'Supply Armed' Device Alert (Alert Code: 0x8F32) to the DCC, which the DCC forwards to the Supplier;
- Displays the Supply State on the User Interface.

If the state of the supply is Disabled as a result of:

- A Disable Supply Command (Electricity Smart Meter and Gas Smart Meter);
- Loss of power to the Gas Smart Meter (Supply Depletion State);
- An Unauthorised Physical Access and Supply Tamper State (Electricity Smart Meter and Gas Smart Meter);

then the Smart Meter Arms the supply and sets the Supply State to Armed. Otherwise the Meter does not Arm the supply. Any changes to the Supply State are displayed on the User Interface.

If the Supply State is set to Armed, the Meter:

- Returns from a Locked state to an Unlocked State; and
- Sends a Response to the DCC.

The DCC receives the Response and send a Service Response (SRV 7.3) to the Supplier.

The Supplier may inform the Energy Consumer that the Meter can now be Enabled, which is an out-of-band process. This information will be displayed in the PPMID / IHD.

The Energy Consumer Enables the supply on the Electricity Smart Meter by closing the load switch or Gas Smart Meter by opening the valve through the Smart Meter's User Interface. The Consumer may use the PPMID to enable the supply of electricity by following instructions on the PPMID.

The supply is now Enabled. The Supply State on the User Interface is set to Enabled.

7.5.4.6.2 Enable Supply

To Enable supply remotely, the Import Supplier composes an 'Enable Supply' Service Request (SRV 7.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends a 'Remotely Close the Load Switch on the Electricity Smart Meter' (ECS42) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command and executes it by first checking the current Supply State.

If the Supply State is Armed, the Electricity Smart Meter sets the Supply State to Enabled. The Supply State is displayed on the User Interface.

If the state of the Supply is Disabled as a result of:

- a Disable Supply Command; or
- an Unauthorised Physical Access and the Supply Tamper State,

the Electricity Smart Meter Enables the supply and sets the Supply State to Enabled. Otherwise the Electricity Smart Meter does not Enable the supply. Any changes to the Supply State are displayed on the User Interface.

If the Supply State is set to Enabled, the Electricity Smart Meter:

- Returns from a Locked state to an Unlocked State;
- Closes the Load Switch to physically enable the electricity supply; and
- Sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 7.1) to the Import Supplier.

7.5.4.6.3 Disable Supply

A supply can be Disabled by the Supplier or by the Meter itself. The process for disabling the supply by the Supplier is described below:

The Supplier composes a 'Disable Supply ' Service Request (SRV 7.2) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing, and sends a ‘Remotely Open the Load Switch / close Valve’ (ECS43) Command to the Electricity Smart Meter or ‘Remotely Open the Load Switch / close Valve’ (GCS32) Command to the Gas Smart Meter.

The Smart Meter does the following things:

- Disables the supply by opening the Load Switch (Electricity Smart Meter), or closing the Valve (Gas Smart Meter);
- Sets the Supply State to Disabled and displays it in the User Interface;
- Establishes a Locked state; and
- Sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 7.2) to the Supplier.

7.5.4.6.4 Disable Supply Device Alerts

The Smart Meter may Disable the supply for the following reasons:

- Unauthorised Physical Access through the Device’s Secure Perimeter. On the occurrence of such event, the Smart Meter:

- Closes the valve or opens the Load Switch to Disable the physical supply;
- Sets the Supply State to Disabled and displays it on the User Interface;
- Sends an 'Unauthorised Physical Access – Tamper Detect' (Alert Code: 0x8F3F) Device Alert to the DCC (Note: The device may instead send a different Device Alert from the "Mandated -Conditional Group 1" of Alerts), which the DCC forwards to the Supplier; and
- Where the Supply Tamper State is configured to require Locking, sends a 'Supply Disabled then Locked – Supply Tamper State Cause' (Alert Code: 0x81BE) Device Alert to the DCC, which the DCC forwards to the Supplier, and establishes a Locked state if the supply is Disabled. This means that the Supply can only be Armed in response to a Command to Arm Supply or Enable Supply (Electricity Smart Meter only).

- Gas Smart Meter only, loss (or impending loss) of Gas Smart Meter power. On the occurrence of such event, the Gas Smart Meter:
  - Closes the valve to Disable the physical supply;
  - Sets the Supply State to Disabled and displays it on the User Interface;
  - Sends a 'Gas Smart Meter Power Supply Loss' (Alert Code: 0x8F1D) Device Alert to the DCC, which the DCC forwards to the Gas Supplier; and
  - Where the Supply Depletion State is configured to require Locking, establishes a Locked state if the supply is Disabled. This means that the supply can only be Armed in response to a Command to Arm supply.

- Gas Smart Meter only, where the flow rate exceeds a level defined by the Uncontrolled Gas Flow Rate. On the occurrence of such event the Gas Smart Meter:
  - Closes the valve to disable the physical supply;
  - Sets the Supply State to Disabled and then to Armed and displays it on the User Interface; and
  - Sounds an Alarm via its User Interface.

- For Smart Meters in Prepayment Mode, the combined credit of the **Error! Reference source not found.** and **Error! Reference source not found.** falls below the **Error! Reference source not found.**, the Smart Meter:
  - Disables the supply, sets that Supply State to Disabled and displays it on the User Interface; and
  - Displays an Alert on its User Interface and sends a 'Credit Below Disablement Threshold (Prepayment Mode)' (Alert Code: 0x8F0F) Device Alert to the DCC, which the DCC forwards to the Supplier.

- Electricity Smart Meter only, when the Active Power Import is above, for the Load Limit Period, the Load Limit Power Threshold. On occurrence of such event the Electricity Smart Meter:
  - Sends a 'Supply Disabled then Armed – Load Limit triggered' (Alert Code: 0x8F33) Device Alert to the DCC, which the DCC forwards to the Import Supplier;
  - Disables the supply if the Load Limit Supply State has been configured to require Disablement;
  - Immediately Arms the supply;
  - After the Load Limit Restoration Period has elapsed Enables the supply;
  - Displays any changes in the Supply State on the User Interface; and
  - Sends a 'Supply Enabled after Load Limit Restoration Period (Load Limit triggered)' (Alert Code: 0x8F34) Device Alert to the DCC, which the DCC forwards to the Import Supplier.

7.5.4.7 Associated Process Areas

#	Process Areas
7.3.2	Prepayment
7.8.4	Service Request Processing

7.5.5 Manage Load Control

7.5.5.1 Introduction

This process area describes how Suppliers can manage Auxiliary Load Control Switches (ALCS) (embedded in the Electricity Smart Meter) and HCALCS (HAN controlled) via the DCC. ALCS and HCALCS configuration and management is important in effective management of the supply of electricity to a premises. While there are no obligations on Import Suppliers to configure and operate ALCS and HCALCS, Import Suppliers may have commercial incentives to do so.

7.5.5.2 Scope

This process area includes Manage Load Control.

This process area involves but does not specifically describe Configure Device. This process is described in more detail in Section 7.3.1.6.3 of the BAD.

7.5.5.3 Inputs

- 'Update Device Configuration (Auxiliary Load Control Description)' Service Request (SRV 6.14.1)
- 'Update Device Configuration (Auxiliary Load Control Scheduler)' Service Request (SRV 6.14.2)
- 'Activate Auxiliary Load' Service Request (SRV 7.5)

- ‘Deactivate Auxiliary Load’ Service Request (SRV 7.6)
- ‘Reset Auxiliary Load’ Service Request (SRV 7.8)
- ‘Add Auxiliary Load to Boost Button’ Service Request (SRV 7.9)
- ‘Remove Auxiliary Load from Boost Button’ Service Request (SRV 7.10)

7.5.5.4 Actors

- Import Supplier
- DCC
- HCALCS
- ALCS

7.5.5.5 Process Description

7.5.5.5.1 Configure Device – Set Randomised Offset Limit

The Import Supplier composes a ‘Set Randomised Offset Limit’ Service Request (SRV 7.12) and sends it to the DCC. The process is described in Section 7.3.1.6.3 of the BAD. Note that GBCS v2.0 mandates the Electricity Smart Meter to have the Randomisation Offset Limit pre-configured to 600 seconds at manufacturing.

7.5.5.5.2 Manage Load Control

To operate ALCS / HCALCS via the DCC, the Import Supplier has a number of Service Requests available to it to access functionalities on ALCS / HCALCS via the DCC.

The list of Manage Load Control Service Requests is below.

Table 10. Manage Load Control Service Requests

SRV	Service Request Name	Command Reference	Eligible User Roles	Target Device	Critical / Non-Critical
7.9	Add Auxiliary Load to Boost Button	ECS62	Import Supplier	Electricity Smart Meter	Non-Critical
7.10	Remove Auxiliary Load from Boost Button	ECS62	Import Supplier	Electricity Smart Meter	Non-Critical
6.14.1	Update Device Configuration (Auxiliary Load Control Description)	ECS46a	Import Supplier	Electricity Smart Meter	Critical
6.14.2	Set Configurations for load control in Electricity Smart Meter	ECS46c	Import Supplier	Electricity Smart Meter	Critical

	(excluding HC ALCS and ALCS Labels)				
7.5	Activate Auxiliary Load	ECS47	Import Supplier	Electricity Smart Meter	Critical
7.6	Deactivate Auxiliary Load	ECS47	Import Supplier	Electricity Smart Meter	Critical
7.8	Reset Auxiliary Load	ESC47	Import Supplier	Electricity Smart Meter	Critical

The Import Supplier composes a Service Request and sends it to the DCC.

The DCC receives the Service Request, completes Critical / Non-Critical Service Request processing and sends a Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command, executes it and sends a Response the DCC.

The DCC receives the Response and sends a Service Response to the Import Supplier.

Once the ALCS Calendar has been configured (SRV 6.14.2), the Electricity Smart Meter monitors the ALCS Calendar. At the scheduled times, the Electricity Smart Meter checks that Supply is Enabled, applies the Randomised Offset, and then switches the ALCS or HCALCS on or off by setting the switch to closed or open.

For ALCS, this is achieved by a machine-to-machine instruction. For HCALCS this is achieved by a HAN Command.

The Import Supplier may choose to issue Commands which have the effect of overriding the switch schedule, and reverting to it at a later point in time. This is achieved by Activating, Deactivating, or Resetting the Auxiliary Load.

7.5.5.1 Associated Process Areas

#	Process Areas
7.8.4	Service Request Processing

7.5.6 Manage Alerts

7.5.6.1 Introduction

Alerts are unsolicited messages triggered by specific events.

DCC Alerts are generated by the DCC in response to specific events, and sent to Users on the occurrence of the specified events.

Specific events may result in specific DCC behaviour, for example SMI update by the DCC. See Section 7.5.6.8 of the BAD for a list of DCC Alerts and the relevant process areas.

Device Alerts are generated by Devices in response to specific events. They are unsolicited, which means that are not generated in response to a Service Request. They are sent to the DCC, which DCC forwards to Users (Suppliers or Electricity Distributors).

This process area describes the Alerts that Users can receive. In the context of Devices Alerts, it describes how Users can configure their receipt by enabling or disabling them.

Device Alerts can be categorised as follows:

- ***Critical or Non-Critical***
  Critical Device Alerts cannot be disabled through configuration. Critical Device Alerts must also be signed by the Device before sending. Non-Critical Device Alerts may be configurable. (The majority are, but exceptions exist.)

- ***Mandated, Mandated-Conditional or Non-Mandated***
  Mandated Device Alerts are required by the SMETS. Mandated-Conditional Device Alerts refer to a group of Device Alerts where at least one Device Alert of that group must be supported by the Device. Non-Mandated Alerts are optional; the Device may or may not be set up to create and send that type of Device Alert.

- ***Require Encryption (or not)***
  Where a Device Alert contains Data which may be considered 'personal' in accordance with the Data Protection Act, that Device Alert must be encrypted before being sent by the Device, such that to read it, the recipient needs to decrypt it.

- ***Configurable (or not)***
  Only a sub-set of Non-Critical Device Alerts are configurable. Configurable Device Alerts can only be configured by either Supplier or Electricity Distributor. Although many Devices can be capable of sending Device Alerts, only Smart Meters can have alert behaviour configured by a Service Request.

- ***WAN Alert (or not)***
  Only a sub-set of Device Alerts are sent to the User (Supplier or Electricity Distributor) via the DCC. Other Device Alerts are generated and stored on the Device Security or Event Log(s) and displayed on the Smart Meter's User Interface.

7.5.6.2 Scope

This process area includes:

- Configure Alert Behaviour

- Power Outage Alert

- PPMID related DCC Alerts

This process area involves but does not specifically describe Update Device Configuration (Billing Calendar). This process in described in more detail in Section 7.4.1.6.1 of the BAD.

7.5.6.3 Inputs

- ‘Configure Alert Behaviour’ Service Request (SRV 6.22)

7.5.6.4 Actors

- Supplier
- Network Operator
- Smart Meter
- CH
- PPMID

7.5.6.5 Process Description

7.5.6.5.1 Configure Device - Configure Alert Behaviour

The Supplier or Electricity Distributor composes a ‘Configure Alert Behaviour’ Service Request (SRV 6.22) and sends it to the DCC. This Service Request includes the list of Device Alerts to be configured, and whether they should be enabled or disabled. The process is described in Section 7.3.1.6.3 of the BAD.

7.5.6.5.2 Power Outage Alert

In the event of a loss of mains power to the CH for 3 minutes or more, the DCC sends a ‘Power Outage Event’ (AD1) DCC Alert to the following Users:

- Supplier; and
- Electricity Distributor, if an Electricity Smart Meter is Associated with the CH; or
- Gas Transporter, if a Gas Smart Meter is Associated with the CH.

In the event of a loss of mains power to the Polyphase Electricity Smart Meter, it sends the following Device Alerts to the DCC which the DCC sends to the Electricity Distributor:

- For phase 1, ‘Supply Interrupted on Phase 1’ (Alert Code: 0x8F58);
- For phase 2, ‘Supply Interrupted on Phase 2’ (Alert Code: 0x8F59);
- For phase 3, ‘Supply Interrupted on Phase 3’ (Alert Code: 0x8F5A).

7.5.6.5.3 PPMID Related Alerts

Where the DCC receives either of the following Device Alerts originating from the PPMID:

- 'Unauthorised Physical Access' (Alert Code: 0x8F3F)
- 'Unauthorised Physical Access - Other' (Alert Code: 0x8F78)

- ‘Unauthorised Communication Access attempted' (Alert Code: 0x8F3E)

the DCC sends a 'PPMID Alert' (N39) DCC Alert to the Import Supplier (registered against the Primary Electricity Smart Meter) and the Gas Supplier.

7.5.6.5.4 Update Device Configuration (Billing Calendar)

To create a Billing Calendar, the Supplier composes an ‘Update Device Configuration (Billing Calendar)’ Service Request (Service Reference Variant 6.8) and sends it to the DCC. The process for setting up and operating Billing Calendars is described in Section 7.4.1.6.1 of the BAD.

7.5.6.6 Associated Process Areas

#	Process Areas
7.1.1	Manage Inventory
7.1.2	CPA / CPL
7.2.1	Install and Commission
7.2.3	Post Commissioning Obligations
7.5.2	Change of Tenant
7.5.3	Manage Firmware
7.6.1	Replace Communications Hub
7.6.2	Remove and Decommission Devices
7.7.1	Transitional Change of Supplier
7.8.5	Error Processing

7.5.6.7 Governance

Actor	SEC Document	Clause	Text
7.5.6 Manage Alerts			
DCC	SEC Appendix AB - Service Request Processing Document	15.1	Where the DCC receives an Alert from a Communications Hub Function, the DCC shall Digitally Sign the Alert, and send it as a DCC Alert to (as specified in the DCC User Interface Specification) the Responsible Supplier(s), the Electricity Distributor and/or the Gas Transporter for the Smart Metering Systems of which the Communications Hub Function forms part (as identified in the Registration Data). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	15.2	Where the DCC receives from a Device either a Response that is destined for a Remote Party or an Alert which is destined for one or more Remote Parties and/or Supplementary Remote Parties, then the DCC shall send the Response (as a Service Response) or the Alert (as a DCC Alert or Device Alert) to those Remote Parties and/or Supplementary Remote Parties as prescribed by the DCC User Interface Specification. https://smartenergycodecompany.co.uk/download/2271

Actor	SEC Document	Clause	Text
DCC	SEC Appendix AB - Service Request Processing Document	15.4	Where the DCC receives a Response or an Alert from a Device which is destined for an Unknown Remote Party, the DCC shall: (a) Check Cryptographic Protection for the Response or Alert; (b) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Response or Alert; and (c) subject to (a) and (b) being successful, send the Response (as a Service Response) or the Alert (as a Device Alert or DCC Alert) to the recipient(s) identified in the Response or Alert. https://smartenergycodecompany.co.uk/download/2271
7.5.6.5.2 Power Outage Alert			
DCC	Smart Energy Code	Section F4.9	Where the DCC receives an Alert from a Communications Hub Function indicating that no power supply has been available to that Communications Hub Function for a period of at least three minutes, the DCC shall send a copy of the Alert to the Import Supplier (if any) and Electricity Distributor (if any) for that Communications Hub Function. https://smartenergycodecompany.co.uk/download/2476

7.5.6.8 DCC Alerts

The complete list of DCC alerts is available in the DUIS section 3.6.3.4

7.5.7 Manage Device

7.5.7.1 Introduction

There are a number of Service Requests that support Suppliers and Gas Transporters in operating Devices via the DCC. These Service Requests do not fit naturally into any specific business process, but rather exist to resolve specific operational problems.

Clear Event Log – Allows the Supplier to clear the Event Log on the Electricity Smart Meter, Gas Smart Meter or GPF. This process can only be used to clear the Event Log, the Security Log cannot be cleared in this way.

Synchronise Clock – Smart Meters, CH and other Devices need to maintain accurate time, both because it is a SEC requirement (see the SMETS & CHTS) and because it is needed for normal operations, such as ToU tariffs on Meters. The Meter and other Devices on the HAN get their time from the CH, which in turn gets its time from the DCC. This process of time synchronisation first occurs when Devices are Commissioned. CHs synchronise their time with the Network Time when they are Commissioned, while Smart Meters synchronise their time with the Associated CH when they are Commissioned. Smart Meters then synchronise their time with the CH time not more than

once every 24 hours. Where the mechanism breaks down, the Supplier will need to prompt the Smart Meter to synchronise itself with the CH by sending a Service Request.

Record Network Data (Gas) – The Gas Transporter may wish to read Consumption Data for analysis. This information is held in the Network Data Log on the Gas Smart Meter, a log capable of storing four hours of UTC date and time stamped six-minute Consumption Data arranged as a circular buffer. The Gas Smart Meter has to be instructed to start populating the Data Log, using a Service Request, before any attempt to read the Data can be successful.

7.5.7.2 Scope

This process area includes:

- Clear Event Log
- Synchronise Clock
- Record Network Data (Gas)

7.5.7.3 Inputs

- 'Clear Event Log' Service Request (SRV 3.3)
- 'Synchronise Clock' Service Request (SRV 6.11)
- 'Record Network Data (Gas)' Service Request (SRV 14.1)

7.5.7.4 Actors

- Supplier
- Gas Transporter
- DCC
- CHF
- GPF
- Smart Meter

7.5.7.5 Process Description

7.5.7.5.1 Clear Event Log

The Supplier composes a 'Clear Event Log' Service Request (SRV 3.3) and sends it to the DCC. If the Electricity Smart Meter is the target Device, the Service Request specifies whether the Electricity Smart Meter Event Log or the ALCS Event Log is to be cleared.

The DCC receives the Service Request, completes Non-Critical Service Request processing and, depending upon the target Device, sends a 'Clear Electricity Smart Meter Event Log' (ECS15a), 'Clear ALCS Event Log' (ECS15c) or a 'Clear ZigBee Device Event Log' (CS11) Command to the Device.

The Device receives the Command from the DCC, executes it by clearing its Event Log, and sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 3.3) to the Supplier.

7.5.7.5.2 Synchronise Clock

The CH reports to the Smart Meter that it does not have a valid time. The Smart Meter sends a 'Clock not adjusted (adjustment greater than 10 seconds)' (Alert Code: 0x8F0C) Device Alert to the DCC, which the DCC forwards to the Supplier.

The Supplier may also be made aware of the lack of time synchronisation between the Smart Meter and the CH through the receipt of a time-stamped Response within a Service Response, such as one containing instantaneous register readings. Timestamps in such Responses contain the Smart Meter's time status and its current time, at the point of sending the Response. A time status other than 'reliable', or a time value materially different than that expected, indicates issues.

At this point the Supplier does not know whether the problem lies with the Smart Meter, CH, or elsewhere in the network. The Supplier may check for Incidents related to that CH on the SSI, along with the status of such Incidents to check if and when such issues have been cleared and whether they have addressed the Smart Meter Clock issues.

The Supplier may attempt to resolve the problem by synchronising the CH time with the Smart Meter time. To do so, the Supplier composes a 'Synchronise Clock' Service Request (SRV 6.11) and sends it to the DCC. The Service Request includes both the current date time and the tolerance period.

The DCC receive the Service Request, completes Critical Service Request processing, and sends a 'Set Clock' (ECS70 / GCS28) Command to the Smart Meter.

The Smart Meter receives the Command and executes it by requesting the CH time from the CH. If the CH returns time to the Smart Meter:

- Where the time returned by the CH falls between the tolerance specified in the Service Request, the Smart Meter adopts the time provided by the CH and sets its Time Status to 'Reliable';

- Where the time returned by the CH falls outside the tolerance specified in the Service Request, the Meter's time remains unchanged and its time status is set to 'Unreliable' or remains 'Unreliable'; or

- Where the CH does not respond, or returns the value indicating it does not have accurate time, the Smart Meter's time and Time Status remains unchanged.

The Smart Meter sends a Response to the DCC, including its current time and Time Status. The DCC receives the Response and sends a Service Response (SRV 6.11) to the Supplier.

If the Service Response indicates that the Meter Time Status is 'Unreliable', this suggests a CH time issue. Resolving CH time issues is the responsibility of the DCC, and the Supplier needs to raise an Incident. For more detail see Section 7.9.4 of the BAD.

7.5.7.5.3 Record Network Data (Gas)

The Gas Transporter composes a 'Record Network Data (Gas)' Service Request (SRV 14.1) and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Start Network Data Log' (GCS31) Command to the Gas Smart Meter.

The Gas Smart Meter receives the Command, executes it by starting the Network Data Log, and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 14.1) to the Gas Transporter.

7.5.7.6 Associated Process Areas

#	Process Areas
7.8.4	Service Request Processing
7.9.4	Manage Incidents

7.5.8 Manage Dual Band Communications Hub

7.5.8.1 Introduction

Dual band Communications Hubs form and maintain HANs at both 2.4GHz and sub-GHz frequencies. Unlike the 2.4GHz network, the Sub-GHz network supports "frequency agility", this is the ability of the network to dynamically change communications channel based on information from the operating environment, or via a service request (SR 6.29). The Sub-GHz radio is also required to meet regulated duty cycle limitations.

The DBCH stores a number of configurable data items on the CHF in order to control how the sub-GHz related features operate, these data items can be configured using the 6.28 service request.

Whenever the Dual Band CH performs a Sub-GHz related action, such as:

- A change in the Sub-Ghz configuration Parameters,
- Performing a channel Scan,
- Changing the current operating Channel; and
- Duty cycle related actions.

The supplier will receive an N54 Dual Band CH Sub GHz Alert, with the payload set to identify the action taken, as described in section 7.5.6.8

7.5.8.2 Scope

This process area includes:

- Set CHF Sub-GHz Configuration
- Request CHF Sub GHz Channel Scan

7.5.8.3 Inputs

- 'Set CHF Sub GHz Configuration' Service Request (SRV 6.28)
- 'Request CHF Sub GHz Channel Scan' Service Request (SRV 6.29)

7.5.8.4 Actors

- Supplier
- DCC
- CHF – Dual Band Only

7.5.8.5 Process Description

7.5.8.5.1 Set CHF Sub GHz Configuration

A dual band communications hub may require the Sub-GHz configuration settings, regarding available channels and duty cycle, to be configured. To achieve this the supplier may compose a "Set CHF Sub GHz Configuration" SR, 6.28. This service request sets configuration values such as, Sub-GHz channel masks, Duty cycle thresholds and scan trigger parameters, for further information refer to GBCS section 10.6.

7.5.8.5.2 Request CHF Sub GHz Channel Scan

A DBCH is able to scan the available Sub-GHz channels to identify a channel with a lower interference level, allowing the DBCH to subsequently change to the quieter channel. A channel scan may be triggered either locally due to environmental factors or via the "Request CHF Sub GHz Channel Scan" Service Request (SRV 6.29), refer to GBCS section 10.6 for further information regarding triggering a channel scan.

7.5.8.6 Associated Process Areas

#	Process Areas
7.2.1	Install and commission
7.2.2.	Install and leave
7.6.1	Replace Communications Hub.

7.6 Decommission and Replace

This functional area describes how replacement or decommissioning of Devices forming part of SMSs is managed via the DCC. If a Device other than the CH is removed from a premises and replaced, the process for replacing it follows the same processes described in Section 7.2.1 or 7.2.2 of the BAD, depending on WAN availability on installation. The replacement of a CH follows a slightly different process. This process does not require the Lead Supplier to add Devices to the CHF Device Log one by one. Instead, the CHF and GPF Device Log of the CH that has been replaced can be replicated on the newly installed CH. The processes facilitating CH removal and replacement are described in Section 7.6.1 of the BAD. The processes supporting the removal and decommissioning of Devices other than the CH are described in Section 7.6.2 of the BAD.

7.6.1 Replace Communications Hub

7.6.1.1 Introduction

This process area describes how to manage replacement of CHs forming part of an Enrolled SMS via the DCC. The circumstances under which this may take place include but are not limited to equipment failure. Suppliers are not required to read any Data or unjoin Devices from the GPF as part of this process. Nonetheless, it is understood if that is possible some Suppliers may wish to do so. Therefore, these processes are mentioned here.

7.6.1.2 Scope

This process area includes:

- Restore HAN Device Log
- Restore GPF Device Log

This process area involves but does not specifically describe:

- Read (Device). This is described in Section 7.4.1.6.2 of the BAD.
- Clear Event Log. This is described in Section 7.5.1.5.1 of the BAD.
- Unjoin Service - Unjoin GPF. This is described in Section 7.6.2.5.3 of the BAD.
- Install Communications Hub. This is described in Section 7.2.1.6.4 of the BAD.
- Join Service – Join Gas Smart Meter to GPF. This is described in Section 7.2.1.6.12 of the BAD.
- Decommission Device – Decommission CH. This is described in Section 7.6.2.5.5 of the BAD.
- Communications Hub Status Update – Fault Return and No Fault Return. This is described in Section 7.9.1.6.2 of the BAD.
- Post Commissioning Obligations. This is described in Section 7.2.3 of the BAD.

7.6.1.3 Inputs

- 'Restore HAN Device Log' Service Request (SRV 8.12.1)
- 'Restore GPF Device Log' Service Request (SRV 8.12.2)

7.6.1.4 Actors

- Supplier
- DCC
- CH
- Smart Meter
- CHF
- GPF
- PPMID
- IHD
- Installer

7.6.1.5 Prerequisites

- The CH that is being replaced and new CH are on the SMI;
- Both the CHF and GPF of the CH that is being replaced have a SMI Status 'Commissioned';
- Both the new CHF and GPF have a SMI Status of 'Pending'.

7.6.1.6 Process Description

7.6.1.6.1 Read (Device)

Prior to the CH replacement, the Supplier may choose to read Data on the Device if the CH is working. For example, the Supplier may compose a 'Read Active Import Profile Data' Service Request (SRV 4.8.1) and send it to the DCC. This process is detailed in Section 7.4.1.6.2 of the BAD.

If the CH forms part of more than one SMS and one of the SMS is a Gas SMS, the Gas Supplier may need to be notified before such replacement to enable it to read Data on the GPF. There is currently no mechanism in the SEC for the Gas Supplier to be notified before replacement.

7.6.1.6.2 Clear Event Log

The Gas Supplier may choose to clear the Event Log on the GPF, provided that the CH is working and the Gas Supplier is aware that the CH is due to be replaced. To do so the Gas Supplier composes a

'Clear Event Log' Service Request (SRV 3.3), and sends it to the DCC. This process is described in more detail in Section 7.5.7.5.1 of the BAD.

7.6.1.6.3 Unjoin Service – Unjoin GPF

Both Import Supplier and Gas Supplier can unjoin the Gas Smart Meter from the GPF, while only the Gas Supplier can unjoin the GPF from the PPMID, and the GPF from the IHD. To unjoin a Device from the GPF, the Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2). This process is described in more detail in Section 7.6.2.5.3 of the BAD.

7.6.1.6.4 Install Communications Hub

The Installer physically removes the existing CH, installs the replacement and powers it on. For further detail on this process, see Section 7.2.1.6.4 of the BAD. If the Communications Hub being replaced is Dual Band, the supplier may wish to read the Sub-GHz Configuration parameters and the current Sub-GHz Channel, from the old CH, if it is operational, using SR 6.30 "Read CHF Sub-GHz Configuration" and SR6.31 "Read CHF Sub-GHz Channel" respectively.

If the Sub-GHz configuration from the old CH is required in the new, the supplier should configure the sub-GHz configuration in the new CH using SR 6.28, prior to restoring the HAN device log.

7.6.1.6.5 Restore HAN Device Log

The Supplier composes a 'Restore HAN Device Log ' Service Request (SRV 8.12.1), to replicate the CHF Device Log from the removed CH on to the CHF Device Log of the replacement CH, and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request Processing, and sends a 'Restore CHF Device Log (CCS03)' Command to the CHF.

The CHF receives the Command, executes it by updating the CHF Device Log, and sends a Response to the DCC.

The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.12.1) to the Supplier; and
- Sends Other Suppliers a 'CHF Device Log Restored' (N30) DCC Alert.

Following successful execution of the Command, the CHF configures its HAN identifier to match the replaced CH's. Each Device then detects the HAN and requests to join it. The CHF receives the request from the Device and Authenticates the Device to join the HAN using the credentials from the previous network. The CHF and Device effect the join between the two Devices using the mechanisms described in GBCS and the CHF sends a 'Device Addition To / Removal From HAN Whitelist Alerts' CS14 (Alert Code 0x8F12) with an updated Device Log to the DCC.

When the Gas Smart Meter or Electricity Smart Meter joins, the Smart Meter sends a 'Device joined SMHAN' (Alert Code:0x8183) Device Alert to the DCC. The DCC forwards the Device Alert to the person whose Organisation Certificate is populated in the Supplier's Trust Anchor Cells.

7.6.1.6.6 Restore GPF Device Log

The Supplier composes a 'Restore GPF Device Log ' Service Request (SRV 8.12.2), to replicate the GPF Device Log from the removed CH on to the new GPF Device Log of the replacement CH, and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing, and sends a 'Restore GPF Device Log' (GCS59) Command to the GPF.

The GPF receives the Command, executes it by updating its Device Log, and sends a Response to the DCC.

The DCC receives the Response from GPF and sends a Service Response (SRV 8.12.2) to the Supplier.

If the sender of the Service Request is not the Gas Supplier, the DCC sends a 'GPF Device Log Restored' (N31) DCC Alert to the Gas Supplier.

7.6.1.6.7 Join Service – Join Gas Smart Meter to GPF

If the replaced CH was part of a gas SMS, the GPF of the replaced CH would have been typically joined to one (or more) Devices on the HAN (Gas Smart Meter and PPMID or IHD). As the new GPF has now been restored, it is now joined to the PPMID or IHD. However, the Gas Smart Meter is still joined to the GPF of the replaced CH. To ensure that the Gas Smart Meter and the new GPF communicate, the Supplier needs to join the Gas Smart Meter to the new GPF. However, first it needs to unjoin the Gas Smart Meter from the GPF. To unjoin the Gas Smart Meter from the replaced GPF, the Supplier composes a 'Unjoin Service (non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC. The process is described in Section 7.6.2.6.12 of the BAD. Once this process is complete, the Supplier needs to join the Gas Smart Meter to the new GPF. To do that the Supplier composes a 'Join Service (non-Critical)' Service Request (SRV 8.7.2) and sends it to the DCC. This process is described in more detail in Section 7.2.1 of the BAD.

The Supplier is required to re-send any TOM commands (as defined in GBCS section 10.3.4) previously sent to the GSME when connected to the old communications Hub to repopulate the TOM related GPF data items in the new Communications Hub. The supplier may also need to send the 'Restrict Access for Change of Tenancy' Service Request (SRV 3.2) if previously sent to the old Communications Hub, refer to section 7.5.2.5.1 for details.

7.6.1.6.8 Decommission Device – Decommission CH

To Decommission the replaced CH, the Supplier composes a 'Decommission Device' Service Request (SRV 8.3) and sends it to the DCC. This process is described in more detail in Section 7.6.2.5.5 of the BAD.

The DCC sets the SMI Status of other Devices forming part of the SMS to 'Decommissioned' if the replacement CH is not Commissioned within a reasonable period.

7.6.1.6.9 Communications Hub Status Update – Fault Return and No Fault Return

The Installer physically returns the replaced CH to the Supplier. The Supplier receives the CH and returns it to the DCC. This process is described in more detail in Section 7.9.1.6.2 of the BAD.

7.6.1.6.10 Post Commissioning Obligations

The Post Commissioning Obligations in relation to the replacement CH need to be fulfilled by the DCC and Supplier. For more information, please see Section 7.2.3 of the BAD.

7.6.1.7 Commentary

Send 'GPF Device Log Restored (N31)' Alert (if Gas Supplier)

There is an inconsistency between SEC Appendix AB - Service Request Processing Document and SEC Appendix AD - DCC User Interface Specification as to who should receive this DCC Alert. The SEC Appendix AB - Service Request Processing Document states that the Gas Supplier should receive it unless the Gas Supplier sent the 'Restore GPF Device Log' Service Request (SRV 8.12.2), while Appendix AD - DCC User Interface Specification states that all Responsible Suppliers (except for the Responsible Supplier who sent the Service Request) should receive it. This inconsistency is planned to be resolved through a Modification Proposal.

7.6.1.8 Associated Process Areas

#	Process Areas
7.1.1	Manage Inventory
7.2.1	Install and Commission
7.2.2	Install and Leave
7.2.3	Post Commissioning Obligations
7.4.1	Read
7.5.7	Manage Device
7.6.2	Remove and Decommission Devices
7.9.1	Order and Return Communications Hub

7.6.1.9 Governance

Actor	SEC Document	Clause	Text
7.6.1.6.5 Restore HAN Device Log			
Supplier	SEC Appendix AB - Service Request Processing Document	10.2	An Import Supplier shall not send a Service Request to add or remove a Gas Proxy Function to or from the Device Log of a Gas Smart Meter other than as part of managing the replacement of a Communications Hub (by it or another Responsible Supplier) pursuant to Clause 10.1. https://smartenergycodecompany.co.uk/download/2271
Supplier	SEC Appendix AB - Service Request Processing Document	10.1(a)	Where a Supplier Party replaces a Communications Hub in a premise then that Supplier Party must, as soon as reasonable practicable after the replacement, send the necessary Service Requests to the DCC to ensure that: the Device Log of the new Communications Hub Function replicates that of the old Communications Hub Function; https://smartenergycodecompany.co.uk/download/2271

DCC	SEC Appendix AB - Service Request Processing Document	10.4	The DCC shall, where it has processed a Service Request which successfully replaces the Device Log of a Communications Hub Function, send a DCC Alert to all Responsible Suppliers for that Communications Hub Function (other than the Responsible Supplier which sent the original Service Request) notifying them of the replacement. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.6.3.4	For the purposes of **Error! Reference source not found.** the Registered ED is the Electricity Distributor and the Registered GT is the Gas Transporter for the relevant Smart Metering System or Device. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.6.3.4	**DCC Alert Codes** https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	8.2	Where DCC receives a 'Restore HAN Device Log' or 'Restore Gas Proxy Function Device Log' Service Request, the DCC shall use the up-to-date electronic record referred to in Clause 8.1 in relation to the relevant Device for the purposes of determining the information to be used to restore the Device Log of the relevant Device. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	8.3	Where a Communications Hub is replaced and the Communications Hub Function and Gas Proxy Function that comprise the replacement Communications Hub are Commissioned, such Devices shall (for the avoidance of doubt) be considered to be newly Commissioned and any provisions of the Code which require steps to be taken by any Party in relation to a newly Commissioned Device shall apply. https://smartenergycodecompany.co.uk/download/2275
7.6.1.6.6 Restore GPF Device Log			
Supplier to DCC	SEC Appendix AB - Service Request Processing Document	10.1(b)	Where a Supplier Party replaces a Communications Hub in a premises then that Supplier Party must, as soon as reasonable practicable after the replacement, send the necessary Service Requests to the DCC to ensure that: (b) the Device Log of the new Gas Proxy Function is replaced with that of the old Gas Proxy Function (or replicates that of the old Gas Proxy Function); https://smartenergycodecompany.co.uk/download/2271

DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	8.2	Where DCC receives a 'Restore HAN Device Log' or 'Restore Gas Proxy Function Device Log' Service Request, the DCC shall use the up-to-date electronic record referred to in Clause 8.1 in relation to the relevant Device for the purposes of determining the information to be used to restore the Device Log of the relevant Device. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AB - Service Request Processing Document	10.5	The DCC shall, where it has processed a Service Request to successfully replace the Device Log of a Gas Proxy Function, send a DCC Alert to the Gas Supplier who is the Responsible Supplier for that Gas Proxy Function (save where it is the Gas Supplier that has sent the Service Request). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.6.3.4	Trigger - Upon successful completion of Service Request 8.12.2 Restore GPF Device Log if the sender is not the registered GS. DCC Alert Recipient - All Responsible Suppliers for the CHF, other than the IS / GS that submitted the Request https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.6.3.4	Trigger - Upon successful completion of Service Request 8.12.2 Restore GPF Device Log if the sender is not the registered GS. DCC Alert Recipient - All Responsible Suppliers for the CHF, other than the IS / GS that submitted the Request https://smartenergycodecompany.co.uk/download/4639
7.6.1.6.7 Join Service – Join Gas Smart Meter to GPF			
DCC	SEC Appendix AB - Service Request Processing Document	10.1(c)	Where a Supplier Party replaces a Communications Hub in a premises then that Supplier Party must, as soon as reasonable practicable after the replacement, send the necessary Service Requests to the DCC to ensure that: (c) following steps (a) and (b) above, the new Gas Proxy Function is added to the Device Log of the Gas Smart Meter; and https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	10.2	An Import Supplier shall not send a Service Request to add or remove a Gas Proxy Function to or from the Device Log of a Gas Smart Meter other than as part of managing the replacement of a Communications Hub (by it or another Responsible Supplier) pursuant to Clause 10.1. https://smartenergycodecompany.co.uk/download/2271
7.6.1.6.8 Decommission Device – Decommission CH			

Supplier	Smart Energy Code	Section F8.3	Each Supplier Party that: (a) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, is entitled to remove that Communications Hub from the premises at which it is installed (but must install a replacement Communications Hub unless the Communications Hub Function is Withdrawn); (b) Decommissions a Communications Hub Function, shall remove the Communications Hub of which the Communications Hub Function forms part from the premises at which it is installed; and (c) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, may also be obliged under another provision of this Code to remove a Communications Hub, including where it is obliged to do so in accordance with the Incident Management Policy or the CH Support Materials. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.4	Where a Supplier Party removes a Communications Hub from a premises, it shall do so in accordance with the CH Installation and Maintenance Support Materials https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.5	Where a Communications Hub is removed by a Supplier Party from a premises at which it was previously installed, then the risk of loss or destruction of or damage to that Communications Hub shall vest in that Supplier Party as set out in Section F7.4(a) (Risk in the Communications Hubs following Installation). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section H6.6	On the Decommissioning of a Communications Hub Function, the other Devices forming part of a Smart Metering System should also be Decommissioned; provided that the Devices forming part of a Smart Metering System (other than the Gas Proxy Function) may remain Commissioned notwithstanding the Decommissioning of the Communications Hub Function if a replacement Communications Hub Function is Commissioned within a reasonable period. https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AB - Service Request Processing Document	10.1(d)	Where a Supplier Party replaces a Communications Hub in a premises then that Supplier Party must, as soon as reasonable practicable after the replacement, send the necessary Service Requests to the DCC to ensure that: (d) following the step set out in (c) above, the Communications Hub Function and the Gas Proxy Function comprising the Communications Hub that has

			been replaced are decommissioned (through the sending of a 'Decommission Device' Service Request). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	10.3	The DCC shall, following the decommissioning of a Communications Hub Function and the associated Gas Proxy Function (arising as a consequence of the processing of a 'Decommission Device' Service Request), send a DCC Alert to all Responsible Suppliers and Network Parties for Smart Metering Systems which incorporated either or both of those Devices, notifying them of the decommissioning (other than to the Responsible Supplier which sent the 'Decommission Device' Service Request). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5(a)	Upon successful execution of a *DecommissionDevice* Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions. a) Where the existing Device status is not one of 'Decommissioned', 'Pending' or 'Withdrawn', update the Smart Metering Inventory and set the Device's SMI Status of the DeviceId to 'Decommissioned'. Note that this allows for an update where the SMI Status is 'Recovery' https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5(a)	Upon successful execution of a *DecommissionDevice* Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions. a) Where the existing Device status is not one of 'Decommissioned', 'Pending' or 'Withdrawn', update the Smart Metering Inventory and set the Device's SMI Status of the DeviceId to 'Decommissioned'. Note that this allows for an update where the SMI Status is 'Recovery' https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5(c)	Where the relevant Device specified within the Service Request is a Communication Hub Function, set the Device's SMI Status of the associated Gas Proxy Function to 'Decommissioned' https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface	3.8.100.5(c)	Where the relevant Device specified within the Service Request is a Communication Hub Function, set the Device's SMI Status of the associated Gas Proxy Function to 'Decommissioned' https://smartenergycodecompany.co.uk/download/4639

	Specification v2.0		
DCC	SEC Appendix AD - DCC User Interface Specification	3.8.92.5(d)	Generate DCC Alerts N1, N2 or N9 to notify specified Users of the Device decommissioning as per DCC Alert definitions clause 3.6.3.4 https://smartenergycodecompany.co.uk/download/4639
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5(d)	Generate DCC Alerts N1, N2 or N9 to notify specified Users of the Device decommissioning as per DCC Alert definitions clause 3.6.3.4 https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification	3.8.92.5(f)	Where the Device Type is a Communication Hub Function, delete all DCC Schedules held for the associated Gas Proxy Function and send a DCC Alert N6 to the DCC Schedule owner. https://smartenergycodecompany.co.uk/download/4639
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5(f)	Where the Device Type is a Communication Hub Function, delete all DCC Schedules held for the associated Gas Proxy Function and send a DCC Alert N6 to the DCC Schedule owner. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification	3.8.92.5(h)	For all Device Types of Communication Hub Function also delete all Future Dated (DSP) requests for the associated Gas Proxy Function with future dated execution dates that have not been sent to the Device and send a DCC Alert (N34) to the original sender of the request https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5(h)	For all Device Types of Communication Hub Function also delete all Future Dated (DSP) requests for the associated Gas Proxy Function with future dated execution dates that have not been sent to the Device and send a DCC Alert (N34) to the original sender of the request https://smartenergycodecompany.co.uk/download/4639

7.6.2 Remove and Decommission Device

7.6.2.1 Introduction

This process area describes how Suppliers unjoin Devices and Decommission Devices (other than Type 2 Devices) via the DCC. It also describes how Users can unjoin CADs via the DCC.

The primary reason for Decommissioning is that the Device is not working, but there may be other reasons e.g. product recall.

There is no SEC obligation to unjoin Devices before removing and Decommissioning them. However, it is recognised that some Suppliers may choose to do so if the Device to be unjoined is working as it may not be possible to join a replacement Device until space has been freed in the Device Log of other Devices on the HAN. Therefore, this process is described here.

Suppliers have obligations under the Data Protection Act to safeguard customer's Personal Data. In this context, that is primarily the Consumption Data held on the Electricity Smart Meter and GPF. Removing the Gas Smart Meter from the CHF Device Log has the effect of clearing Data considered as personal, and we describe this process here.

There is not a prescribed sequence of steps such as the physical removal of Devices, Decommissioning and the installation of replacement Devices (if required). The processes described in this process area assume the following sequence: Suppliers remove the Device, install replacement (if required) and Decommission it afterwards.

7.6.2.2 Scope

This process area includes:

- Unjoin Service
- Update HAN Device Log - Remove Device
- Decommission Device

This process area involves but does not specifically describe:

- Read (Device). This is described in Section 7.4.1.6.2 of the BAD.
- Clear Event Log. This is described in Section 7.5.7.5.1 of the BAD.
- Install and Commission or Install and Leave. This is described in Section 7.2.1 or 7.2.2 of the BAD.

This process area excludes disposal or re-use of Devices.

7.6.2.3 Inputs

- 'Decommission Device' Service Request (SRV 8.3)
- 'Unjoin Service (Critical)' Service Request (SRV 8.8.1)
- 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2)
- 'Update HAN Device Log' Service Request (SRV 8.11)

7.6.2.4 Actors

- Supplier
- DCC
- Other User
- CH
- Smart Meter
- Installer

7.6.2.5 Process Description

7.6.2.5.1 Read (Device)

The Supplier decides to remove a Device. To identify the Devices joined to the Device to be removed, the Supplier may compose a 'Read Device Log' Service Request (SRV 8.9) and send it to the DCC. This process is detailed in Section 7.4.1.6.2 of the BAD.

The Supplier may also obtain this information from reading the SMI. This process is also detailed on Section 7.4.1.6.3 of the BAD.

7.6.2.5.2 Clear Event Log

The Supplier may choose to clear the Event Log on the Device (Electricity Smart Meter, GPF or Gas Smart Meter). To do so, the Supplier composes a 'Clear Event Log' Service Request (SRV 3.3) and sends it to the DCC. This process is described in Section 7.5.7.5.1 of the BAD.

7.6.2.5.3 Unjoin Service

The Supplier unjoins the Smart Meter from the Devices identified in the Smart Meter's Device Log.

Unjoin Electricity Smart Meter from PPMID

The Import Supplier composes an 'Unjoin Service (Critical)' Service Request (SRV 8.8.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing, and sends a 'Method A or C Unjoin' (CS04AC) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command, executes it by removing the PPMID's Device ID from its Device Log and sends a Response to the DCC. The DCC receives it, and does the following things:

- Sends a Service Response (SRV 8.8.1) to the Import Supplier; and
- Terminates the Association between the PPMID and Electricity Smart Meter in the SMI.

Unjoin Electricity Smart Meter from IHD

The Import Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing, and sends a 'Method B Unjoin' (CS04B) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command, executes it by removing the IHD's Device ID from its Device Log, and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.2) to the Import Supplier; and
- Terminates the Association between the Electricity Smart Meter and IHD in the SMI.

Unjoin HCALCS from Electricity Smart Meter

The Import Supplier composes an 'Unjoin Service (Critical)' Service Request (SRV 8.8.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing, and sends a 'Method A or C Unjoin' (CS04AC) Command to the HCALCS.

The HCALCS receives the Command, executes it by removing the Electricity Smart Meter's Device ID from its Device Log and sends a Response to the DCC.

The DCC receives the Response and sends a Service Response (SRV 8.8.1) to the Import Supplier.

Unjoin PPMID from Electricity Smart Meter

The Import Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (Service Request Variant 8.8.2) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Method A or C Unjoin' (CS04AC) Command to the PPMID.

The PPMID receives the Command, executes it by removing the Electricity Smart Meter's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 8.8.2) to the Import Supplier.

Unjoin Gas Smart Meter from PPMID

The Gas Supplier composes an 'Unjoin Service (Critical)' Service Request (SRV 8.8.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends a 'Method A or C Unjoin' (CS04AC) Command to the Gas Smart Meter.

The Gas Smart Meter receives the Command, executes it by removing the PPMID's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.1) to the Gas Supplier; and
- Terminates Association between the Gas Smart Meter and the PPMID in the SMI.

Unjoin Gas Smart Meter from GPF

The Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method B Unjoin' (CS04B) Command to the Gas Smart Meter.

The Gas Smart Meter receives the Command, executes it by removing the GPF's Device ID from its Device Log and sends a Response to the DCC.

The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.2) to the Supplier, and
- Terminates the Association between the Gas Smart Meter and the GPF in the SMI.

Unjoin PPMID from Gas Smart Meter

The Gas Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (Service Request Variant 8.8.2) and sends it to the DCC.

The DCC receives it, completes Non-Critical Service Request processing and sends a 'Method A or C Unjoin' (CS04AC) Command to the PPMID.

The PPMID receives the Command, executes it by removing the Gas Smart Meter's Device ID from its Device Log, and sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 8.8.2) to the Gas Supplier.

Unjoin GPF from PPMID

The Gas Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Method B Unjoin' (CS04B) Command to the GPF.

The GPF receives the Command, executes it by removing the PPMID's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.2) to the Gas Supplier; and
- Terminates the Association between the PPMID and the GPF in the SMI.

Unjoin Electricity Smart Meter from PPMID

The Import Supplier composes an 'Unjoin Service (Critical)' Service Request (SRV 8.8.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends a 'Method A or C Unjoin' (CS04AC) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command, executes it by removing the PPMID's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.1) to the Import Supplier; and
- Terminates the Association between the PPMID and the Electricity Smart Meter in the SMI.

Unjoin GPF from IHD

The Gas Supplier composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Method B Unjoin' (CS04B) Command to the GPF.

The GPF receives the Command, executes it by removing the IHD's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.2) to the Gas Supplier; and
- Terminates the Association between the IHD and the GPF in the SMI.

7.6.2.5.4 Update HAN Device Log - Remove Device

The Supplier composes an 'Update HAN Device Log' Service Request (SRV 8.11) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Remove Device from CHF Device Log' (CCS02) Command to the CHF.

The CHF receives the Command, executes it by removing the Device's Device ID from the CHF Device Log, and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Where a Supplier removed a PPMID which was joined to both an Electricity Smart Meter and a Gas Smart Meter, the DCC sends a 'PPMID Removal' (N43) DCC Alert to all Responsible Suppliers for the CHF other than the Supplier that submitted the Service Request (Service Reverence Variant 8.11).
- Sends a Service Response (SRV 8.11) to the Supplier.

Removing the Gas Smart Meter from the CHF Device Log has the effect of clearing Data considered as personal in accordance with the Data Protection Act.

The Installer removes the Device. If required, the Installer replaces the Device and follows the process in Section 7.2.1 or Section 7.2.2 of the BAD, depending on WAN availability.

7.6.2.5.5 Decommission Device

The Supplier Decommissions the Device. To do that, the Supplier composes a 'Decommission Device' Service Request (SRV 8.3) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Device Service Request processing, and does the following things:

- Changes the SMI Status of the Smart Meter or Type 1 Device to 'Decommissioned';
- Terminates the Association between the Device and other Devices forming part of the SMS in the SMI;
- For Smart Meters, deletes schedules held against the Smart Meter, and sends a 'Schedule removal because of Device decommission' (N6) DCC Alert to each User that created a schedule for the Smart Meter;
- For Smart Meters and HCALCS, cancels all Future Dated Service Requests not yet sent to the Smart Meter or HCALCS, and sends a 'Cancellation of Future Dated Response Pattern (DSP) requests because of Device Decommission' (N33) DCC Alert to each User that sent a Future Dated Service Request for the Smart Meter or HCALCS to the DCC;
- For Smart Meters, terminates the Association between the Smart Meter and the MPxN in the SMI;
- For Electricity Smart Meter, sends an 'Electricity Smart Meter Decommission or withdrawal' (N1) DCC Alert to the Electricity Distributor and, if applicable, the Export Supplier;
- For Gas Smart Meter, sends a 'Gas Smart Meter Decommission or withdrawal' (N2) DCC Alert to the Gas Transporter;
- For CH, sends a 'Communications Hub Decommission' (N9) DCC Alert; and
- Sends the Service Response (SRV 8.3) to the Supplier.

Type 2 Devices cannot be Decommissioned via the DCC.

No Service Requests can be scheduled for HCALCS, and hence no such DCC Alert is triggered by Decommissioning an HCALCS. No Service Requests for PPMID can be future dated or scheduled, and hence no such DCC Alerts are triggered by Decommissioning a PPMID.

7.6.2.5.6 Install and Commission or Install and Leave

If a Device requires replacement, the Supplier follows either Install and Commission or Install and Leave processes. They are described in Section 7.2.1 and 7.2.2 of the BAD respectively.

7.6.2.5.7 Remote CAD Unpairing

Unjoin Electricity Smart Meter from CAD

The User composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Method B Unjoin' (CS04B) Command to the Electricity Smart Meter.

The Electricity Smart Meter receives the Command, executes it by removing the CAD's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.2) to the User, and
- Terminates the Association between the Electricity Smart Meter and the CAD in the SMI.

Unjoin GPF from CAD

The Other User composes an 'Unjoin Service (Non-Critical)' Service Request (SRV 8.8.2) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Method B Unjoin' (CS04B) Command to the GPF.

The GPF receives the Command, executes it by removing the CAD's Device ID from its Device Log and sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 8.8.2) to the Other User; and
- Terminates the Association between the GPF and the CAD in the SMI.

Update HAN Device Log - Remove Device

The User composes an 'Update HAN Device Log' Service Request (SRV 8.11) and sends it to the DCC.

The DCC receives the Service Request, completes Non-Critical Service Request processing and sends a 'Remove Device from CHF Device Log' (CCS02) Command to the CHF.

The CHF receives the Command, executes it by removing the CAD's Device ID from the CHF Device Log, and sends a Response to the DCC. The DCC receives the Response and sends a Service Response (SRV 8.11) to the Other User.

7.6.2.6 Type 2 Devices cannot be Decommissioned via the DCC. Associated Process Areas

#	Process Areas
7.2.1	Install and Commission
7.2.2	Install and Leave
7.4.1	Read

7.5.7	Manage Device

7.6.2.7 Governance

Actor	SEC Document	Clause	Text
7.6.2.5.3 Unjoin Service			
DCC	SEC Appendix AB - Service Request Processing Document	11.2	Where the DCC receives a Response in respect of a Command sent to join or unjoin a Pre-Payment Meter Interface Device, the DCC shall send the Response (as a Service Response) to the User that sent the corresponding Service Request. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	6.1	In the case of any Device other than a Communications Hub Function or a Smart Meter, on the Successful Execution of an 'UnJoin Service' Service Request to remove the Device from the Device Log of a Smart Meter or Gas Proxy Function, the DCC shall terminate the Association between that Device and the applicable Smart Meter or Gas Proxy Function. https://smartenergycodecompany.co.uk/download/2275
7.6.2.5.4 Update HAN Device Log - Remove Device			
DCC	SEC Appendix AB - Service Request Processing Document	3.8.101.4	When a User requests the Request Type “Remove” variant of this Service Request 8.11, then the Command Response indicates whether the specified Device provided in the Service Request was either successfully removed from the CHF Device Log or the removal was unsuccessful. Upon receipt of a successful Response resulting from the UpdateHANDeviceLog Service Request to Remove a Device, the DCC shall, where the Device Status is currently ‘Whitelisted’, set the Device status to ‘Pending’. No additional DCC Alerts are produced by the DCC Systems. https://smartenergycodecompany.co.uk/download/2271
7.6.2.5.5 Decommission Device			
Supplier	Smart Energy Code	Section H6.1	Where a Device other than a Type 2 Device is no longer to form part of a Smart Metering System otherwise than due to its Withdrawal, then that Device should be Decommissioned. A Device may be Decommissioned because it has been uninstalled and/or is no longer operating (whether or not it has been replaced, and including where the Device has been lost, stolen or destroyed).

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2483
Supplier	Smart Energy Code	Section H6.2	Only the Responsible Supplier(s) for a Communications Hub Function, Smart Meter, Gas Proxy Function or Type 1 Device may Decommission such a Device. https://smartenergycodecompany.co.uk/download/2483
Supplier	Smart Energy Code	Section H6.3	Where a Responsible Supplier becomes aware that a Device has been uninstalled and/or is no longer operating (otherwise than due to its Withdrawal), that User shall send a Service Request requesting that it is Decommissioned https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AB - Service Request Processing Document	16.1(d)(i)	in the case of any Non-Device Service Request that changes or creates information held (or intended to be reflected) on the DCC Systems (including the Smart Metering Inventory), update the information held on DCC Systems accordingly; and/or https://smartenergycodecompany.co.uk/download/2271
DCC	Smart Energy Code	Section H6.4(a)	On successful processing of a Service Request from a Responsible Supplier in accordance with Section H6.3, the DCC shall: (a) set the SMI Status of the Device to 'decommissioned'; https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5(a)	Upon successful execution of a Decommission Device Service Request, the DCC shall, for the specified Device ID identified within the Service Request, perform the following actions. a) Where the existing Device status is not one of 'Decommissioned', 'Pending' or 'Withdrawn', update the Smart Metering Inventory and set the Device's SMI Status of the Device ID to 'Decommissioned'. Note that this allows for an update where the SMI Status is 'Recovery' https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User	3.8.100.5(a)	Upon successful execution of a Decommission Device Service Request, the DCC shall, for the specified Device ID identified within the Service Request, perform the following actions.

Actor	SEC Document	Clause	Text
	Interface Specification v2.0		a) Where the existing Device status is not one of 'Decommissioned', 'Pending' or 'Withdrawn', update the Smart Metering Inventory and set the Device's SMI Status of the Device ID to 'Decommissioned'. Note that this allows for an update where the SMI Status is 'Recovery' https://smartenergycodecompany.co.uk/download/4639
Supplier	Smart Energy Code	Section H6.4 (b)	On successful processing of a Service Request from a Responsible Supplier in accordance with Section H6.3, the DCC shall: (b) where relevant, amend the Smart Metering Inventory so that the Device is no longer Associated with any other Devices; and https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5 (b)	b) Where the relevant Device specified within the Service Request is a Gas Smart Meter or an Electricity Smart Meter, disassociate the Device from any MPAN or MPRN with which it is associated in the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5 (b)	Where the relevant Device specified within the Service Request is a Gas Smart Meter or an Electricity Smart Meter, disassociate the Device from any MPAN or MPRN with which it is associated in the Smart Metering Inventory https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AB - Service Request Processing Document	16.1(d)(vii)(B)	where the relevant Device is a Smart Meter, disassociate the Device in the Smart Metering Inventory from any MPRN or MPAN with which it is Associated; and https://smartenergycodecompany.co.uk/download/2271
Supplier	Smart Energy Code	Section H6.4(c)	On successful processing of a Service Request from a Responsible Supplier in accordance with Section H6.3, the DCC shall: (c) where the Device in question is a Communications Hub Function, notify any and all Responsible Suppliers (other than the Responsible Supplier that procured such Decommissioning) for that Communications Hub Function of such Decommissioning.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AC - Inventory Enrolment and Withdrawal Procedures	9.1	As soon as reasonably practicable following the Decommissioning, Withdrawal or Suspension of a Smart Meter, the DCC shall notify the Electricity Distributor or Gas Transporter for that Smart Meter of such Decommissioning, Withdrawal or Suspension, such notification to be made via the DCC User Interface. https://smartenergycodecompany.co.uk/download/2275
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5 (d)	Generate DCC Alerts N1, N2 or N9 to notify specified Users of the Device decommissioning as per DCC Alert definitions clause 3.6.3.4. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5 (d)	Generate DCC Alerts N1, N2 or N9 to notify specified Users of the Device decommissioning as per DCC Alert definitions clause 3.6.3.4. https://smartenergycodecompany.co.uk/download/4639
DCC	Smart Energy Code	Section H3.20	The DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services for which the Command has not yet been sent and which are due to be undertaken in respect of a Device after the Decommissioning or Suspension of that Device (and shall notify the relevant User of such cancellation via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5 (e)	Where the Device Type is a Device Type other than Communication Hub Function, delete all DCC Schedules held for the Device and send a DCC Alert N6 to the DCC Schedule owners. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5 (e)	Where the Device Type is a Device Type other than Communication Hub Function, delete all DCC Schedules held for the Device and send a DCC Alert N6 to the DCC Schedule owners. https://smartenergycodecompany.co.uk/download/4639

Actor	SEC Document	Clause	Text
DCC	Smart Energy Code	Section H3.20	The DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services for which the Command has not yet been sent and which are due to be undertaken in respect of a Device after the Decommissioning or Suspension of that Device (and shall notify the relevant User of such cancellation via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.92.5 (g)	For all Device Types other than Communication Hub Function, delete all Future Dated (DSP) requests with future dated execution dates that have not been sent to the Device and send a DCC Alert (N33) to the original sender of the request. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.100.5 (g)	For all Device Types other than Communication Hub Function, delete all Future Dated (DSP) requests with future dated execution dates that have not been sent to the Device and send a DCC Alert (N33) to the original sender of the request. https://smartenergycodecompany.co.uk/download/4639
DCC	Smart Energy Code	Section H6.6	On the Decommissioning of a Communications Hub Function, the other Devices forming part of a Smart Metering System should also be Decommissioned; provided that the Devices forming part of a Smart Metering System (other than the Gas Proxy Function) may remain Commissioned notwithstanding the Decommissioning of the Communications Hub Function if a replacement Communications Hub Function is Commissioned within a reasonable period. https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.93.5	Where a User wishes to decommission a Device and re-use the Device at another premise then the DCC Service User must not use the Update Inventory Service Request to perform this activity. Instead, a Service Request 8.3 Decommission Device (see clause 3.8.92) should be used to update the Device's SMI Status to 'Decommissioned' followed by a subsequent Service Request 12.2 Device Pre-notification (see clause 3.8.113) to update the Device's SMI Status to 'Pending'. The Device can then be commissioned as per normal process.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.101.5	Where a User wishes to decommission a Device and re-use the Device at another premise then the User must not use the Update Inventory Service Request to perform this activity. Instead, a Service Request 8.3 Decommission Device (see clause 3.8.100) should be used to update the Device's SMI Status to 'Decommissioned' followed by a subsequent Service Request 12.2 Device Pre-notification (see clause 3.8.122) to update the Device's SMI Status to 'Pending'. The Device can then be commissioned as per normal process. https://smartenergycodecompany.co.uk/download/4639
7.6.2.5.7 Remote CAD Unpairing			
User	Smart Energy Code	Section I1.3	Each User undertakes that it will not send either a 'Join Service' or 'Unjoin Service' Service Request (respectively to join a Type 2 Device to, or unjoin it from, any Smart Meter or Device Associated with a Smart Meter) unless: (a) the User is the Responsible Supplier for the Smart Meter or Associated Device to which the Service Request is sent, and sends that Service Request for the purpose of complying with an obligation under its Energy Supply Licence; or (b) the Energy Consumer at the premises at which the Smart Meter is located has given the User Unambiguous Consent, which has not been withdrawn, to (as the case may be): (i) join that Type 2 Device to the Smart Meter or Associated Device, and the User has clearly informed the Energy Consumer before obtaining such Unambiguous Consent that a consequence of joining the Type 2 Device may be that Data relating to the Energy Consumer will be shared with third parties; or (ii) unjoin it from the Smart Meter or Associated Device, save that the Responsible Supplier for a Smart Metering System at the premises need not obtain such Unambiguous Consent where it has reasonable grounds to believe that the Type 2 Device has Compromised or is likely to Compromise any Device forming part of that Smart Metering System (and the Responsible Supplier shall, where it unjoins a Type 2 Device in such circumstances, take all reasonable steps to inform the Energy Consumer that it has done so). https://smartenergycodecompany.co.uk/download/2486

7.7 Manage Security Credentials

The security of communications between Users and Devices via the DCC relies on the use of Device Security Credentials established under SMKI every time either of those entities is involved in a transaction.

There are two categories of Device Security Credentials:

- Device Certificates
- Organisation Certificates

At manufacture, Devices generate their Private Key Material, store corresponding Device Certificates and have a range of Organisation Certificates placed on them. The following Organisation Certificates are stored on the following Devices:

Table 11. Organisation Certificates stored on specific Devices

				Type of Device (✓= is required; empty = is not required)					
				Electricity Smart Meter	Gas Smart Meter	CH (CHF)	CH (GPF)	HCALCS	PPMID
			deviceType value(s)	1	0	2	3	4	5
	TrustAnchorCellIdentifier								
No	**remotePartyRole**	**keyUsage**	**cellUsage**						
1	Root	keyCertSign	Management	✓	✓	✓	✓	✓	✓
2	Recovery	digitalSignature	Management	✓	✓	✓	✓	✓	✓
3	Supplier	digitalSignature	Management	✓	✓		✓	✓	
4	Supplier	keyAgreement	Management	✓	✓		✓		
5	Supplier	keyAgreement	prePaymentTopUp	✓	✓				
6	networkOperator	digitalSignature	Management	✓			✓		
7	networkOperator	keyAgreement	Management	✓			✓		
8	accessControlBroker	digitalSignature	Management			✓			✓
9	accessControlBroker	keyAgreement	Management	✓	✓	✓	✓	✓	✓
10	transitionalCoS	digitalSignature	Management	✓	✓		✓	✓	
11	wanProvider	digitalSignature	Management			✓			

There are various points within the lifecycle of a Device where its Device Security Credentials require replacement. The events and associated processes that enable Device Security Credentials replacement via the DCC are described in this functional area and include:

- Before Smart Meters and HCALCS are Commissioned, the Supplier needs to ensure that its Organisation Certificates are populated in the Supplier's Trust Anchor Cells on the Devices. This may involve replacing the DCC's Organisation Certificates or Supplier's group Organisation Certificates.
- After Smart Meters and GPF are Commissioned, the Supplier needs to comply with Post Commissioning Obligations to regenerate and replace relevant Device's Security Credentials. The same obligation applies to the DCC in respect of CHs.
- At CoS, where the Losing Supplier's Organisation Certificates on Smart Meters, GPF and HCALCS need to be replaced by those of the Gaining Supplier.

- Periodic replacement of Organisation Certificates. Device Certificates may also be periodically replaced but this is not a requirement.
- After Private Key Material has been compromised and an SMKI Recovery has been invoked.

This functional area also describes the processes for obtaining and retrieving Organisation and Device Certificates from the DCC.

7.7.1 Transitional Change of Supplier

7.7.1.1 Introduction

This process area describes the process for transferring of ability to operate a SMS from one Supplier (the Losing Supplier) to another (the Gaining Supplier) following a CoS event.

In the context of smart metering, this process involves the replacement of Organisation Certificates on certain Devices forming part of that SMS. This process does not refer to any wider industry processes operated by the MRA or Xoserve.

This process area describes the transitional approach to CoS, which is triggered by the Gaining Supplier and requires the DCC to replace the Organisation Certificates. This process is expected to be superseded by the Enduring CoS process at a future date[19].

7.7.1.2 Scope

This process area includes Update Security Credentials (CoS).

This process area involves but does not specifically describe:

- Read (Device). This process is described in Section 7.4.1.6.2 of the BAD.
- Update Payment Mode. This process is described in Section 7.3.2.5.1 of the BAD.
- Read (Non-Device) - Read Inventory. This process is described in more detail in Section 7.4.1.6.3 of the BAD.
- Update Supplier Name. This process is described in Section 7.5.1.5.2 of the BAD.
- Configure Device. This process is described in Section 7.3.1.6.3 of the BAD.

This process area excludes:

- Business processes associated with Suppliers acquiring Energy Consumers;
- Financial reconciliation at the point an Energy Consumer switches Supplier; and

[19] Enduring Change of Supplier processes have been discussed, however SMIP has not taken any proposals forward and it is unknown currently if/when ECOS will be implemented. As a consequence, Supplier of Last Resort processes for changing Supplier Certificates may continue to rely on Transitional Change of Supplier processes.

- Updates to RDP Systems.

7.7.1.3 Inputs

- 'Update Security Credentials (CoS)' Service Request (SRV 6.23)

7.7.1.4 Actors

- Losing Supplier
- Gaining Supplier
- DCC - acting as both the DCC and the CoS Party
- Smart Meter
- HCALCS
- GPF

7.7.1.5 Process Description

The Losing Supplier will be made aware of the CoS event through current industry registration processes.

7.7.1.5.1 Read (Device)

In advance of the CoS date, the Losing Supplier may obtain profile data. To do that the Losing Supplier composes a 'Read Active Import Profile Data' Service Request (SRV 4.8.1) / 'Read Reactive Import Profile Data' Service Request (SRV 4.8.2) and sends it to the DCC. For more information see Section 7.4.1.6.3 of the BAD

7.7.1.5.2 Update Payment Mode

Where the Smart Meter is in Prepayment Mode, the Losing Supplier may update the Prepayment Mode to Credit, immediately prior to the CoS date[20]. The Supplier composes an 'Update Payment Mode' Service Request (SRV 1.6) and sends it to the DCC. For more information see Section 7.3.2.5.1 of the BAD.

7.7.1.5.3 Read (Non-Device) – Read Inventory

The Gaining Supplier looks up the SMI to check what Devices form part of the SMS they are due to gain. The Gaining Supplier may look up the SSI or compose a 'Read Inventory' Service Request (SRV 8.2) and send it to the DCC. For more information on the process see Section 7.4.1.6.3 of the BAD.

7.7.1.5.4 Update Security Credentials (CoS)

The Gaining Supplier composes an 'Update Security Credentials (CoS)' Service Request (SRV 6.23) to change the Supplier Organisation Certificates on each Device forming part of the SMS which require

[20] Whilst this requirement does not currently appear in the SEC it is an Ofgem supported initiative that will result in changes to relevant industry codes

Certificate change (Gas Smart Meter, Electricity Smart Meter, HCALCS and GPF) and sends it to the DCC. The Gaining Supplier sends one Service Request for each Device and each Organisation Certificates that require replacement.

The Organisation Certificate to be replaced depends upon the target Device:

- For an Electricity Smart Meter or Gas Smart Meter, a Digital Signing Organisation Certificate, a Key Agreement Organisation Certificate and a Prepayment Key Agreement Organisation Certificate;
- For a GPF, Digital Signing Organisation Certificate and a Key Agreement Organisation Certificate; or
- For an HCALCS, a Digital Signing Organisation Certificate.

The DCC receives the Service Request and applies checks to it.

If any of the checks fail, the DCC rejects the Service Request and notifies the Gaining Supplier of such rejection.

If the checks are successful, the DCC sends a Digitally Signed communication to the CoS Party.

The CoS Party receives the Digitally Signed communication from the DCC and applies the following checks:

- Checks Cryptographic Protection for both the communication and for the Service Request included within it;
- Confirms Validity of the Certificates used to Check Cryptographic Protection for both the communication and for the Service Request included within it;
- Confirms that User ID of the User who submitted the Service Request and the User ID contained within in each of the Organisation Certificates included within the Service Request are all associated with the same User; and
- Confirms that the User ID in each of the Organisation Certificates included within the Service Request is that of the Party who is identified via:
    - The relevant MPRN or MPAN (as applicable) included within the Service Request; and
    - The Registration Data for that relevant MPRN or MPAN

    as being the Party who is (or is to be) the Gaining Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

Where the Service Request fails any of these checks, the CoS Party does not undertake any further processing and notifies the DCC. The DCC sends an 'Update Security Credentials (CoS) – access control failure' (N26) DCC Alert to the Gaining Supplier.

If the checks are successful, the CoS Party then creates a Signed Pre-Command and sends it to the DCC.

The DCC receives the Signed Pre-Command and applies the following checks to it:

- Confirms that the User ID within each Organisation Certificate within the Signed Pre-Command is the same as the User ID within the corresponding Organisation Certificate in the original 'Update Security Credentials (CoS)' Service Request;
- Confirms that the Device ID within the Signed Pre-Command is the same as the Device ID included in the corresponding 'Update Security Credentials (CoS)' Service Request;
- Confirms that the message originated from the CoS Party by Checking the Cryptographic Protection for the message;
- Confirms Validity of the Certificate used to Check Cryptographic Protection for the message;
- Confirms Validity of all Certificates contained within the Signed Pre-Command; and
- Confirms that the User ID in each of the Organisation Certificates included within the Signed Pre-Command is that of the Party who is identified via:
    - The relevant MPRN or MPAN (as applicable) with which the Device specified in the Signed Pre-Command is associated in the Smart Metering Inventory; and
    - The Registration Data for that relevant MPRN or MPAN,

  as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

If the checks fail, the DCC rejects the Signed Pre-Command, and notifies the CoS Party and the Gaining Supplier of the rejection.

If the checks are successful, the DCC sends an 'Update Security Credentials' (CS02b) Command to the Device.

The Device receives the Command and executes it by:

- Replacing the Losing Supplier's Organisation Certificate held in the Supplier's Trust Anchor Cells with the Gaining Suppliers Organisation Certificate;
- For Smart Meters only, updating the Supplier name held on the Device to that of the Supplier in the replaced Organisational Certificate;
- For Smart Meters only, adding an entry in the Billing Data Log to record Meter readings at the CoS Event;
- For Smart Meters only, resetting the Tariff Block Counter Matrix;
- For Smart Meters only, changing the time on any future Update Security Credentials such that they never execute;

- For Smart Meters only, changing the time on any future Activate Firmware Commands such that they never execute;
- For Smart Meters only, reset any Counters and Floor values as defined in Service Request (SRV 6.23).

The Device sends a Response to the DCC. The DCC receives the Response and does the following things:

- Sends a Service Response (SRV 6.23) to the Gaining Supplier; and
- If the Response indicates success:
    - Sends the Losing Supplier a 'Device CoS' (N27) DCC Alert;
    - Cancels any schedules on the Device created by the Losing Supplier, and in respect of each schedule for the Device sends a 'Schedule removal because of CoS' (N17) DCC Alert to the Losing Supplier; and
    - Cancels any Future Dated Service Requests sent by the Losing Supplier for the Device and in respect of each Future Dated Service Request for the Device sends a 'Cancellation of Future Dated Response Pattern (DSP) requests because of CoS' (N38) DCC Alert to the Losing Supplier.

The Gaining Supplier can now operate the Device. Immediately following this, the Gaining Supplier would be expected to update its contact details on the Meter and Configure the Device.

7.7.1.5.5 Update Supplier Name

To ensure the Gaining Supplier's contact details are on the Smart Meter, the Gaining Supplier composes an 'Update Supplier Name' Service Request (SRV 3.4) and sends it to the DCC. For more details on the process see Section 7.5.1.5.2 of the BAD.

7.7.1.5.6 Configure Device

As a minimum, the Gaining Supplier is expected to update the price and tariff to match their quote to the Energy Consumer, and potentially reconfigure the Meter. The Gaining Supplier composes the required Service Requests and sends them to the DCC. For more information see Section 7.3.1.6.3 of the BAD.

7.7.1.6 Associated Process Areas

#	Process Areas
7.3.1	Configure Device
7.3.2	Prepayment
7.4.1	Read
7.5.1	Contact Customer

7.7.1.7 Governance

Actor	SEC Document	Clause	Text
7.7.1.5.4 Update Security Credentials (CoS)			
DCC	SEC Appendix AB - Service Request Processing Document	8.1 (a)	The following shall apply in respect of each 'CoS Update Security Credentials' Service Request: (a) where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the CoS Update Security Credentials Service Request to the CoS Party https://smartenergycodecompany.co.uk/download/2271
CoS Party	SEC Appendix AB - Service Request Processing Document	8.1 (b)	The following shall apply in respect of each 'CoS Update Security Credentials' Service Request: (b) Following receipt of the resulting communication, and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2, the CoS Party shall: (i) Check Cryptographic Protection for both the communication and for the Service Request included within it; (ii) Confirm Validity of the Certificates used to Check Cryptographic Protection for both the communication and for the Service Request included within it; (iii) confirm that User ID of the User who submitted the Service Request and the User ID contained within in each of the Organisation Certificates included within the Service Request are all associated with the same User; and (iv) confirm that the User ID in each of the Organisation Certificates included within the Service Request is that of the Party who is identified via: (A) the relevant MPRN or MPAN (as applicable) included within the Service Request; and (B) the Registration Data for that relevant MPRN or MPAN, as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date. https://smartenergycodecompany.co.uk/download/2271
CoS Party	SEC Appendix AB - Service Request Processing Document	8.2	Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are satisfied, the CoS Party shall: (a) generate the GBCS Payload of an 'Update Security Credentials' Signed Pre-Command that is substantively identical to the 'CoS Update Security Credentials' Service Request; (b) Digitally Sign the GBCS Payload; and (c) send the resultant communication as a Signed Pre-Command to the DCC. https://smartenergycodecompany.co.uk/download/2271

DCC	SEC Appendix AB - Service Request Processing Document	8.4	Where the DCC receives a Signed Pre-Command from the CoS Party, the DCC shall apply the following checks: (a) confirm that the User ID within each Organisation Certificate within the Signed Pre-Command is the same as the User ID within the corresponding Organisation Certificate in the original 'CoS Update Security Credentials' Service Request; (b) confirm that the Device ID within the Signed Pre-Command is the same as the Device ID included in the corresponding 'CoS Update Security Credentials' Service Request; (c) confirm that the message originated from the CoS Party by Checking the Cryptographic Protection for the message; (d) Confirm Validity of the Certificate used to Check Cryptographic Protection for the message; (e) Confirm Validity of all Certificates contained within the Signed Pre-Command; and (f) Confirm that the User ID in each of the Organisation Certificates included within the Signed Pre-Command is that of the Party who is identified via: (i) the relevant MPRN or MPAN (as applicable) with which the Device specified in the Signed Pre-Command is associated in the Smart Metering Inventory; and (ii) the Registration Data for that relevant MPRN or MPAN, as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date. https://smartenergycodecompany.co.uk/download/2271
CoS Party	SEC Appendix AB - Service Request Processing Document	8.3 (a)	Where, in respect of a communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are not satisfied: (a) the CoS Party shall not undertake any further processing of the communication, and shall notify the DCC; and https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	8.3 (b)	Where, in respect of a communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are not satisfied: (b) the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.74.4	Where UpdateSecurityCredentials(CoS) Service Request fails access control by the CoS Party, the DCC Systems shall generate DCC Alert N26 and send this DCC Alert to the original Service Request Sender. The Service Request shall not be processed any further by the DCC Systems. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix	3.8.75.4	Where UpdateSecurityCredentials(CoS) Service Request fails access control by the CoS Party, the DCC Systems shall

	AD - DCC User Interface Specification v2.0		generate DCC Alert N26 and send this DCC Alert to the original Service Request Sender. The Service Request shall not be processed any further by the DCC Systems. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AB - Service Request Processing Document	8.5	Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4 are satisfied in respect of a Signed Pre-Command received from the CoS Party, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	8.6	Where any of the checks in Clause 8.4 are not satisfied in respect of a Signed Pre-Command received from the CoS Party, the DCC shall: (a) not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Signed Pre-Command; (b) save where Clause 8.4(c) is not satisfied, notify the CoS Party of such rejection and of the reasons for such rejection; and (c) notify the User that sent the original 'CoS Update Security Credentials' Service Request. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.74.4 (a)	Upon successful execution of a UpdateSecurityCredentials(CoS) Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions: (a) Generate DCC Alert N27 to notify the old registered Import Supplier or Gas Supplier of the successful change of Security Credentials to support the CoS event. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.75.4 (a)	Upon successful execution of a UpdateSecurityCredentials(CoS) Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions: (a) Generate DCC Alert N27 to notify the old registered Import Supplier or Gas Supplier of the successful change of Security Credentials to support the CoS event. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.74.4 (b)	Upon successful execution of a UpdateSecurityCredentials(CoS) Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions. b) Delete all active DCC Schedules on that Device owned by the old registered Import Supplier will be automatically deleted by

			the DCC Systems. For each deleted DCC Schedule a DCC Alert N17 will be sent to the old registered Import Supplier. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.75.4 (b)	Upon successful execution of a UpdateSecurityCredentials(CoS) Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions. b) Delete all active DCC Schedules on that Device owned by the old registered Import Supplier will be automatically deleted by the DCC Systems. For each deleted DCC Schedule a DCC Alert N17 will be sent to the old registered Import Supplier. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.74.4 (c)	Upon successful execution of a UpdateSecurityCredentials(CoS) Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions. c) Cancel all Future Dated Response Pattern (DSP) requests for the specified Device submitted by the old registered Import Supplier not yet sent to the Device. For each cancelled Future Dated Response Pattern (DSP) Service Request a DCC Alert N38 will be sent to the old registered Import Supplier. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.754.4 (c)	Upon successful execution of a UpdateSecurityCredentials(CoS) Service Request, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following actions. c) Cancel all Future Dated Response Pattern (DSP) requests for the specified Device submitted by the old registered Import Supplier not yet sent to the Device. For each cancelled Future Dated Response Pattern (DSP) Service Request a DCC Alert N38 will be sent to the old registered Import Supplier. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AB - Service Request Processing Document	14.2	The DCC shall ensure that it sends each 'Update Security Credentials' Command resulting from a 'CoS Update Security Credentials' Service Request as close to the specified execution time as is reasonably practicable whilst still allowing time for the Command to be received and executed by the relevant Device. https://smartenergycodecompany.co.uk/download/2271

7.7.2 Manage Security Credentials

7.7.2.1 Introduction

This process area takes a lifecycle approach to managing Security Credentials and covers the following things:

- How Parties can become Authorised Subscribers for Device and Organisation Certificates;
- How Parties can obtain Device Certificates and Organisation Certificates from the DCC;
- How Organisation Certificates can be revoked; and
- Processes supporting the change of Device and Organisation Certificates on Devices via the DCC. This excludes the replacement of Organisation Certificates on CoS, as this process is described in Sections 7.7.1.5.4 of the BAD.

7.7.2.2 Scope

This process area includes:

- Become Authorised Subscriber (for a Device Certificate and Organisation Certificate)
- Obtain Organisation Certificate
- Obtain Device Certificate
- Revoke Organisation Certificate
- Request Handover of DCC Controlled Device
- Update Security Credentials (KRP)
- Issue Security Credentials
- Update Security Credentials (Device)

This process area involves but it does not specifically describe:

- Update Security Credentials (CoS). This process is described in more detail in Section 7.7.1.5.4 of the BAD.
- Read (Device) - Retrieve Device Security Credentials (both Device Certificate and Organisation Certificate). This process is described in more detail in Section 7.4.1.6.2 of the BAD.

This process area excludes:

- Generation of Private Key Material by the Device at manufacture
- Adding Organisation Certificates at manufacture

7.7.2.3 Inputs

- 'Update Security Credentials (KRP)' Service Request (SRV 6.15.1)
- 'Update Security Credentials (Device)' Service Request (SRV 6.15.2)
- 'Issue Security Credentials' Service Request (SRV 6.17)

- ‘Request Handover of DCC Controlled Device’ Service Request (SRV 6.21)

7.7.2.4 Actors

- DCC - as SMKI Registration Authority
- User - as Authorised Subscriber
- Supplier
- Network Operator
- Smart Meter
- GPF
- HCALCS

7.7.2.5 Process Description

7.7.2.5.1 Become Authorised Subscriber

To gain access to the SMKI Services, Parties must become Authorised Subscribers. To become an Authorised Subscriber, the Party needs first to nominate a Senior Responsible Officer (SRO) and at least one Authorised Responsible Officer (ARO).

The Party then submits a series of forms to the SMKI Registration Authority:

- A Company Information Form;
- A SRO Nomination Form; and
- An ARO Nomination Form.

A SRO can only be nominated by a Director or Company Secretary of that Party or of SECCO, RDP or in the case of DCC Service Provider personnel, the DCC.

The SMKI Registration Authority verifies the information provided and meets the individuals to confirm their identity. If successful, the SMKI Registration Authority adds the individuals to the list of ARO/ SRO and notifies the Party in writing.

Once the SRO and ARO are appointed, the Party submits an Authorised Subscriber Application Form. The SMKI Registration Authority verifies this, and, if successful, approves the Party as an Authorised Subscriber.

The SRO and ARO are provided with the means of accessing the SMKI Portal to request Organisation and Device Certificates and retrieve Device and Organisation Certificates from the SMKI Repository.

7.7.2.5.2 Obtain Organisation Certificate

The Authorised Subscriber accesses the SMKI Portal either via the DCC Gateway Connection or via the Internet. The Authorised Subscriber generates and submits a Certificate Signing Request (CSR) for the Organisation Certificate via the SMKI Portal to the DCC.

The DCC receives it, validates the format, verifies the Digital Signature, and if successful, accepts the CSR. The DCC notifies the Authorised Subscriber of acceptance or rejection via the SMKI Portal.

Following the acceptance of the Organisation CSR, the DCC verifies the content of the CSR, and notifies the Authorised Subscriber of approval or rejection via the SMKI Portal. In doing so the DCC will verify the content of the CSR, which includes checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the ARO submitting the CSR is authorised to submit CSRs (as per 2.6.1.3 of the Appendix M - SMKI Interface Design Specification).

The DCC issues the Organisation Certificate. The DCC lodges it in the SMKI Repository and makes it available for download via the SMKI Portal.

The Authorised Subscriber downloads the Organisational Certificate and checks it against the CSR. If there are inconsistencies, it rejects the Organisation Certificate and notifies the DCC through the DCC Service Desk.

The DCC investigates the inconsistency, and revokes the Organisation Certificate. The DCC places the revoked Organisation Certificate on the Organisation Certificate Revocation List held in the SMKI Repository.

7.7.2.5.3 Obtain Device Certificate

The Authorised Subscriber can submit a Device CSR in an Ad Hoc or Batched form for the Device Certificate via the SMKI Portal.

The Authorised Subscriber submits a Device CSR (Ad Hoc) / CSRs (Batched) for the Device Certificate via the SMKI Portal to the DCC. The Device CSR comes from a CS02c Response.

The DCC receives it, validates the format, verifies the Digital Signature, and if successful, accepts the CSR. The DCC notifies the Authorised Subscriber of acceptance or rejection via the SMKI Portal.

The DCC then verifies the content of the CSR, and checks that fewer than 100 Device Certificates have previously been issued for this Device ID. The DCC notifies the Authorised Subscriber of the approval or rejection via the SMKI Portal.

The DCC issues the Device Certificate. The DCC lodges it in the SMKI Repository and makes it available for download via the SMKI Portal for up to 30 days.

The Authorised Subscriber downloads the Device Certificate and checks it against the CSR. If there are inconsistencies, it rejects the Device Certificate and notifies the DCC through the DCC Service Desk.

The DCC investigates the inconsistency.

7.7.2.5.4 Revoke Organisation Certificates

Only certain Parties can request revocation of an Organisation Certificate. They are as follows:

- SMKI PMA Member on behalf of the SMKI PMA;

- An SRO on behalf of an Authorised Subscriber; or
- The SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel on behalf of the DCC.

They must do so by submitting a Certificate Revocation Request either in writing (via registered post), through a secure electronic means, or in person at the SMKI Registration Authority offices.

The request must include details of which certificate(s) are to be revoked, the reason why, and the identity of the person raising the Certificate Revocation Request.

The DCC validates the Certificate Revocation Request, and informs the SRO for the Authorised Subscriber whether the Certificate Revocation Request has been accepted or rejected.

If accepted, the DCC revokes the Certificate, and updates the Certificate Revocation List held in the SMKI Repository.

The DCC notifies the SRO for the Authorised Subscriber in writing that the Certificate has been revoked.

Once revoked Organisation Certificates cannot be restored.

It should be noted that the revocation of a Device Certificate is prohibited by the SMKI RAPP.

7.7.2.5.5 Request Handover of DCC Controlled Device

This process takes place under the following circumstances:

- Where the Supplier needs to replace the DCC Organisation Certificate with its own Organisation Certificate in the Supplier Trust Anchor Cell; and
- Where the Supplier needs to replace the DCC Organisation Certificate with the Network Operator Organisation Certificate in the Network Operator Trust Anchor Cell.

In the latter case, the Supplier needs to obtain the Network Operator Organisation Certificate (from the SMKI Repository).

The Service Request enables the Supplier to replace all Certificate types (Key Agreement and Digital Signing). However, if the replacement of each Certificate type were carried out using separate Service Requests, the replacement of Certificates would need to start with the replacement of the Key Agreement Certificate followed by the Digital Signing Certificate, as otherwise the Supplier's Digital Signature would not be valid for signing the Command to update the Key Agreement Certificate.

The Supplier composes a 'Request Handover of DCC Controlled Device' (SRV 6.21) Service Request, and sends it to the DCC. The DCC receives it, completes Non-Critical Service Request processing and sends an 'Update Security Credentials' (CS02b) Command to the Device.

The Device receives the Command, and does the following things:

- Completes Certification Path Validation and checks for certificate expiry;

- If the validation is successful, the Device replaces the Certificate; and
- Sends a Response to the DCC.

The DCC receives the Response, and does the following things:

- In the case of placing the Network Operator Organisation Certificate on the Device by the Supplier, if the validation is successful, sends a 'Security Credentials updated on the Device' (N42) DCC Alert to the Network Operator whose Certificate has been placed in the Device; and
- Sends a Service Response (SRV 6.21) to the Supplier.

This process may need to be repeated multiple times depending on the certificate types to be replaced and the Device.

7.7.2.5.6 Update Security Credentials (KRP)

This process takes place under the following circumstances:

- Where the Supplier / Network Operator needs to replace own Organisation Certificate in the Supplier/Network Operator Trust Anchor Cell; and
- Where the Supplier needs to replace own Organisation Certificate with the Network Operator Organisation in the Network Operator Trust Anchor Cell.

The Service Request enables the Supplier / Network Operator to replace all Certificate types (Key Agreement and Digital Signing). However, if the replacement of each Certificate type were carried out using separate Service Requests, the replacement of Certificates would need to start with the replacement of the Key Agreement Certificate followed by the Digital Signing Certificate, as otherwise the Supplier's / Network Operator's Digital Signature would not be valid for signing the Command to update the Key Agreement Certificate.

To do that, the Supplier / Network Operator composes an 'Update Security Credentials' Service Request (SRV 6.15.1) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing and sends an 'Update Security Credentials' (CS02b) Command to the Device.

The Device receives the Command, and does the following things:

- Completes Certification Path Validation and checks for certificate expiry;
- If the validation is successful, the Device replaces the Certificate; and
- Sends a Response to the DCC.

The DCC receives the Response, and does following things:

- In the case of placing the Network Operator Organisation Certificate on the Device by the Supplier, if the validation is successful, sends a 'Security Credentials updated on the Device'

(N42) DCC Alert to the Network Operator whose Organisation Certificate has been placed in the Device; and

- Sends Service Response (SRV 6.15.1) to the Supplier.

This process may need to be repeated multiple times depending on the certificate types to be replaced and the Device.

7.7.2.5.7 Issue Security Credentials

For Digital Signing and Key Agreement use, Smart Meters, CHF and GPF can generate new Public-Private Key Pairs and so issue a CSR, receive and store signed Device Certificates and provide a copy of the Device Certificate on request.

To regenerate the Device Key Agreement Private Keys, the Supplier sends an 'Issue Security Credentials' Service Request (SRV 6.17) to the DCC. The DCC receives it, completes Critical Service Request processing, and sends an 'Update Security Credentials' (CS02c) Command to the Device.

The Device receives the Command and does the following things:

- Generates a new Public-Private Key Pair (in this case, Key Agreement);
- Stores the new Private Key (in this case, the Key Agreement Private Key) in the Pending Private Key Trust Anchor Cell on the Device (in this case, the Pending Key Agreement Private Key Trust Anchor Cell);
- Creates a Device CSR;
- Creates a Response, that includes the Device CSR; and
- Sends the Response to the DCC. (The Device CSR in the Response is signed with the new Key Agreement Private Key, the CS02c Response itself is signed with the Device's current Digital Signing Private Key.)

The DCC receives the Response and sends a Service Response (SRV 6.17), and sends it to the Supplier.

7.7.2.5.8 Update Security Credentials (Device)

The Supplier downloads the Device Certificate from the SMKI Portal and creates an 'Update Security Credentials (Device)' Service Request (SRV 6.15.2) and sends it to the DCC.

The DCC receives the Service Request, completes Critical Service Request processing, and sends an 'Update Security Certificates on Device' (CS02d) Command to the Device.

The Device receives the Command and does the following things:

- Validates:
    - the Public Key contained within the Device Certificate against its Pending Key for the Certificate's Key Usage;

- The signature and MAC on the Command;
- That the required fields are present in the Certificate;
- That the Certificate contains the Device's serial number; and
- That the KeyUsage in the Certificate is permitted.

- If the validation checks are successful, stores the Device Certificate and sets the Current Private Key to have the value of the Private Key held in the Pending Private Key Cell (in this example, the current Key Agreement Private Key to have the value of the Key Agreement Private Key held in the Pending Key Agreement Private Key Trust Anchor Cell); and
- Sends a Response. (If the Command is Successfully Executed, the Response is signed by the Private Key corresponding to the replaced Device Certificate. If the Command failed to be executed, the Response is signed by the existing Private Key.)

The DCC receives the Response, and does the following things:

- If the Response indicates success, updates its systems to record which Device Certificates are currently in use by the Device; and
- Sends a Service Response (SRV 6.15.2) to the Supplier.

If the Response does not indicate success, the DCC sends a Service Response (SRV 6.15.2) to the Supplier.

The Supplier upon receipt of the Service Response (SRV 6.15.2) may update Device Certificate records for that Device in their own systems.

The process described above results in the Key Agreement Certificate being stored on the Device. The same process needs to be repeated such that the Digital Signing Certificate is stored on the Device too. The order in which the Certificates are stored is not important, but in the end both Certificates much be stored on the Device.

7.7.2.5.9 Update Security Credentials (CoS)

To trigger the process for updating the Supplier Organisation Certificates on Devices on CoS, the Gaining Supplier composes an 'Update Security Credentials (CoS)' Service Request (SRV 6.23) and sends it to the DCC. The process is described in more detail in Section 7.7.1.5.4 of the BAD.

7.7.2.5.10 Read (Device) - Retrieve Device and Organisation Security Credentials

A Supplier may wish to retrieve the current Device or Organisation Security Credentials. To do so they use a 'Retrieve Device Security Credentials (Device)' Service Request (SRV 6.24.2) or a 'Retrieve Device Security Credentials (KRP)' Service Request (SRV 6.24.1).

This process is described in Section 7.4.1.6.2 of the BAD.

7.7.2.6 Associated Process Areas

#	Process Areas
7.2.1	Install and Commission
7.2.2	Install and Leave
7.2.3	Post Commissioning Obligations
7.4.1	Read
7.7.1	Transitional Change of Supplier

7.7.2.7 Governance

Actor	SEC Document	Clause	Text
7.7.2.5.1 Become Authorised Subscriber			
Subscriber	Smart Energy Code	Section L3.2	For the purposes of this Section L3: (a) any Party which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of any of the Certificate Policies; (b) any RDP which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of the Organisation Certificate Policy; and (c) SECCo in respect of the IKI Certificate Policy, may apply to become an Authorised Subscriber in accordance with, and by following the relevant procedures set out in, that Certificate Policy and the SMKI RAPP. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L3.3	The DCC shall authorise SECCo, any Party or any RDP to submit a Certificate Signing Request, and so to become an Authorised Subscriber, where SECCo, that Party or that RDP has successfully completed the relevant procedures and satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L3.4	The DCC shall provide any SMKI Services that may be requested by an Authorised Subscriber where the request is made by that Authorised Subscriber in accordance with the applicable requirements of the SMKI SEC Documents. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L3.5	The DCC shall ensure that in the provision of the SMKI Services it acts in accordance with Good Industry Practice. https://smartenergycodecompany.co.uk/download/2503
7.7.2.5.2 Obtain Organisation Certificate			
Subscriber	Smart Energy Code	Section L11.1	Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate. https://smartenergycodecompany.co.uk/download/2503

Actor	SEC Document	Clause	Text
Subscriber	Smart Energy Code	Section L11.2	No Eligible Subscriber may make a Certificate Signing Request which contains: (a) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or (b) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.3	Each Eligible Subscriber shall ensure that either: (a) where appropriate, in the case of a Certificate Signing Request for the Issue of an IKI Certificate, that Certificate Signing Request has been generated using a Cryptographic Credential Token that was provided by the DCC to the Eligible Subscriber in accordance with the SMKI RAPP; or (b) in every other case, the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.4	No Eligible Subscriber may make a Certificate Signing Request for the Issue of: (a) a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate; (b) an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of the Root OCA Certificate to the extent to which it is expressly permitted in accordance with the Organisation Certificate Policy); or (c) an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.5	Where any Organisation Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall: (a) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

Actor	SEC Document	Clause	Text
			(b) if it identifies that the Certificate contains any information which is untrue or inaccurate: (i) reject that Certificate; and (ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and (c)where it does not reject the Certificate, become a Subscriber for that Certificate. https://smartenergycodecompany.co.uk/download/2503
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.3.1.1	Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they: a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.2	Following receipt by the DCC of an Organisation CSR, the DCC shall: a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10; and b) either accept, or reject the CSR; i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or ii. where the CSR is rejected, log an error and return an error message via the SMKI Portal interface to the Authorised Subscriber. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.3	Where an Organisation CSR is accepted, the DCC shall: a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and b) either approve the CSR for further processing or reject the CSR; i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors and reasons for the rejection of that CSR, where such errors shall be in accordance with “Response Status” table in Appendix A of this document. xii. If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with

Actor	SEC Document	Clause	Text
			a relevant Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.4	Where an Organisation CSR is approved by the DCC, the DCC shall: a) Issue a corresponding Organisation Certificate; b) lodge the resulting Organisation Certificate in the SMKI Repository; and c) make the Organisation Certificate available for download via the SMKI Portal interface via DCC Gateway Connection and the SMKI Repository. https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.3.1.5	Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.4 of the Code, establish that the information contained in the resulting Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR. xv. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in accordance with L11.4 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate. xvi. Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated CRL in the SMKI Repository in accordance with Appendix B of the Code. https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.6.1.1	Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they: a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design	2.6.1.2	Following receipt of an Organisation CSR, the DCC shall: a) validate the format, and verify the signature of the CSR in line with Appendix F of this document and PKCS#10; b) either accept, or reject the CSR:

Actor	SEC Document	Clause	Text
	Specification		i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or ii. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix A of this document, and return an error message via the SMKI Portal interface to the Authorised Subscriber. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.6.1.3	Where an Organisation CSR is accepted, the DCC shall: a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and b) either approve the CSR for further processing or reject the CSR; i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors, which shall be in accordance with "Response Status" table in Appendix A of this document, and reasons for the rejection of that CSR. xlviii. If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with a relevant Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.6.1.4	Where an Organisation CSR is approved by the DCC, the DCC shall: a) process the CSR; b) Issue a corresponding Organisation Certificate; c) lodge the resulting Organisation Certificate in the SMKI Repository; and d) make the Organisation Certificate available for download via the SMKI Portal interface via the Internet and the SMKI Repository. https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.6.1.5	Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.4 of the Code, establish that the information contained in the resulting Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR. li. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in

Actor	SEC Document	Clause	Text
			accordance with L11.4 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate. lii. Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated CRL in the SMKI Repository in accordance with Appendix B of the Code. https://smartenergycodecompany.co.uk/download/2348
7.7.2.5.3 Obtain Device Certificate			
Subscriber	Smart Energy Code	Section L11.1	Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.2	No Eligible Subscriber may make a Certificate Signing Request which contains: (a) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or (b) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.3	Each Eligible Subscriber shall ensure that either: (a) where appropriate, in the case of a Certificate Signing Request for the Issue of an IKI Certificate, that Certificate Signing Request has been generated using a Cryptographic Credential Token that was provided by the DCC to the Eligible Subscriber in accordance with the SMKI RAPP; or (b) in every other case, the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.4	No Eligible Subscriber may make a Certificate Signing Request for the Issue of: (a) a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate;

Actor	SEC Document	Clause	Text
			(b) an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of the Root OCA Certificate to the extent to which it is expressly permitted in accordance with the Organisation Certificate Policy); or (c) an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate. https://smartenergycodecompany.co.uk/download/2503
Subscriber	Smart Energy Code	Section L11.6	Where any Device Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall: (a) take reasonable steps to establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request; (b) if it identifies that the Certificate contains any information which is untrue or inaccurate: (i) reject that Certificate; and (ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and (c) where it does not reject the Certificate, become a Subscriber for that Certificate. https://smartenergycodecompany.co.uk/download/2503
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.3.1.6 and 2.6.1.6	A Device Certificate can be submitted through the SMKI Portal interface via DCC Gateway Connection in Ad Hoc CSR form or as a number in Batched CSR form. Authorised Subscribers wishing to be issued with a Device Certificate or Device Certificates shall ensure that they generate the relevant Device CSRs in line with Appendix F of this document, and Appendix A of the Code. b) Ad Hoc Device CSR submission - where the Authorised Subscriber wishes to submit an Ad Hoc Device CSR, the Authorised Subscriber shall paste the CSR into the Ad Hoc Device CSR form (as set out in the SMKI User Guide) and then submit it to the SMKI Portal interface; or c) Batched CSR submission - where the Authorised Subscriber wishes to submit a Batched CSR, the Authorised Subscriber shall: i. generate the relevant Device CSRs; and ii. create a .zip file containing the individual Device CSRs, formatted in line with Appendix F of this document, then upload and submit the .zip file using the Batched CSR web form (as set out in the SMKI User Guide) to the SMKI Portal interface.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.7 (a) and 2.6.1.7 (a)	Following receipt by the DCC of an Ad Hoc Device CSR or Batched CSR to the SMKI Portal via DCC Gateway Connection, the DCC shall: a) for an Ad Hoc Device CSR submission: i. validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10; ii. apply the Eligible Subscriber checks as set out in [Section L3.16] of the Code; and iii. either accept, or reject the CSR; and A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or B. where the CSR is rejected, log an error and return an error message that is in accordance with "Response Status" table in Appendix A of this document, via the SMKI Portal interface to the Authorised Subscriber; or https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.7 (b) and 2.6.1.7 (b)	Following receipt by the DCC of an Ad Hoc Device CSR or Batched CSR to the SMKI Portal via DCC Gateway Connection, the DCC shall: for a Batched CSR submission: i. validate that the structure of the submitted .zip file is in accordance with the format set out in Appendix F to this document; ii. validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000; A. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR) ; or B. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below; iii. either accept, or reject the Batched CSR and/or each constituent Device CSR, log relevant errors and return a synchronous response via the SMKI Portal interface to notify the Authorised Subscriber as to: A. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR; or B. where the Batched CSR is rejected, relevant error messages that are in accordance with "Response Status" table in Appendix C of this document. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface	2.3.1.8 (a) and 2.6.1.8	If a Device CSR is accepted, the DCC shall: a) for an Ad Hoc Device CSR submission: i. perform such additional checks as DCC determines is necessary on the Device CSR, which may include checking that

Actor	SEC Document	Clause	Text
	Design Specification	(a)	all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy; ii. check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates; iii. either approve, or reject the Device CSR; and A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or B. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix A of this document, and return an error message via the SMKI Portal interface to the Authorised Subscriber; or https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.8 (b) and 2.6.1.8 (b)	If a Device CSR is accepted, the DCC shall: b) for a Batched CSR submission: i. validate the format, and verify the signature of each Device CSR contained within the Batched CSR in line with Appendix F of this document and PKCS#10; ii. perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy; iii. apply the Eligible Subscriber checks as set out in [Section L3.16] of the Code; iv. check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates; v. either approve, or reject each Device CSR in the Batched CSR; and A. where the CSR is approved, include a notification in the Batched CSR response file, as set out in section 2.3.4.4d) of this document, to the Authorised Subscriber; or B. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix C of this document, and include an error notification in the Batched CSR response file, as set out in section 2.3.4.4d) of this document. v. Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the DCC's Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it. vi. vii. If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and resubmit the CSR. The

Actor	SEC Document	Clause	Text
			Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.3.1.9 and 2.6.1.9	Where a Device CSR is approved by the DCC, the DCC shall: a) Issue a corresponding Device Certificate; b) lodge the resulting Device Certificate in the SMKI Repository; and c) for Ad Hoc Device CSRs: i. make the corresponding Device Certificate, for up to 30 days following provision by the DCC, available for download via the 'certificate pickup' page on the SMKI Portal interface via DCC Gateway Connection (as set out in the SMKI User Guide) and the SMKI Repository; ix. In order to retrieve the Device Certificate, the Authorised Subscriber will establish a connection to the SMKI Portal interface via DCC Gateway Connection using the IKI Certificate Issued for the purposes of submitting Device CSRs and retrieving Device Certificates; or d) for Batched CSRs: i. make available, for up to 30 days following provision by the DCC, two files for download via the 'certificate pickup' page on the SMKI Portal interface, comprising: A. a .zip file containing the Certificates in Base64 encoded DER format resulting from successfully processed CSRs; and B. a .txt file containing a report showing the processed status of each CSR in the Batched CSR, including errors. x. In order to retrieve the response files (as set out above) which correspond with a Batched CSR submission, the Authorised Subscriber will establish a connection to the SMKI Portal interface via DCC Gateway Connection using the IKI Certificate Issued for the purposes of submitting Device CSRs and retrieving Device Certificates. https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.3.1.10 and 2.6.1.10	xi. Upon downloading the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.5, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR. xii. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.5 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.4.1.1	Authorised Subscribers wishing to be Issued with a Device Certificate via the Ad Hoc Device CSR Web Service interface shall ensure that they: a) generate a Device CSR in line with Appendix F of this document and Appendix A of the Code; and b) include the Device CSR in the XML format defined in the XML Schema set out in Appendix B of this document and submit the CSR via HTTP POST to the Ad Hoc Web Service interface. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.4.1.2	Following receipt of a Device CSR to the Ad Hoc Device CSR Web Service interface, the DCC shall: a) validate that the format of the XML document complies with the XML schema as set out in Appendix B of this document; b) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10; c) either accept, or reject the CSR; i. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.4.1.3	If a Device CSR is accepted, the DCC shall: a) check that at least one Key Agreement Certificate or Digital Signing Certificate has previously been Issued for the Device ID to which the Device CSR relates; b) check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates; c) either approve, or reject the Device CSR; and i. where the CSR is approved, return a notification of acceptance in the synchronous XML response, to the Authorised Subscriber's systems; or ii. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.4.1.4	Where a Device CSR submitted via the Ad Hoc Device CSR Web Service interface is approved, the DCC shall: a) Issue a corresponding Device Certificate; b) lodge the resulting Device Certificate in the SMKI Repository; and c) return the Device Certificate to the Authorised Subscriber, as set out in Appendix A to this document, in the synchronous XML response to the submission of the Device CSR via the Ad Hoc Device CSR Web Service interface. https://smartenergycodecompany.co.uk/download/2348

Actor	SEC Document	Clause	Text
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.4.1.5	Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.5, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR. xxiii. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.5 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.5.1.1	An Authorised Subscriber wishing to be Issued with Device Certificates in response to a Batched CSR submission via the Batched Device CSR Web Service interface shall ensure that it: a) generates each CSR to be contained within the Batched CSR in line with Appendix F of this document and Appendix A of the Code; b) include each Device CSR in the Batched CSR in the XML format defined in the XML Schema set out in Appendix E of this document; and c) submit the XML document containing the Batched CSR via HTTP POST to the Batched Web Service interface. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.5.1.2	On receipt of an XML document containing a Batched Device CSR to the Batched Device CSR Web Service interface from an Authorised Subscriber's system, the DCC shall: a) validate that the format of the XML document complies with the XML schema as set out in Appendix E of this document; b) validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000; i. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR) ; or ii. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below; c) either accept, or reject the Batched CSR, log relevant errors and return in the synchronous XML response to the Authorised Subscriber's systems, to notify the Authorised Subscriber as to: i. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR; ii. where the Batched CSR is rejected, relevant error messages; and iii. a Batched CSR identifier that can be used to retrieve the Batched CSR XML response file as set out in section 2.5.3.4 of this document.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.5.1.3	Upon acceptance of a Batched CSR as set out immediately above, the DCC shall: a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10; b) perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy; c) apply the Eligible Subscriber checks as set out in [Section L3.16] of the Code; d) check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates; e) either approve, or reject each Device CSR in the Batched CSR and include (where applicable) resulting Device Certificates, notifications and error messages in a Batched CSR XML response file that is separate from the synchronous response file described in section 2.5.3.2 of this document; and i. where the CSR is approved, include a notification in the Batched CSR XML response file, to the Authorised Subscriber; or ii. where the CSR is rejected, log an error and include an error notification in the Batched CSR XML response file. xxx. Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the DCC's Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it. xxxi. If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and resubmit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition. https://smartenergycodecompany.co.uk/download/2348
DCC	SEC Appendix M - SMKI Interface Design Specification	2.5.1.4	Where a Device CSR submitted via the Batched CSR Web Service interface is approved, the DCC shall: a) Issue a corresponding Device Certificate; b) lodge the resulting Device Certificate in the SMKI Repository; c) make the Device Certificate available to the Authorised Subscriber for download in the Batched CSR XML response

Actor	SEC Document	Clause	Text
			file, as described in section 2.5.3.3, Appendix D and Appendix E to this document; and d) generate files for download via the 'certificate pickup' page on the SMKI Portal interface, as set out in section 2.3.4.4 of this document. xxxiii. An Authorised Subscriber may, at any point up to 30 days following provision by the DCC, download the XML response file containing success and error information and Device Certificates Issued in response to Device CSRs in a Batched CSR, by: a) establishing a TLS mutual authentication session to the Batched Device CSR Web Service interface; and b) appending the Batched CSR identifier supplied in response to the Batched CSR submission to the URL as defined in the SMKI User Guide for the purposes of retrieving response XML files for Batched CSR submissions. https://smartenergycodecompany.co.uk/download/2348
Subscriber	SEC Appendix M - SMKI Interface Design Specification	2.5.1.5	Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.5, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR. xxxv. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.5 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate. https://smartenergycodecompany.co.uk/download/2348
7.7.2.5.4 Revoke Organisation Certificate			
Subscriber	SEC Appendix B - Organisation Certificate Policy	3.4.1	Provision is made in the SMKI RAPP in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation Request and verify that they are authorised to submit that request. https://smartenergycodecompany.co.uk/download/2311
Subscriber	SEC Appendix B - Organisation Certificate Policy	4.9.1	(A)A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate: (i) (subject to the provisions of the SMKI Recovery Procedure) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; or

Actor	SEC Document	Clause	Text
			(ii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate. (B)The OCA must revoke a Certificate upon: (i) (subject to the provisions of the SMKI Recovery Procedure) receiving a Certificate Revocation Request if the Certificate to which that request relates has been Authenticated in accordance with Part 3.4.1 of this Policy; or (ii) being directed to do so by the SMKI PMA. (C)The OCA must revoke a Certificate in relation to which it has not received a Certificate Revocation Request: (i) (subject to the provisions of the SMKI Recovery Procedure) where it becomes aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; (ii) where it has determined that the Subscriber for that Certificate does not continue to satisfy the criteria set out in this Policy and the SMKI RAPP for being an Authorised Subscriber; (iii) where it becomes aware that the Subscriber for that Certificate has ceased to be an Eligible Subscriber in respect of the Certificate. (D) In an extreme case, where it considers it necessary to do so for the purpose of preserving the integrity of the SMKI Services, the OCA may, on the receipt of a Certificate Revocation Request in relation to a Certificate which has not been Authenticated in accordance with Part 3.4.1 of this Policy, revoke that Certificate. (E) Where the OCA revokes a Certificate in accordance with paragraph (D) it shall notify the SMKI PMA and provide a statement of its reasons for the revocation. https://smartenergycodecompany.co.uk/download/2311
Subscriber	SEC Appendix B - Organisation Certificate Policy	4.9.2	(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Subscriber, and shall on doing so: (i) provide all the information specified in the SMKI RAPP (including all the information necessary for the Authentication of the Certificate); and (ii) specify its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1(A) of this Policy). (B) The SMKI PMA may direct the OCA to revoke a Certificate. (C) The OCA may elect to revoke a Certificate in accordance with Part 4.9.1(D) of this Policy https://smartenergycodecompany.co.uk/download/2311

Actor	SEC Document	Clause	Text
OCA	SEC Appendix B - Organisation Certificate Policy	4.9.3	(A) Provision is made in the SMKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request. (B) On receiving a Certificate Revocation Request, the OCA shall take reasonable steps to: (i) Authenticate the Subscriber making that request; (ii) Authenticate the Certificate to which the request relates; and (iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy. (C) Where the OCA, in accordance with Part 4.9.1(C) of this Policy, intends to revoke a Certificate in relation to which it has not received a Certificate Revocation Request, it shall use its best endeavours prior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation. (D) The OCA shall inform the Subscriber for a Certificate where that Certificate has been revoked. https://smartenergycodecompany.co.uk/download/2311
OCA	SEC Appendix B - Organisation Certificate Policy	4.9.5	(A) The OCA shall ensure that it processes all Certificate Revocation Requests promptly, and in any event in accordance with such time as is specified in the SMKI RAPP. https://smartenergycodecompany.co.uk/download/2311
DCC	SEC Appendix D - Smart Metering Key Infrastructure Registration Authority Policy and Procedures Organisation Certificate Policy	8.1	In line with the SMKI Device Certificate Policy, Device Certificates cannot be revoked. As a result: a) no organisation shall submit a Certificate Revocation Request (CRR) in respect of a Device Certificate; and b) the DCC shall not be obliged to maintain a Device Certificate Revocation List (CRL) Device Authority Revocation List (ARL). https://smartenergycodecompany.co.uk/download/2320
DCC	SEC Appendix D - Smart Metering Key Infrastructure	8.2.1	The DCC shall permit each of the following individuals to request the revocation of an Organisation Certificate, where the reasons for such revocation request must be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9 in Appendix B of the Code: a) Any SMKI PMA member, on behalf of the SMKI PMA; b) Any Senior Responsible Officer for a Subscriber for an Organisation

Actor	SEC Document	Clause	Text
	Registration Authority Policy and Procedures Organisation Certificate Policy		Certificate; or c) Any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, on behalf of the DCC. The DCC, in its role as SMKI Registration Authority, shall only accept CRRs through the following mechanisms (or a combination of such mechanisms): a) in writing, via registered post; b) via a secured electronic means; or c) in Person, at the offices of the SMKI Registration Authority, where the address of such offices shall be as set out on the DCC Website. The revocation of an Organisation Certificate shall be permanent and the SMKI Registration Authority shall ensure that no revoked Organisation Certificate may be reinstated. The DCC shall, each month, prepare and submit a report to the SMKI PMA regarding the number and nature of Organisation Certificate revocations. https://smartenergycodecompany.co.uk/download/2320
SRO	SEC Appendix D - Smart Metering Key Infrastructure Registration Authority Policy and Procedures Organisation Certificate Policy	8.3.1	A Senior Responsible Officer on behalf of a Party, RDP SECCo or the DCC (in its role as DCC Service Provider) may request the revocation of access credentials in respect of an Authorised Responsible Officer acting on behalf of that Party, RDP, SECCo or the DCC (as DCC Service Provider) or revocation of an IKI File Signing Certificate for which that Party, RDP, SECCo is an Authorised Subscriber, using the form as set out in Annex A (A7) and clearly identifying the credentials to be revoked. The permitted reasons for revocation of authentication credentials shall be as listed immediately below: a) An applicant wishes an IKI File Signing Certificate or the credentials of an ARO to be revoked. b) A Party, RDP, SECCo or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or SMKI Repository Services or ceases to become an Authorised Subscriber for Device Certificates or Organisation Certificates, or both, as appropriate. c) If there is a change to any of the information that was used to verify the identity of an ARO (but where the renewal or replacement of documents used to verify such identity, where the identity information remains the same, shall not constitute a change). d) A Party, RDP, DCC (as DCC Service Provider), or SECCo notifies the SMKI Registration Authority that it reasonably believes that the ARO is a threat to the security, integrity, or stability of the SMKI Services and/or SMKI Repository Services. e) The information on which the identity of an ARO was established is known, or is reasonably suspected, to be inaccurate. f) The authentication credentials issued to the ARO are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to an ARO is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

Actor	SEC Document	Clause	Text
			Where access credentials have been revoked and the Party, RDP, SECCo or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, SECCo or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form. https://smartenergycodecompany.co.uk/download/2320
Parties	SEC Appendix D - Smart Metering Key Infrastructure Registration Authority Policy and Procedures Organisation Certificate Policy	8.3.3	The following parties may request the revocation of authentication credentials in respect of SMKI Registration Authority Personnel, using the form referred to in Annex A (A7): a) Any SMKI PMA member, on behalf of the SMKI PMA; and b) Any member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority. The permitted reasons for revocation of authentication credentials shall be as listed immediately below: a) A SMKI Registration Authority Manager wishes the credentials of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel to be revoked b) A member of SMKI Registration Authority Personnel becomes ineligible to access SMKI Services and/or SMKI Repository Services. c) A member of SMKI Registration Authority Personnel fails to comply with Appendix A and Appendix B of the Code, or this SMKI RAPP. d) Any information used to verify the identity of a member of SMKI Registration Authority Personnel changes, the individual leaves the employment of the DCC, or moves within DCC to a role in which they are not entitled to access SMKI Services and/or SMKI Repository Services. e) A SMKI Registration Authority Manager becomes aware that the member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager is a potential threat to the security, integrity, or stability of the SMKI Services and/or SMKI Repository Services. f) The information on which the identity of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel was established is known, or is suspected, to be inaccurate. g) The authentication credentials issued to the member of SMKI Registration Authority Personnel are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to a member of SMKI Registration Authority Personnel is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times. https://smartenergycodecompany.co.uk/download/2320
7.7.2.5.5 Request Handover of DCC Controlled Device			
DCC	SEC Appendix	3.8.72.4	When the DCC receives a Response indicating Success from an Update Security Credentials command for all certificates and

Actor	SEC Document	Clause	Text
	AD - DCC User Interface Specification v1.1		where the Remote Party whose certificate has been placed on the Device is not the sender of the Service Request, the DCC shall send a DCC Alert N42 to each of the relevant User(s) whose certificate has been placed on the Device. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.73.4	When the DCC receives a Response indicating Success from an Update Security Credentials command for all certificates and where the Remote Party whose certificate has been placed on the Device is not the sender of the Service Request, the DCC shall send a DCC Alert N42 to each of the relevant User(s) whose certificate has been placed on the Device. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AB - Service Request Processing Document	15.3	Where the DCC successfully processes a Service Request to replace the Security Credentials of a User that are held on a Device, or to place a User's Security Credentials on to a Device, then (other than to the extent that the User is notified via a Service Response) the DCC shall send a DCC Alert to the relevant User informing it of the change. https://smartenergycodecompany.co.uk/download/2271
7.7.2.5.6 Update Security Credentials (KRP)			
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.65.4	When the DCC receives a Response indicating Success from an Update Security Credentials command for all certificates and where the Remote Party whose certificate has been placed on the Device is not the sender of the Service Request (or Root), the DCC shall send a DCC Alert N42 to each of the relevant User(s) whose certificate has been placed on the Device. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.66.4	When the DCC receives a Response indicating Success from an Update Security Credentials command for all certificates and where the Remote Party whose certificate has been placed on the Device is not the sender of the Service Request (or Root), the DCC shall send a DCC Alert N42 to each of the relevant User(s) whose certificate has been placed on the Device. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AB - Service Request Processing Document	15.3	Where the DCC successfully processes a Service Request to replace the Security Credentials of a User that are held on a Device, or to place a User's Security Credentials on to a Device, then (other than to the extent that the User is notified via a Service Response) the DCC shall send a DCC Alert to the relevant User informing it of the change.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2271
7.7.2.5.8 Update Security Credentials (Device)			
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.66.4	When the DCC receives a Response indicating Success from an Update Security Credentials (Device) the DCC Systems are updated to record which Device Certificates are currently in use by the Device. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.67.4	When the DCC receives a Response indicating Success from an Update Security Credentials (Device) the DCC Systems are updated to record which Device Certificates are currently in use by the Device. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AB - Service Request Processing Document	17.1	Where the Device Security Credentials of a Device erroneously include Data from one or more of a Party's Organisation Certificates, that Party shall cooperate with other Parties in order to rectify the position (including, were necessary, by sending Service Requests to update the Device Security Credentials) https://smartenergycodecompany.co.uk/download/2271

7.7.3 SMKI Recovery

7.7.3.1 Introduction

Over the lifetime of an Organisation Certificate, there may be cases where the Private Keys Material relating to that Organisation Certificate has been Compromised, or is thought to be Compromised. This process area describes how Authorised Subscribers can recover from such a Compromise or potential Compromise.

As part of the provision of the SMKI Services, the DCC plays a key role in managing the SMKI Recovery procedure.

This process area describes how the DCC manages the SMKI Recovery processes and the different mechanisms by which Users can recover from a Compromise.

The Recovery method used depends on which type of Private Key has been compromised and the nature of the compromise. The decision on which method to use depends on the Compromised Party, the DCC and the SMKI PMA.

The Recovery process comprises:

- Pre-recovery or preparation stage
- Recovery execution stage

- Post-recovery or closure stage

7.7.3.2 Scope

This process area includes:

- Recovery of Private Keys associated with Organisation Certificates by affected Subscribers
- Recovery of Private Keys associated with Organisation Certificates by the DCC installing ACB Certificates
- Recovery of Private Keys associated with Organisation Certificates by the DCC installing Organisation Certificates
- Recovery using Contingency Private Key
- Recovery of Contingency Private Key or the Contingency Symmetric Key
- Recovery of Recovery Private Key
- Recovery of Issuing OCA Private Key

This process area involves but does not specifically describe:

- Manage Incident. This process in described in Section 7.9.4.5.1 of the BAD.
- Set Anomaly Detection Threshold. This process is described in Section 7.8.2.5.1 of the BAD.
- Revoke Organisation Certificate. This process is described in Section 7.7.2.5.4 of the BAD.
- Obtain Organisation Certificate. This process is described in Section 7.7.2.5.2 of the BAD.
- Request Handover of DCC Controlled Device / Update Security Credentials (KRP). This process is described in Section 7.7.2.5.5 /7.7.2.5.6 of the BAD.

This process area excludes DCC testing of the Recovery procedures.

7.7.3.3 Actors

- DCC
- SMKI PMA
- Subscriber
- Supplier

7.7.3.4 Process Description

7.7.3.4.1 Manage Incident

The person who identifies a Compromise of a Private Key notifies the DCC. The DCC raises an Incident. For more details see Section 7.9.4.5.1 of the BAD.

As part of the incident management process, the DCC notifies the Authorised Subscriber associated with the Organisation Certificate containing the Private Key, and asks them to investigate.

If the Authorised Subscriber determines there has been no Compromise, the DCC closes the Incident.

If a Compromise is confirmed, the DCC informs any Responsible Supplier impacted by the Compromise, and proceeds to Recovery.

7.7.3.4.2 Recovery of Private Keys associated with Organisation Certificates by affected Subscribers (Method 1)

Pre-recovery

The Subscriber confirms Compromise. The Subscriber submits the following to the DCC:

- Certificate Revocation Requests for Organisation Certificates to the DCC, which revokes the compromised Certificates. For more detail see Section 7.7.2.5.4 of the BAD.
- Organisation Compromise Notification File (OCNF) containing details of the Compromise; and
- A request to temporarily change the ADTs that are required to support replacement of affected Organisation Certificates on Devices. This process is described in Section 7.8.3.5.1 of the BAD.

The DCC notifies the SMKI PMA of the Compromise and that the Subscriber wishes to recover from it using the method to which this section 7.7.3.4.2 relates. The DCC also notifies the Responsible Supplier if the Responsible Supplier is not the Authorised Subscriber.

Recovery

The DCC amends the ADT. This process is described in Section 7.8.2.5.1 of the BAD.

The Subscriber obtains new Organisational Certificates. This process is described in Section 7.7.2.5.2 of the BAD.

The User composes and sends an 'Update Security Credentials (KRP)' Service Requests (Service Reference Variant 6.15.1) to the DCC to replace the Organisation Certificates on the affected Devices. This process is described in Section 7.7.2.5.6 of the BAD. The User notifies the DCC of the success or failure of the changes.

Where the Subscriber is not the Responsible Supplier, the DCC informs the Responsible Supplier of any failures.

Post-recovery

The Subscriber submits a request to change the ADTs. This process in described in Section 7.8.2.5.1 of the BAD. The DCC amends the ADTs and notifies the SMKI PMA that recovery is complete.

7.7.3.4.3 Recovery of Private Keys associated with Organisation Certificates by the DCC installing ACB Certificates (Method 2)

Pre-recovery

The Subscriber confirms Compromise. The Subscriber submits the following to the DCC:

- Certificate Revocation Requests for Organisation Certificates to the DCC, which revokes the compromised Certificates. This is described in Section 7.7.2.5.4 of the BAD.
- OCNF containing details of the Compromise, and
- A request to temporarily change the ADTs that are required to support replacement of affected Organisation Certificates on Devices. This is described in Section 7.8.2.5.1 of the BAD.

The DCC does the following things:

- Notifies the SMKI PMA of the Compromise and that the Subscriber wishes to recover from it using the method to which this section 7.7.3.4.3 relates;
- Sets the SMI Status of the affected Devices to 'Recovery';[21]
- Notifies the relevant Network Operator of the affected Devices and that the Supplier wishes to recover using this method;
- Begins preparation for the Key Activation Ceremony if the use of the Recovery Private Key is likely to be needed.

The SMKI PMA confirms to the DCC the recovery method. The DCC notifies the Subscriber.

Recovery

The DCC amends the ADTs. This process in described in Section 7.8.2.5.1 of the BAD.

The DCC completes the Key Activation Ceremony for the Recovery Private Key.

The DCC sends Commands, digitally signed with the Recovery Private Key, to the affected Devices to replace the compromised Organisation Certificates with the DCC ACB Certificate on the affected Devices.

If the replacement is successful, the DCC does the following things:

- Sets the SMI status of the Device to 'Recovered'; and
- Sends a 'Recovery complete (ACB Credentials)' (N44) DCC Alert to the Supplier.

The Subscriber(s) obtain new Organisational Certificates. This process is described in Section 7.7.2.5.2 of the BAD.

[21] The SMI status of 'Recovery' means that further messages will not be sent to a Device.

The Supplier composes and sends a 'Request Handover of DCC Controlled Device'' Service Requests (Service Reference Variant 6.21) to the DCC to replace the Organisation Certificates on the affected Devices. This process in described in Section 7.7.2.5.5 of the BAD. It notifies the DCC of the success or failure of the changes.

If the DCC ACB Certificate replacement is successful, the DCC sets the SMI Status of the affected Device to that held before the Compromise.

Post-recovery

The Subscriber submits a request to change the ADTs. This process is described in Section 7.8.2.5.1 of the BAD. The DCC amends the ADTs and notifies the SMKI PMA that recovery is complete.

7.7.3.4.4 Recovery of Private Keys associated with Organisation Certificates by the DCC installing Organisation Certificates (Method 3)

Pre-recovery

The Subscriber confirms Compromise. The Subscriber submits the following to the DCC:

- Certificate Revocation Requests for Organisation Certificates to the DCC, which revokes the compromised Certificates. This process is described in Section 7.7.2.5.4 of the BAD.
- OCNF containing details of the Compromise, and
- A request to temporarily change the ADTs that are required to support replacement of affected Organisation Certificates on Devices. This process is described in Section 7.8.2.5.1 of the BAD.

The DCC does the following things:

- Notifies the SMKI PMA of the Compromise and that the Subscriber wishes to recover from it using the method to which this section 7.7.3.4.4 relates;
- Sets the SMI Status of the affected Devices to 'Recovery';
- If the Subscriber is not the Responsible Supplier, notifies the Responsible Supplier of the affected Devices and that the Subscriber wishes to recover using this method;
- Begins preparation for the Key Activation Ceremony if the use of the Recovery Private Key is likely to be needed.

The SMKI PMA confirms to the DCC the recovery method. The DCC notifies the Subscriber. The Subscriber identifies the Organisation Certificates to be replaced, and obtains new Organisation Certificates. This process is described in Section 7.7.2.5.2 of the BAD. The Subscriber notifies the DCC which Organisation Certificates should be placed on the affected Devices.

Recovery

The DCC amends the ADT. This process is described in Section 7.8.2.5.1 of the BAD.

The DCC completes the Key Activation Ceremony for the Recovery Private Key.

The DCC sends Commands, digitally signed with the Recovery Private Key, to the affected Devices to replace the compromised Organisation Certificates with the Organisation Certificate on the affected Devices. If the replacement is successful, the DCC does the following things:

- Sets the SMI Status of the affected Device to that held before the Compromise; and
- Sends a 'Recovery Complete' (N45) DCC Alert to Suppliers and Network Operator.

Post-recovery

The Subscriber submits a request to change the ADTs. This process is described Section 7.8.2.5.1 of the BAD. The DCC amends the ADTs and notifies the SMKI PMA that recovery is complete.

7.7.3.4.5 Recovery using Contingency Private Key

This method is used to recover from:

- Compromise of the Root OCA Private Key; or
- Where the use of the Recovery Private Key has been unsuccessful.

Pre-recovery

The DCC notifies the SMKI PMA and all affected Subscribers that recovery from the Compromise could require use of the Contingency Private Key.

The DCC begins preparation for the Key Activation Ceremony.

The SMKI PMA confirms to the DCC the recovery method. The DCC does the following things:

- Notifies the Subscriber;
- Revokes the Root OCA and Issuing OCA Certificates;
- Updates the Authority Revocation List (ARL) in the SMKI Repository and destroys the Compromised Private Keys; and
- Sets the SMI status of the affected Devices to 'Recovery'.

Recovery

The Subscriber submits a request to temporarily change the ADTs that are required to support replacement of affected Organisation Certificates on Devices. The DCC amends the ADTs. This process is described in Section 7.8.2.5.1 of the BAD.

The DCC completes the Key Activation Ceremony to generate the following keys:

- A new Contingency Symmetric Key;
- A new Contingency Key Pair;

- A new wrappedApexContingencyKey;
- A new Root OCA Key Pair; and
- A new Issuing OCA Key Pair.

The DCC generates a new Root OCA Certificate, embedding the new wrappedApexContingencyKey. The new Root OCA Certificate is Digitally Signed by the new Root OCA Private Key. The DCC generates a replacement Issuing OCA Certificate, signed by the new Root OCA Private Key.

The DCC stores the new Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.

The DCC completes a Key Activation Ceremony to activate the Contingency Private Key and the Contingency Symmetric Key.

The DCC sends Commands to all Devices, Digitally Signed using the Contingency Private Key and including the Contingency Symmetric Key to enable activation, to replace the following Certificates (depending upon the Device type):

- A new Root OCA Certificate;
- A replacement new DCC Transitional CoS Certificate;
- A replacement new Recovery Certificate;
- A replacement new DCC Access Control Broker Certificate;
- A replacement new DCC WAN Provider Certificate; and
- A new DCC ACB Certificate to be placed in each Supplier Device slot or Network Operator Device slot in the corresponding Device.

If the replacement is successful, the DCC does the following things:

- Sets the SMI Status of the Device to 'Recovered'; and
- Sends a 'Recovery complete (ACB Credentials)' (N44) DCC Alert to the Supplier.

Post-recovery

The Subscriber obtains new Organisational Certificates. This process is described in Section 7.7.2.5.2 of the BAD.

The Supplier composes and sends a 'Request Handover of DCC Controlled Device' Service Requests (SRV 6.21) to the DCC to replace the Organisation Certificates on the affected Devices. This process is described in Section 7.7.2.5.5 of the BAD. It notifies the DCC of the success or failure of the changes.

If the DCC ACB Certificate replacement is successful, the DCC sets the SMI Status of the affected Device to that held before the Compromise.

The Subscriber submits a request to change the ADTs. This process is described in Section 7.8.2.5.1 of the BAD. The DCC amends the ADTs and notifies the SMKI PMA that recovery is complete.

7.7.3.4.6 Recovery of Contingency Private Key or Contingency Symmetric Key

Pre-recovery

The DCC notifies the SMKI PMA and all affected Subscribers of a Compromise to the Contingency Private Key or Contingency Symmetric Key.

The DCC begins preparation for the Key Activation Ceremony.

The SMKI PMA confirms to the DCC the recovery method. The DCC notifies the Subscriber.

Recovery

The Subscriber submits a request to temporarily change the ADTs that are required to support replacement of affected Organisation Certificates on Devices. The DCC amends the ADTs. This process in described in Section 7.8.2.5.1 of the BAD.

The DCC completes the Key Activation Ceremony to generate the following keys:

- A new Contingency Symmetric Key;
- A new Contingency Key Pair;
- A new wrappedApexContingencyKey;
- A new Root OCA Key Pair; and
- A new Issuing OCA Key Pair.

The DCC generates a new Root OCA Certificate, embedding the new wrappedApexContingencyKey. The new Root OCA Certificate is Digitally Signed by the new Root OCA Private Key. The DCC generates a replacement Issuing OCA Certificate, signed by the new Root OCA Private Key.

The DCC stores the new Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.

The DCC informs Responsible Suppliers of the deadline for submitting Service Requests to replace the Root OCA Certificates.

Each Subscriber retrieves the Root OCA Certificate from the SMKI Repository, and sends an 'Update Security Credentials (KRP)' Service Request (SRV 6.15.1) to each affected Device. This process is described in Section 7.7.2.5.6 of the BAD.

The DCC monitors progress and notifies the Subscriber if the replacement has not been successful.

Post-recovery

The Subscriber submits a request to change the ADTs. This process is described in Section 7.8.2.5.1 of the BAD. The DCC:

- Amends the ADTs;
- Destroys the replaced Root OCA Private Key, Issuing OCA Private Key, Contingency Private Key and Contingency Symmetric Key; and
- Notifies the SMKI PMA that the recovery is complete.

7.7.3.4.7 Recovery of Recovery Private Key

Pre-recovery

The DCC notifies the SMKI PMA and each Subscriber of a Compromise to the Recovery Private Key.

The DCC begins preparation for the Key Activation Ceremony.

The SMKI PMA confirms to the DCC the recovery method. The DCC notifies the Subscriber.

Recovery

The DCC temporarily changes the ADTs that are required to support replacement of affected Organisation Certificates on Devices. This process in described in Section 7.8.2.5.1 of the BAD.

The DCC completes the Key Activation Ceremony to activate and generate a new Recovery Private Key.

The DCC sends Commands to the affected Devices to replace the Recovery Certificate. The DCC notifies each Responsible Supplier if the Certificate replacement has not been successful.

Post-recovery

The DCC does the following things:

- Amends the ADTs;
- Destroys the replaced Recovery Private Key;
- Revokes the Recovery Certificate; and
- Notifies the SMKI PMA that recovery is complete.

7.7.3.4.8 Recovery of Issuing OCA Private Key

Pre-recovery

The DCC notifies the SMKI PMA and each Subscriber of a Compromise to the Issuing OCA Private Key.

The DCC begins preparation for the Key Activation Ceremony.

The SMKI PMA confirms to the DCC the recovery method. The DCC notifies the Subscriber.

The DCC revokes the Issuing OCA Certificate and destroys the compromised Issuing OCA Private Key.

Recovery

The Subscriber submits a request to temporarily change the ADTs that are required to support replacement of affected Organisation Certificates on Devices. The DCC amends the ADTs. This process is described in Section 7.8.2.5.1 of the BAD.

The DCC generates a new Issuing OCA Key Pair and Issuing OCA Certificate.

The DCC completes the Key Activation Ceremony to activate and generate a new Recovery Private Key.

The DCC sends Commands, Digitally Signed with the Recovery Private Key, to the affected Devices to replace the compromised Organisation Certificates with the Organisation Certificate on the affected Devices. The DCC notifies the Subscriber if the replacement has been successful.

The Subscriber checks if any of the Organisation Certificates are signed using the Compromised Issuing OCA Private Key. The Subscriber composes and sends an 'Update Security Credentials (KRP)' Service Request (SRV 6.15.1) to replace these Organisation Certificates. This process is described in Section 7.7.2.5.6 of the BAD.

The DCC monitors progress and notifies the Subscriber if the replacement has not been successful.

Post-recovery

The Subscriber submits a request to change the ADTs. This process is described in Section 7.8.2.5.1 of the BAD. The DCC:

- Amends the ADTs; and
- Notifies the SMKI PMA that recovery is complete.

7.7.3.5 Associated Process Areas

#	Process Areas
7.7.2	Manage Security Credentials
7.9.4	Manage Incidents
7.8.2	Threshold Anomaly Detection

7.7.3.6 Governance

Actor	SEC Document	Clause	Text
7.7.3 SMKI Recovery			
DCC	SEC Appendix L - SMKI Recovery Procedure	3.1	The DCC shall: a) conduct the procedures set out in this document; b) comply with any decisions made by the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise, or suspected Compromise; c) where the DCC attempts but fails to replace one or more Certificates as part of operating these procedures, execute as many retries to replace

Actor	SEC Document	Clause	Text
			such Certificates as DCC can reasonably accommodate given the circumstances of the Compromise and capability of the DCC Systems, prior to any deadline for recovery as approved by the SMKI PMA; d) where the DCC consults with the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise, or suspected Compromise, and the DCC is directed such that recovery using the Recovery Private Key or Contingency Private Key should not be performed, the DCC shall inform all affected Parties of the outcome and any reasons provided by the SMKI PMA, as soon as reasonably practicable following such instruction, via a secured electronic means; e) maintain confidential, auditable and secured records relating to the recovery from a Compromise (or suspected Compromise), and the Devices and Subscribers affected by such Compromise; and f) within three Working Days of the recovery from a Compromise or suspected Compromise, prepare a report regarding execution of the recovery and provide such report to the SMKI PMA, where such report shall include: i. the process steps executed and the timing of the procedure to recover from the Compromise; ii. where possible, analysis of which communications have been submitted to Devices and any anomalous activity that should be investigated further by the DCC and/or affected Subscribers, and/or addressed via remedial actions; and iii. any proposed modifications to the SMKI Recovery Procedure that the DCC believes are necessary for the SMKI Recovery Procedure to more effectively meet the objectives as set out in the SEC. https://smartenergycodecompany.co.uk/download/2345
7.7.3.4.1 Manage Incidents			
DCC	SEC Appendix L - SMKI Recovery Procedure	3.2	Any person may notify the DCC that there is a Compromise or suspected Compromise of a Relevant Private Key. Where the DCC is notified or becomes aware of a Compromise or suspected Compromise of a Relevant Private Key, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall notify the SMKI PMA, via secured electronic means, that a Compromise or suspected Compromise has been notified. The DCC shall contact the Subscriber for the Certificate associated with that Private Key or Contingency Symmetric Key (which may include the DCC itself as the Subscriber), as soon as reasonably practicable, via

Actor	SEC Document	Clause	Text
			telephone and email using the contact details held by the SMKI Registration Authority. The DCC shall provide the Subscriber, via secured electronic means, with the appropriate Incident reference number and information relating to the notified Compromise. The DCC shall request confirmation from the Subscriber as to whether the Subscriber reasonably believes that a Compromise has occurred, and wishes to proceed with one or more of the recovery processes, which shall be confirmed by: a) A SMKI Senior Responsible Officer (SMKI SRO) on behalf of a Party; or b) A SMKI SRO, SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel on behalf of the DCC. The Subscriber shall take reasonable steps to ensure that confirmation of whether it reasonably believes that a Compromise has occurred is provided to the DCC by the representatives above, within 24 hours of the request for confirmation from the DCC, via secured electronic means. Where the Subscriber confirms that it does not reasonably believe that a Compromise has occurred, the DCC shall close the Incident in accordance with section 2.12 of the Incident Management Policy. Where the DCC receives confirmation that the Subscriber reasonably believes that a Compromise has occurred, the DCC shall also identify any Responsible Supplier(s) that are affected by the confirmed Compromise, in accordance with the procedures as set out in this document. Where the DCC receives multiple Compromise notifications, the DCC may execute a common set of procedural steps to address such multiple Compromises, where it reasonably believes that such an approach would achieve the required recovery in an efficient manner. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	3.3	The DCC shall only accept the confirmation of a Compromise or suspected Compromise from a representative of the Subscriber as is defined in section 3.2 of this document, for a Certificate associated with a Compromised Private Key or from the DCC in respect of a Compromised Contingency Symmetric Key, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means. https://smartenergycodecompany.co.uk/download/2345

Actor	SEC Document	Clause	Text
7.7.3.4.2 Recovery of Private Keys associated with Organisation Certificates by affected Subscribers (Method 1)			
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.1.1.1	The affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates that are affected by the Compromise (or suspected Compromise). The DCC shall revoke such Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.1.1.2	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.1.1.3	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a) that a Compromise of an Organisation's Private Key has been notified; b) that the Subscriber intends to use method 1 (as set out in section 4.1 of this document) to recover; and c) of details relating to the

Actor	SEC Document	Clause	Text
			Compromise, comprising the Subscriber and the number of Devices affected, which will include the Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.1.1.4	Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.1.1.1, the DCC shall notify the Responsible Supplier, via secured electronic means, that a Subscriber wishes to recover using its own Private Key to recover. The DCC shall also provide to the Responsible Supplier, via a secured electronic means, one or more Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC, which together contain details of the Device IDs to which the Compromise relates https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.1.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds for the affected Subscriber to allow submission of Service Requests to replace affected Organisation Certificates, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall inform, via a secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.1.1.2, that the Anomaly Detection Threshold values have been successfully amended. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.1.2.2	The affected Subscriber shall either: a) identify replacement Organisation Certificates; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI	4.1.2.3	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification, to replace affected

Actor	SEC Document	Clause	Text
	Recovery Procedure		Organisation Certificates on all relevant Devices and shall, in doing so, monitor replacement of such affected Organisation Certificates. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.1.2.4	Upon completion of its activities to replace affected Organisation Certificates on affected Devices, the affected Subscriber shall inform the DCC, via a secured electronic means: a) that its activities in respect of the replacement of Organisation Certificates have been completed; and b) of the Devices for which replacement of affected Organisation Certificates has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.1.2.5	Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.1.1.1, he DCC shall notify the Responsible Supplier for affected Devices, via secured electronic means, which Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.1.3.1	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure https://smartenergycodecompany.co.uk/download/2345

Actor	SEC Document	Clause	Text
DCC	SEC Appendix L - SMKI Recovery Procedure	4.1.3.2	The DCC shall notify the SMKI PMA via a secured means of: a) the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1; and b) the Devices for which recovery was not completed, which may be provided in one or more which shall be Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC. https://smartenergycodecompany.co.uk/download/2345
7.7.3.4.3 Recovery of Private Keys associated with Organisation Certifies by the DCC installing ACB Certificates (Method 2)			
Subscriber, DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.1.1	The affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.2.1.2	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more Organisation Compromise Notification Files that each comply with Annex B of this document and which together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection

Actor	SEC Document	Clause	Text
			Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.1.3	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise (or suspected Compromise) of an Organisation Certificate or Organisation Certificates, using the procedure as set out in section 4.2.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Certificates on Devices). The DCC shall disable processing of communications destined for Devices that it has been notified (in Step 4.2.1.2) are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those Devices to 'recovery' The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out. https://smartenergycodecompany.co.uk/download/2345
Subscriber, DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.1.5	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices, which may be provided in in one or more Organisation Compromise Notification Files that comply with Annex B of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); d) anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI	4.2.1.5	The DCC shall notify the relevant Network Parties via secured electronic means: a) that a Responsible Supplier wishes to recover using the procedure as set

Actor	SEC Document	Clause	Text
	Recovery Procedure		out in section 4.2.2 of this document; and b) the Device IDs to which the Compromise relates, which shall submitted in one or more Organisation Compromise Notification Files that comply with Annex B of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.1.6	Where the DCC believes that use of the Recovery Private Key is likely to be agreed by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c) notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and d) activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key https://smartenergycodecompany.co.uk/download/2345
SMKI PMA	SEC Appendix L - SMKI Recovery Procedure	4.2.1.7	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.2.1.4 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.1.8	The DCC shall inform the affected Subscriber, of the SMKI PMA's decision whether or not to execute the procedure as set out in section 4.2.2. https://smartenergycodecompany.co.uk/download/2345

Actor	SEC Document	Clause	Text
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.2.1	Should the decision of the SMKI PMA be not to disable device communications, the DCC shall re-enable communications to any devices where communications have previously been disabled by setting the SMI Status of any Device that had been set to "recovery" pursuant to Step 4.2.1.3 back to the SMI Status each such Device held immediately prior to the execution of step 4.2.1.3 of this procedure. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.2.2	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of recovery Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.2.1 of this document; and b) for the affected Subscriber, to allow submission of Service Requests to replace DCC Access Control Broker Certificates with new Organisation Certificates. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.2.1.2, that the Anomaly Detection Threshold values have been successfully amended. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.2.3	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.2.4	The DCC shall send Commands to each affected Device, Digitally Signed using the Recovery Private Key, in order to replace Organisation Certificates in all of the Supplier slots on Devices as notified in step 4.2.1.2, with a DCC Access Control Broker Certificate. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI	4.2.2.5	Upon completion of step 4.2.2.4 for each Device, the DCC shall restore processing of communications

Actor	SEC Document	Clause	Text
	Recovery Procedure		destined for the affected Device by setting the SMI Status to 'recovered'. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.2.6	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected Devices: a) upon replacement of affected Certificates on each Device, using a DCC Alert issued via the DCC User Interface; and b) upon completion of attempts to replace all affected Certificates on relevant Devices, in one or more Organisation Compromise Recovery Progress Files that comply with Annex C of this document, provided via secured electronic means. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.2.2.7	The affected Subscriber shall either: a) identify replacement Organisation Certificates; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates https://smartenergycodecompany.co.uk/download/2345
Supplier	SEC Appendix L - SMKI Recovery Procedure	4.2.2.8	Where the DCC has recovered by replacing Organisation Certificates of the Responsible Supplier, with a DCC Access Control Broker Certificate, the Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace the DCC Access Control Broker Certificate in each Supplier Device slot with a replacement Organisation Certificate, for each Device as established in step 4.2.1.1 within section 4.2 of this document. Upon successful completion of such replacement for a Device, the DCC shall set the SMI Status for that Device to the SMI Status that was in place immediately prior to the execution of step 4.2.2.1 of this procedure https://smartenergycodecompany.co.uk/download/2345
Supplier	SEC Appendix L - SMKI Recovery Procedure	4.2.2.9	The Responsible Supplier shall notify the DCC in respect of replacement of such DCC Access Control Broker Certificates with new Organisation Certificates, via secured electronic means and in one or more Organisation Compromise Recovery Progress Files that comply with Annex C of this document.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.3.1	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the affected Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.2 of this document https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.2.3.2	The DCC shall notify the SMKI PMA, via a secured means, of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Organisation Compromise Recovery Progress Files that comply with Annex C of this document; and b) the number of Devices for which recovery was not successful https://smartenergycodecompany.co.uk/download/2345
7.7.3.4.4 Recovery of Private Keys associated with Organisation Certificates by the DCC installing Organisation Certificates (Method 3)			
Subscriber, DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.1.1	The Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.3.1.2	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or

Actor	SEC Document	Clause	Text
			Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.1.3	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise (or suspected Compromise) of its Organisation Certificate using the procedure as set out in section 4.3.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Certificates on Devices). Where the Compromise affects Supplier or CSP Certificates the DCC shall disable processing of communications destined for those Devices that it has been notified (in Step 4.3.1.2) that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those Devices to 'recovery'. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.1.4	Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means: a) that a Subscriber wishes to recover using the procedure as set out in section 4.3.2 of this document; and b) the Device IDs to which the Compromise relates, which shall be submitted in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.1.5	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices, which may be provided in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and d) anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.1.6	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d) activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key https://smartenergycodecompany.co.uk/download/2345
SMKI PMA	SEC Appendix L - SMKI	4.3.1.7	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document

Actor	SEC Document	Clause	Text
	Recovery Procedure		should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.3.1.5 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.1.8	The DCC shall notify the affected Subscriber, via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2. Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.1	Should the decision of the SMKI PMA be not to disable device communications, the DCC shall re-enable communications to any devices where communications have previously been disabled by setting the SMI Status of any Device that had been set to "recovery" pursuant to Step 4.3.1.3 back to the SMI Status each such Device held immediately prior to the execution of step 4.3.1.3 of this procedure https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.2	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.3.1 of this document. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.3.1.2, that the Anomaly

Actor	SEC Document	Clause	Text
			Detection Threshold values have been successfully amended. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	4.3.2.3	The affected Subscriber shall either: a) identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Private Key; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are not Digitally Signed by the Compromised Private Key. The affected Subscriber shall notify the DCC of the serial number of the replacement Organisation Certificate that should be used to populate a Device and specify the Device slot to which the replacement Organisation Certificate relates, which shall be provided via secured electronic means in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.4	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.5	The DCC shall send Commands to all Devices, Digitally Signed using the Recovery Private Key, in order to replace affected Organisation Certificates on relevant Devices as notified in step 4.3.1.1 with replacement Certificates as notified by the affected Subscriber. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.6	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected Devices: a) upon replacement of affected Certificates on each Device, using a DCC Alert issued via the DCC User Interface; and b) upon completion of attempts to replace all affected Certificates on relevant Devices, in

Actor	SEC Document	Clause	Text
			one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC, provided by secured electronic means. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.7	Upon completion of step 4.3.2.6 for each Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status for that Device to the SMI Status that was in place immediately prior to the execution of step 4.3.2.1 of this procedure https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.2.8	The DCC shall notify each Responsible Supplier for affected Devices, by secured electronic means, which Devices were not recovered successfully in one or more one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.3.1	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.3 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	4.3.3.2	The DCC shall notify the SMKI PMA, via a secured electronic means, of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC; and b) the number of Devices for which recovery was not successful.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
7.7.3.4.5 Recovery using Contingency Private Key			
DCC	SEC Appendix L - SMKI Recovery Procedure	5.1.1	The DCC shall notify the SMKI PMA and all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Root OCA Key has been notified, or that use of the Recovery Private Key has been unsuccessful that the DCC reasonably believes that the nature of the Compromise could require use of the Contingency Private Key. The DCC shall also provide details to affected Subscribers of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Annex D of this document. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Annex D of this document; b) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Root OCA Private Key; c) the extent to which the vulnerabilities that caused the Compromise have been addressed; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.1.3	Where the DCC believes that use of the Contingency Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) inform the requisite number of Key Custodians, via a secured electronic means, that a Key Activation Ceremony for the Contingency Private Key is required (which may be greater than the minimum

Actor	SEC Document	Clause	Text
			number required to activate the Contingency Private Key), and the date, time and location of each Key Activation Ceremony; b) notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and c) activities required to prepare the systems environment required to support activation and use of the Contingency Private Key. https://smartenergycodecompany.co.uk/download/2345
SMKI PMA	SEC Appendix L - SMKI Recovery Procedure	5.1.4	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 5.1.2 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.1.5	The DCC shall notify affected Subscribers, via a secured electronic means, of the SMKI PMA's decision whether or not to execute the recovery procedure (amended as directed by the SMKI PMA) as set out in section 5.2. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.1.6	The DCC shall execute steps in order, where applicable in accordance with the SMKI PMA's decision, to revoke: a) the Root OCA Certificate; b) the Issuing OCA Certificate The DCC shall update and lodge the relevant ARL in the SMKI Repository and shall destroy affected Private Keys and Symmetric Keys, which may include: a) the old Root OCA Private Key; b) the old Issuing OCA Private Key; c) the old Contingency Private Key; and d) the old Contingency Symmetric Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.1	The DCC shall disable processing of communications destined for Devices that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status to 'recovery'.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	5.2.2	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.3	The DCC shall temporarily amend the Anomaly Detection Thresholds, as required and including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in step 5.1.2; and b) affected Subscribers to allow submission of Service Requests to replace DCC Access Control Broker Certificates with new Organisation Certificates. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 5.2.2, that the Anomaly Detection Threshold values have been successfully amended. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.4	The DCC, shall conduct relevant Key Generation Ceremonies in accordance with the Organisation CPS, in order to generate: a) a new Contingency Symmetric Key; b) a new Contingency Key Pair; c) a new wrappedApexContingencyKey; d) a new Root OCA Key Pair; and e) a new Issuing OCA Key Pair. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI	5.2.5	The DCC shall generate a new Root OCA Certificate, embedding the new wrappedApexContingencyKey

Actor	SEC Document	Clause	Text
	Recovery Procedure		that has been generated as part of the process as set out in step 5.2.4 of this document. The new Root OCA Certificate shall be Digitally Signed by the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate, signed by the new Root OCA Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.6	The DCC shall lodge the new Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.7	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Contingency Private Key and the plain text version of the Contingency Symmetric Key that were used to generate the wrappedApexContingencyKey that is stored within the Root OCA Certificate that has been deployed to Devices. To facilitate this, the DCC shall bring together all parts of the Contingency Symmetric Key https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.8	The DCC shall send Commands to all Devices, Digitally Signed using the Contingency Private Key and including the Contingency Symmetric Key to enable activation, attaching the following Certificates (where applicable according to the Device type) to the corresponding Devices: a) a new Root OCA Certificate; b) a replacement new DCC Transitional CoS Certificate; c) a replacement new Recovery Certificate; d) a replacement new DCC Access Control Broker Certificate; e) a replacement new DCC WAN Provider Certificate; and f) a new DCC Access Control Broker Certificate which shall be placed in each Supplier Device slot or Network Operator Device slot in the corresponding Device https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.9	Upon completion of step 5.2.8 for each Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status to 'recovered'.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.10	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.11	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected Devices: a) upon replacement of affected Certificates on each Device with a DCC Access Broker Certificate, via DCC Alert issued via the DCC User Interface to the affected Subscriber; and b) upon completion of attempts to replace all affected Certificates (for each affected Subscriber) on relevant Devices, in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, which shall be provided via secured electronic means. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.2.12	The DCC shall notify each Responsible Supplier for affected Devices, via secured electronic means, in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, which Devices were not recovered successfully. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	5.3.1	The affected Subscriber shall either: a) identify replacement Organisation Certificates; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates https://smartenergycodecompany.co.uk/download/2345
Supplier	SEC Appendix L - SMKI Recovery Procedure	5.3.2	The Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace: a) the DCC Access Control Broker Certificate in each Supplier Device slot with a replacement Organisation Certificate that is Issued under the new Issuing OCA, for each Device as established in step 5.2.2 within section 5.2 of this document; and b) the DCC Access Control Broker Certificate in each Network Operator Device slot with an Organisation Certificate to which the Network Operator is the Subscriber that is Issued

Actor	SEC Document	Clause	Text
			under the new Issuing OCA, for each Device as established in step 5.2.2 within section 5.2 of this document. Upon successful completion of such replacement for a Device, the DCC shall set the SMI Status for that Device to the SMI Status that was in place immediately prior to the execution of step 5.2.1 of this procedure. The Responsible Supplier shall notify the DCC in respect of replacement of affected Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document. https://smartenergycodecompany.co.uk/download/2345
SMKI ARO	SEC Appendix L - SMKI Recovery Procedure	5.3.3	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 5 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	5.3.4	The DCC shall notify the SMKI PMA and affected Subscribers, via a secured means, of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document.; and b) the number of Devices for which recovery was not successful. https://smartenergycodecompany.co.uk/download/2345
7.7.3.4.6 Recovery of Contingency Private Key or Contingency Symmetric Key			
DCC	SEC Appendix L - SMKI	6.1.1.1	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable,

Actor	SEC Document	Clause	Text
	Recovery Procedure		that a Compromise, or suspected Compromise, of the Contingency Private Key or Contingency Symmetric Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.1.2	The DCC shall notify all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Contingency Private Key or Contingency Symmetric Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Annex D of this document https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.1.3	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Annex D of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Contingency Private Key; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.1.4	Where the DCC believes that replacement of the Contingency Key Pair and generation of a replacement Root OCA Certificate (and therefore a new Contingency Private Key and Contingency Symmetric Key) is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) informing the requisite number of Key Custodians, via a secured electronic means, that a Key

Actor	SEC Document	Clause	Text
			Generation Ceremony for the Contingency Key Pairs is required and the date, time and location of each the Key Generation Ceremony; b) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony may be required; and c) activities required to prepare such systems environment required to support generation of a new Contingency Key Pair, Contingency Symmetric Key, Root OCA Key Pair and replacement Root OCA Certificate, Issuing OCA Key Pair and Issuing OCA Certificate that may be required. https://smartenergycodecompany.co.uk/download/2345
SMKI PMA	SEC Appendix L - SMKI Recovery Procedure	6.1.1.5	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.1.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.1.6	The DCC shall notify all affected Subscribers, via a secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.1.2. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	6.1.2.1	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files

Actor	SEC Document	Clause	Text
			as set out in section 6 of the Threshold Anomaly Detection Procedure. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.2.2	The DCC shall temporarily amend the Anomaly Detection Thresholds; including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for the DCC and affected Responsible Suppliers to allow submission of Service Requests to replace the Root OCA Certificate on Devices. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.2.3	The DCC shall conduct relevant Key Generation Ceremonies, in order to generate the following, in accordance with the Organisation CPS and the Great Britain Companion Specification (GBCS): a) a new Contingency Symmetric Key; b) a new Contingency Key Pair c) a new Root OCA Key Pair; d) a new Issuing OCA Key Pair and e) a new wrappedApexContingencyKey https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.2.4	The DCC shall generate a replacement Root OCA Certificate, embedding the new wrappedApexContingencyKey that has been generated as part of the process as set out in step 6.1.2.3 of this document. The replacement Root OCA Certificate shall be Digitally Signed by the existing Root OCA Private Key and the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate, which shall be Digitally Signed by the new Root OCA Private Key https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.2.5	The DCC shall lodge the replacement Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI	6.1.2.6	The DCC shall notify, via secured electronic means: a) the target deadline for the submission of Service

Actor	SEC Document	Clause	Text
	Recovery Procedure		Requests to replace affected Root OCA Certificates on affected Devices, which shall be assessed by the DCC based on the number of Devices affected; and b) the replacement Root OCA Certificate serial number, which shall be provided in one or more Other Compromise Notification Files as set out in Annex D of this document. Such notification shall be provided by the DCC to the organisation responsible, which shall be: a) for all Communications Hub Functions, the DCC (the Service Provider that is the provider of the WAN for the relevant Region); or b) for all other Devices, shall be the Responsible Supplier that is the Subscriber for the Organisation Certificate held in the supplier digital signing slot on that Device, for that Device. https://smartenergycodecompany.co.uk/download/2345
Supplier	SEC Appendix L - SMKI Recovery Procedure	6.1.2.7	The organisation as defined in step 6.1.2.6, shall retrieve the replacement Root OCA Certificate from the SMKI Repository and shall send such Service Requests, in accordance with the provisions of the DCC User Interface Specification, (or in the case of the DCC, issue such Commands) as are required to replace the existing Root OCA Certificate on all affected Devices with the new Root OCA Certificate. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.2.8	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of replacement of the Root OCA Certificate. The DCC shall also monitor for unauthorised use of the Contingency Private Key and shall take all reasonable steps to keep the SMKI PMA informed as to such unauthorised use. Where directed to amend the recovery steps based on unauthorised use, the DCC execute steps as notified by the SMKI PMA. Following the deadline for Root OCA Certificate replacement as set out in step 6.1.2.7, the DCC shall identify whether recovery for all affected Devices has been successfully completed. Where recovery of all affected Devices has not been completed, the DCC shall notify, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, to each organisation as established in step 6.1.2.7 of the list of Devices where the replacement of Root OCA Certificates has not been successfully completed

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.2.9	The DCC shall notify each Responsible Supplier for affected Devices which Devices were not recovered successfully, using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, via secured electronic means. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.3.1	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by an affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.1 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.3.2	The DCC shall destroy the replaced Root OCA Private Key, Issuing OCA Private Key, Contingency Private Key and Contingency Symmetric Key https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.1.3.3	The DCC shall notify the SMKI PMA, via a secured means of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document; and b) the number of Devices for which recovery was not successful. https://smartenergycodecompany.co.uk/download/2345
7.7.3.4.7 Recovery of Recovery Private Key			

Actor	SEC Document	Clause	Text
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.1.1	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Recovery Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.1.2	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means that the Compromise of the Recovery Private Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification Files which comply with Annex D of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.1.3	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification Files which comply with Annex D of this document; b) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Recovery Private Key; c) the extent to which the vulnerabilities that caused the Compromise have been addressed; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.1.4	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to

Actor	SEC Document	Clause	Text
			activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d) activities required to prepare such systems environment required to support activation and use of the Recovery Private Key. https://smartenergycodecompany.co.uk/download/2345
SMKI PMA	SEC Appendix L - SMKI Recovery Procedure	6.1.2.5	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.2.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.1.6	The DCC shall notify all Subscribers to Organisation Certificates, by secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.2.2. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.2.1	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds for the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.2.1 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.2.2	The DCC shall: a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via

Actor	SEC Document	Clause	Text
			a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6,2.2.3	The DCC shall: a) determine the number of Key Custodians required to attend a Key Generation Ceremony for the Recovery Private Key; b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c) participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.2.4	The DCC shall send Commands to all Devices to replace the Recovery Certificate held on such Devices with the Recovery Certificate generated in step 6.2.2.3. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.2.5	The DCC shall notify each Responsible Supplier for affected Devices, by secured electronic means, which Devices were not recovered successfully, in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.3.1	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of

Actor	SEC Document	Clause	Text
			the procedure set out in this Section 6.2 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.3.2	The DCC shall destroy the replaced Recovery Private Key and shall revoke the Recovery Certificate that has been replaced in the procedure as set out in Section 6.2.2 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.2.3.3	The DCC shall notify the SMKI PMA, via secured electronic means of: a) whether the recovery from the Compromise has been successfully completed; and b) the number of Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document. https://smartenergycodecompany.co.uk/download/2345
Recovery from Compromise of the Issuing OCA Private Key			
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.1.1	The DCC shall notify the SMKI PMA and each Subscriber to affected Organisation Certificates, via a secured electronic means, as soon as reasonably practicable, that a Compromise of an Issuing OCA Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.1.2	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means, the Compromise of the Issuing OCA Private Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Annex D of this document https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.1.3	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to):

Actor	SEC Document	Clause	Text
			a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Annex D of this document; b) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Issuing OCA Private Key; c) the extent to which the vulnerabilities that caused the Compromise have been addressed; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise) e) anticipated timescales for recovery; and f) whether or not DCC is proposing to that multiple Compromises should be dealt with on a common basis and if so why the DCC proposes that they should be so treated https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.1.4	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d) activities required to prepare such systems environment required to support activation and use of the Recovery Private Key. https://smartenergycodecompany.co.uk/download/2345
SMKI PMA	SEC Appendix L - SMKI Recovery Procedure	6.3.1.5	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.3.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.1.6	The DCC shall notify all Subscribers to affected Organisation Certificates, via secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.3.2. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.1.7	The DCC shall revoke the Issuing OCA Certificate to which the affected Issuing OCA Private Key relates, and shall update and lodge the relevant Organisation ARL in the SMKI Repository. The DCC shall destroy the Issuing OCA Private Key that is Compromised or suspected to be Compromised. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	6.3.2.1	A SMKI ARO acting on behalf of each affected Subscribers shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.2	The DCC shall temporarily amend the Anomaly Detection Thresholds; including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for affected Subscribers to allow submission of Service Requests to replace affected Organisation Certificates on Devices. The DCC shall inform, via secured electronic means, a SMKI SRO acting and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended. The DCC shall

Actor	SEC Document	Clause	Text
			amend its Anomaly Detection Thresholds that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of the affected Recovery Certificate on Devices. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.3	The DCC shall generate a new Issuing OCA Key Pair and Issuing OCA Certificate, in accordance with the procedure as set out in the Organisation CPS. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.4	The DCC shall: a) determine the number of Key Custodians required to attend a Key Generation Ceremony for the relevant Recovery Private Key; b) inform such Key Custodians in respect of the relevant Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c) participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate, Digitally Signed using the new Issuing OCA Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.5	The DCC shall: a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.6	The DCC shall send Commands to all Devices to replace the Recovery Certificate held on such Devices with the Recovery Certificate generated in step 6.3.2.4. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected Device that the

Actor	SEC Document	Clause	Text
			Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure. The DCC shall notify each organisation as established in step 6.3.1.3, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, of the list of Devices where the replacement of the Recovery Certificate has been successfully completed. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	6.3.2.7	Each affected Subscriber shall either: a) identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Issuing OCA Private Key; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are Digitally Signed by the new Issuing OCA Private Key. https://smartenergycodecompany.co.uk/download/2345
Subscriber	SEC Appendix L - SMKI Recovery Procedure	6.3.2.8	Each affected Subscriber shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, in order to replace all Organisation Certificates for which it is the Subscriber that are held on Devices and are signed using the Compromised Issuing OCA Private Key, with new Organisation Certificate as identified in accordance with step 6.3.2.7 that are signed by the new Issuing OCA Private Key that is generated in accordance with step 6.3.2.3. Following attempts to replace affected Certificates on Devices, each affected Subscriber shall notify the DCC in respect of replacement of affected Certificates with new Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.9	The DCC shall: a) monitor its records of replacement by affected Subscribers against the list as has been compiled in step 6.3.1.2, to identify successful replacement; b) identify any failures to replace affected Organisation Certificates that have been Digitally Signed using the Issuing OCA Private Key that has been Compromised; and c) monitor revocation of

Actor	SEC Document	Clause	Text
			Organisation Certificates that are Digitally Signed using the Compromised Issuing OCA Private Key. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.2.10	The DCC shall notify each Responsible Supplier for affected Devices, via secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, the Devices for which replacement of the Recovery Certificate or affected Organisation Certificates was not successfully completed. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.3.1	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.2 of this document. https://smartenergycodecompany.co.uk/download/2345
DCC	SEC Appendix L - SMKI Recovery Procedure	6.3.3.2	The DCC shall notify the SMKI PMA, via a secured electronic means of: a) whether the recovery from the Compromise has been successfully completed; and b) the number of Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document. https://smartenergycodecompany.co.uk/download/2345

7.7.4 User to Non-User Churn

In a dynamic marketplace, Energy Consumers switch Suppliers. In the early stages of the Smart Meter roll-out where not all Suppliers are DCC Users, there may be cases where an Energy Customer who has an SMS installed churns from a Supplier who is a DCC User (therefore operates the SMS via the DCC) to a Supplier who is not a DCC User (therefore unable to operate the SMS via the DCC). This is a temporary problem, since all domestic Suppliers are expected to become DCC Users by the end of 2017. (Large domestic Suppliers were required to become Users by 25 May 2017, while small domestic Suppliers by 25 November 2017. However, no decision has been made as to when non-domestic Suppliers supplying sites covered by the roll out obligation will be required to become Users by, which may extend this problem beyond 2017.

As the Gaining Supplier is not a DCC User, they are unable to take control of the SMS via the DCC and place its Organisation Certificates on the relevant Devices. This means that the Losing Supplier's Organisation Certificates remain on the relevant Devices until such time the Gaining Supplier becomes a DCC User and replaces the Organisation Certificates.

The implication of this is that the Losing Supplier is able to send Critical Commands to Devices and continues to receive Device Alerts from the Meters.

While the risk of sending Critical Commands to Devices by the Losing Supplier appears to be low, the Gaining Supplier may be at risk of breaching their duty of care obligations if they fail to act upon certain Device Alerts, for example those relating to a possible gas leak. As there is no SEC obligation on the Losing Supplier to pass Device Alerts to the Gaining Supplier, a voluntary agreement has been made between all Suppliers to do this. Details can be found on the SEC website in the document entitled: "Managing Critical Alerts where there is DCC User to Non-User Churn Guidance Note"[22].

Where a Supplier who is a DCC User (DCC User Supplier) receives a Critical Device Alert for an MPxN for which it is not the current Supplier, they should as a minimum forward the details of the Device Alert to the Supplier the customer churned to (non-DCC User Supplier).

The DCC User Supplier can identify the Supplier for that MPxN using registration information available via the Electricity Central Online Enquire Service, Data Enquiry Service, and / or registration dataflows as received by the non-DCC User Supplier during the CoS process. The DCC User Supplier should use their best endeavours to identify the non-DCC User Supplier.

The DCC User Supplier forwards the details of the Critical Device Alert via email to the non-DCC User Supplier, using the contact details available on the centralised list of contacts available on the SEC website. There are no requirements on ensuring secure exchanges of emails over and above what Suppliers have already established for various existing industry processes.

The DCC User Supplier forwards the relevant information from the original XML Critical Device Alert in an email in a human readable format. This should allow the non-DCC User Supplier to take the relevant action. At a minimum, the email should include the following information:

[22] https://www.smartenergycodecompany.co.uk/docs/default-source/default-document-library/managing-critical-alerts-where-there-is-dcc-user-to-non-user-churn-guidance-note.pdf?sfvrsn=0

- MPxN that the Critical Device Alert relates to;
- Alert Code; and
- Critical Device Alert date / time stamp as per original XML received from the DCC.

If the DCC User Supplier cannot reach the non-DCC User Supplier via the contacts on the list, they should contact the Code Administrator helpdesk.

The non-DCC User Supplier is required to acknowledge receipt of the email. If the non-DCC User Supplier is not the current Supplier for the MPxN that the Critical Device Alert relates to, then that non-DCC User Supplier is required to identify the correct Supplier and forward-on the email.

7.8 DCC Processing

This process area explains how the DCC processes Service Requests received from Users. There are three types of processing the DCC undertakes. This depends on whether Service Requests result in corresponding Commands destined for Devices forming part of a SMS or whether they are for notifying the DCC of an activity (Non-Device Service Requests). Where Service Requests result in corresponding Commands destined for Devices, the difference in processing also depends on whether corresponding Commands are supply affecting (i.e. Critical or Non-Critical).

The DCC Processing functional area describes internal DCC operations that have direct impacts on User operations and so these are instances where a User may need to:

- Provide an input to the process;
- Respond to an output of the process;
- Be reliant on the quality of the Data processed; and
- Rely on the process for its own business processes.

For Non-Critical Service Request processing, the DCC relies on Registration Data, in that it checks that the User is the Responsible Supplier for the MPxN in question. It further uses the Registration Data for determining charges to Suppliers and Network Operators. The interactions and Data passed between Registration Data Providers and the DCC is described in Section 7.8.1 of the BAD.

The Threshold Anomaly Detection process area describes how Users securely inform the DCC of likely volumes of each SRV and likely ranges of values for certain supply affecting parameters within certain Signed Pre-Commands. The DCC quarantines Service Requests / Signed Pre-Commands received that breach these thresholds and notifies the User of the fact. Users may then examine the Service Request / Signed Pre-Command and inform the DCC of the next appropriate action.

The DCC provides a facility for scheduling certain Non-Critical Service Requests. This means that Users can establish a schedule for repetitive events (for instance reading Voltage Data) by providing the SRV, and the frequency with which the User wishes to receive a Service Response corresponding to the specified SRV, to the DCC. Subsequently the DCC creates the Service Request and sends the corresponding Command to the Device at the date / time laid out in the schedule until that schedule

comes to an end or is cancelled. The schedule can be cancelled by the User who created it, or it may be cancelled by the DCC following a specific event e.g. CoS.

7.8.1 Manage Registration Data

7.8.1.1 Introduction

Registration Data is used by DCC Systems to assess User eligibility for Service Requests, and also to calculate charges to Users. The DCC is not liable for the accuracy of the Registration Data or for any Service disruption caused by the inaccuracies of the Registration Data.

The Registration Data is therefore critical in Service Request processing; DCC processing of Service Requests and DCC Alerts relies on Registration Data.

Providing and maintaining an accurate record of the Registration Data is the responsibility of each Network Operator, but it is recognised that Electricity Distributors and Gas Transporters may choose to appoint a third party to carry out this role on their behalf, Registration Data Provider (RDP). The processes described in this process area refer to the RDP as the key actor and focus on the relationship between the DCC and the RDP. No assumption is made as to whether the RDP is a Network Operator or a third party.

The Registration Data is transferred between the RDP and the DCC, using the Registration Data Interface. The RDP and the DCC use a specific code of connection to connect to this interface.

7.8.1.2 Scope

This process area includes Manage Registration Data.

This process area excludes the internal processes of the RDP in creating and maintaining the Registration Data within their own systems.

7.8.1.3 Actors

- RDP
- DCC
- Panel

7.8.1.4 Prerequisites

The DCC and the RDP established a secure connection in accordance with the SEC Appendix Y – Registration Data Interface Code of Connection.

7.8.1.5 Process Description

7.8.1.5.1 Manage Registration Data

The RDP creates a Registration Data File. There are three types of file:

- A Registration Data File containing all the Registration Data from the RDP. This is used for initial upload to populate the DCC Systems. Because the initial upload may be very large, the RDP is obligated to inform the DCC of the proposed file size before uploading, and may choose to split the Data into several discrete files. The DCC is obliged to monitor the volume of traffic and ensure sufficient capacity exists.

- A Registration Data Refresh File containing a sub-set of the Registration Data. This may be sent by the RDP at its own discretion, or on request from the DCC; for example, as part of resolving an Incident which identified missing or corrupt Registration Data. Where the DCC is requesting a full or partial file refresh, the DCC is obligated to notify the RDP no later than 16:00 the previous day; and

- A Registration Data Update File. This contains periodic changes in Registration Data. The RDP is required to send it to the DCC every Working Day (Electricity) or every day (Gas), by 06:00, and include any changes recorded the previous day.

The content of the Registration Data File is the same regardless of whether the file is an initial upload, a refresh or an update, but there are some differences between Electricity and Gas.

The Electricity Registration Data includes:

  - Identity of the Electricity Distributor for the MPAN;
  - MPAN Status as identified in the MRA;
  - Supplier registered;
  - MOP registered;
  - Address and Unique Property Reference Number (UPRN) for the Metering Point;
  - Direction of flow;
  - Profile class assigned to the MPAN; and
  - Any recorded objections to a change of registered Supplier.

The Gas Registration Data includes:

  - Identity of the RDP for the Supply Meter Point;
  - Identity of the Gas Transporter for the Supply Meter Point;
  - MPRN for the Supply Meter Point;
  - Whether the status of the Supply Meter Point in the Uniform Network Code (UNC) indicates gas is off taken;
  - Supplier registered;
  - MAM registered;

- Address and UPRN for the Supply Meter Point; and
- Whether the Supply Meter Point is at a Domestic or Non-Domestic Premises.

On receipt of the Registration Data, the DCC creates a DCC Status File to be sent to the RDP. In the case of gas SMSs, the DCC creates one file per RDP, while in the case of electricity SMSs, one file per Electricity Distributor.

The file identifies any changes to the DCC Service Flag (i.e. whether a Meter Point is Enrolled, Suspended or Withdrawn) for each MPAN or Supply Meter Point.

The DCC sends the file no later than 18:00 each day.

The RDP receives and processes the file and sends a Response File back to the DCC.

Both Registration Data Files and DCC Status Files are sent over the same interface and use the same code of connection, and consequently the process for sending and receiving the files are very similar:

- The Sender creates the file, following the defined structure in the SEC Appendix X – Registration Data Interface Specification;
- The Sender Digitally Signs the file;
- The Sender connects to the Registration Data Interface using the DCC Gateway Connection, (or approved alternative), and initiates the file transfer;
- The Receiver Authenticates the file and validates its structure. If successful, the Receiver processes the file and updates its records;
- If Authentication fails, the Receiver raises an Incident. This process is described in Section 7.9.4.5.1 of the BAD;
- If the structure of a Registration Date File is invalid, the DCC raises an Incident;
- If the structure of a DCC Status File is invalid, the RDP includes the validation faults in its Response File to the DCC.

The Panel may request a copy of the Registration Data held by the DCC. This may be all Registration Data, or a sub-set, and may be in anonymised or clear format, depending upon the requirement.

7.8.1.6 Associated Process Area

#	Process Area
7.9.4	Manage Incidents

7.8.1.7 Governance

Actor	SEC Document	Clause	Text
7.8.1.5.1 Manage Registration Data			

Actor	SEC Document	Clause	Text
DCC	Smart Energy Code	Section E3.1	The DCC shall have no liability to any Party where it provides (or does not provide) a Service in circumstances where it should not (or should) have done so, to the extent that the same arises due to inaccuracies in the Registration Data that are not caused by the DCC. https://smartenergycodecompany.co.uk/download/2473
RDP, DCC	SEC Appendix X - Registration Data Interface Specification	2.11 (a)-(d)	When sending a Registration Data File or DCC Status File, the DCC and each Registration Data Provider shall follow steps (a) to (d) below, and when receiving a Registration Data File or DCC Status File the DCC and each Registration Data Provider shall follow steps (e) to (l) below: (a) structure data files provided under Sections E2.1, E2.2 and E2.4 of the Code, in accordance with the structures defined in clauses 3.17, 3.18, 3.19, 3.26, 3.28 and 3.29 of this document and shall include a unique reference number in accordance with clauses 3.11 and 3.22; (b) Digitally Sign the file in accordance with clause 2.13 of this document; (c) connect to the recipient's FTPS server in accordance with clauses 2.7 to 2.9 of this document using a DCC Gateway Connection; (d) initiate the transfer of the file to the relevant delivery directory on the recipient's FTPS server utilising FTP push mechanisms for all file exchanges; https://smartenergycodecompany.co.uk/download/2390
Electricity Distributors	Smart Energy Code	Section E2.1	The Electricity Network Party in respect of each MPAN relating to its network shall provide (or procure that its Registration Data Provider provides) the following information to the DCC in respect of that MPAN (insofar as such information is recorded in the relevant registration systems). The information in question is the following: (a) the identity of the Electricity Network Party for the MPAN; (b) whether or not the MPAN has a status that indicates that it is 'traded' (as identified in the MRA), and the effective date of that status; (c) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become registered in respect of the MPAN, including (to the extent applicable) the date on which each such

Actor	SEC Document	Clause	Text
			person became or ceased to be (or is to become or ceased to be) Registered in respect of the MPAN; (d) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become the Meter Operator in respect of the MPAN, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Meter Operator in respect of the MPAN; (e) the address, postcode and UPRN for the Metering Point to which the MPAN relates; (f) the direction of energy flow to or from the Metering Point to which the MPAN relates (and the date from which that direction of flow has been effective); (g) the profile class (as defined in the MRA) assigned to the MPAN, and each and every other (if any) profile class assigned to the MPAN at any time within the 24 months preceding the date on which the Registration Data is provided (including the date from and to which such profile class was effective); and (h) details of whether an objection has been received regarding a change to the person who is to be registered in respect of the MPAN, and whether that objection has been removed or upheld, or has resulted in the change to the person who is to be registered being withdrawn (as at the date on which the Registration Data is provided). https://smartenergycodecompany.co.uk/download/2473
Gas Transporters	Smart Energy Code	Section E2.2	The Gas Network Party in respect of each Supply Meter Point on its network shall provide (or procure that its Registration Data Provider provides) the following information to the DCC in respect of that Supply Meter Point (insofar as such information is recorded in the relevant registration systems). The information in question is the following: (a) the identity of the Registration Data Provider for the Supply Meter Point; (b) the identity of the Gas Network Party for the network to which the Supply Meter Point relates, and the identity of the Gas Network Party for any network to which the Supply Meter Point related at any time within the 24 months preceding the date on which the Registration Data is provided (and the date from and to which that was the case); (c) the MPRN for the Supply Meter Point;

Actor	SEC Document	Clause	Text
			(d) whether or not the Supply Meter Point has a status that indicates that gas is offtaken at that point (as identified in the UNC), and where that status has changed since the Registration Data was last provided, notification to that effect. (e) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become Registered in respect of the Supply Meter Point, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Registered in respect of the Supply Meter Point; (f) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become the Meter Asset Manager in respect of the Supply Meter Point, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Meter Asset Manager in respect of the Supply Meter Point; (g) the address, postcode and UPRN for the Supply Meter Point; and (h) whether the Supply Meter Point serves a Domestic Premises or Non-Domestic Premises https://smartenergycodecompany.co.uk/download/2473
Electricity Distributor	Smart Energy Code	Section E2.4	The information to be provided by the DCC: (a) to each Electricity Network Party's Registration Data Provider is: (i) whether there is (or used to be) an Enrolled Smart Metering System associated with each of the MPANs relating to the Electricity Network Party's network (and the date of its Enrolment or Withdrawal); and (ii) the identity of the person which the DCC believes to be Registered in respect of each of the MPANs relating to the Electricity Network Party's network; and (b) to each Gas Network Party's Registration Data Provider is whether there is (or used to be) an Enrolled Smart Metering System associated with each of the Supply Meter Points on the Gas Network Party's network (and the date of its Enrolment or Withdrawal). https://smartenergycodecompany.co.uk/download/2473
Electricity Distributor	Smart Energy Code	Section E2.5	A full set of the Data to be exchanged under this Section E2 shall be provided on or before the date on which this Section E2.5 comes into full force and effect (or, in the

Actor	SEC Document	Clause	Text
			case of Registration Data Providers nominated after this Section E2.5 comes into full force and effect, shall be provided in accordance with Section E4 (RDP Entry Process)). Thereafter, the Data to be exchanged under this Section E2 shall (subject to Section E2.8) be provided by way of incremental updates to Data previously provided (so that only Data that has changed is updated) https://smartenergycodecompany.co.uk/download/2473
Electricity Distributor	Smart Energy Code	Section E2.6	The incremental updates to Data to be provided in accordance with this Section E2 shall be updated at the frequency and/or time required in accordance with the Registration Data Interface Documents. https://smartenergycodecompany.co.uk/download/2473
Network Operator	Smart Energy Code	Section E2.7	Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider shall: (a) where a full set of the Registration Data Provider's Registration Data has been requested, take all reasonable steps (including working outside of normal business hours where reasonably necessary) to provide the DCC with such data as soon as reasonably practicable following such request (and in any event within the shorter of three Working Days or four days); or (b) where a subset of the Registration Data Provider's Registration Data has been requested, provide the DCC with the requested Data in accordance with the Registration Data Interface Documents https://smartenergycodecompany.co.uk/download/2473
DCC, RDP	SEC Appendix X - Registration Data Interface Specification	2.11 (e)-(l)	When sending a Registration Data File or DCC Status File, the DCC and each Registration Data Provider shall follow steps (a) to (d) below, and when receiving a Registration Data File or DCC Status File the DCC and each Registration Data Provider shall follow steps (e) to (l) below: (e) authenticate the source of the file through verifying that the file has been Digitally Signed in accordance with clause 2.13 of this document, and validate the file structure against the structure as defined in clauses 3.17, 3.18, 3.19, 3.26, 3.28 and 3.29 of this document; (f) raise an Incident in accordance with the Incident Management Policy, where the recipient is unable to

Actor	SEC Document	Clause	Text
			authenticate the file pursuant to clause 2.17 of this document; (g) in the case of Electricity Registration Data Providers only, raise an Incident in accordance with the Incident Management Policy, where the Electricity Registration Data Provider is unable to confirm that the file conforms with clause 3.17 of this document; (h) in the case of Registration Data Providers only, generate a Response File as defined in clause 3.18(d) or 3.28(b) of this document, where the Registration Data Provider is unable to validate the file structure pursuant to clauses 3.19 or 3.29 of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) immediately above and on receipt of the Response File containing validation errors the DCC shall raise an Incident as defined in the Incident Management Policy; (i) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to validate the file structure pursuant to clause 2.11(e) of this document; (j) process each record within the file and perform record level validation, where the Registration Data Provider or DCC is able to successfully authenticate and validate the file pursuant to clause 2.11(e) of this document; (k) in the case of Registration Data Providers only, generate a Response File as defined in clauses 3.18(d) and 3.28(b) of this document, where the Registration Data Provider is unable to successfully validate and process each record within the file pursuant to clause 2.11(j) of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) and on receipt of the Response File containing validation errors the DCC shall raise an Incident in accordance with the Incident Management Policy; and (l) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to successfully validate and process each record within the file pursuant to clause 2.11(j) of this document. https://smartenergycodecompany.co.uk/download/2390
Gas RDP	SEC Appendix Y - Registration Data Interface	1.5	Each Gas Registration Data Provider shall produce a Registration Data Update File showing changes to the Registration Data that occurred during the preceding day, provided that where no such changes have occurred, the Registration Data Update File shall record zero changes.

Actor	SEC Document	Clause	Text
	Code of Connection		https://smartenergycodecompany.co.uk/download/2393
Electricity RDP	SEC Appendix Y - Registration Data Interface Code of Connection	1.6	Each Electricity Registration Data Provider shall produce a Registration Data Update File showing changes to the Registration Data that occurred during the preceding Working Day, provided that where no such changes have occurred, the Registration Data Update File shall record zero changes. https://smartenergycodecompany.co.uk/download/2393
Gas RDP	SEC Appendix Y - Registration Data Interface Code of Connection	1.7	Pursuant to clause 1.5 of this document, each Gas Registration Data Provider shall send each Registration Data Update File to the DCC via the Registration Data Interface by 06:00 hours on the following day to which the data in the file relates. https://smartenergycodecompany.co.uk/download/2393
Electricity RDP	SEC Appendix Y - Registration Data Interface Code of Connection	1.8	Pursuant to clause 1.6 of this document, each Electricity Registration Data Provider shall send the Registration Data Update File to the DCC via the Registration Data Interface by 06:00 hours on the following Working Day to which the data in the file relates. https://smartenergycodecompany.co.uk/download/2393
DCC	SEC Appendix Y - Registration Data Interface Code of Connection	1.9	The DCC shall produce a DCC Status File showing the changes to the DCC Service Flag for each MPAN or Supply Meter Point that occurred since the last update, provided that where no such changes have occurred, the DCC Status File shall record zero changes https://smartenergycodecompany.co.uk/download/2393
DCC	SEC Appendix Y - Registration Data Interface Code of Connection	1.10	The DCC shall send a DCC Status File by 18:00 hours every day. In the case of Gas Smart Metering Systems, the DCC shall send one DCC Status File per Registration Data Provider. In the case of Electricity Smart Metering Systems, the DCC shall send one DCC Status File per Electricity Network Party https://smartenergycodecompany.co.uk/download/2393
RDP	SEC Appendix Y - Registration Data Interface Code of Connection	1.11	Each Registration Data Provider shall, prior to sending its first set of Registration Data to the DCC, provide to the DCC a size estimate of a file containing a full Registration Data Refresh File. https://smartenergycodecompany.co.uk/download/2393
RDP	SEC Appendix Y - Registration	1.12	Each Registration Data Provider shall inform the DCC in advance of sending Registration Data Files where the number of records requires the Registration Data

Actor	SEC Document	Clause	Text
	Data Interface Code of Connection		Provider to split the data into multiple files due to file size restrictions within the Registration Data Provider's systems. https://smartenergycodecompany.co.uk/download/2393
DCC	SEC Appendix Y - Registration Data Interface Code of Connection	1.13	The DCC shall monitor use of the Registration Data Interfaces and ensure that adequate capacity is provided for each Registration Data Provider to enable the fulfilment of its obligations to provide Registration Data to the DCC under Section E of the Code https://smartenergycodecompany.co.uk/download/2393
DCC	SEC Appendix Y - Registration Data Interface Code of Connection	1.14	The means by which the DCC shall request a re-submission or a refresh of a Registration Data File is for the DCC to contact the Registration Data Provider https://smartenergycodecompany.co.uk/download/2393
DCC	SEC Appendix Y - Registration Data Interface Code of Connection	1.15	When requesting a full or partial file refresh or re-submission of a Registration Data File, the DCC shall take reasonable steps to contact the Registration Data Provider prior to 16:00 on the day of the request. https://smartenergycodecompany.co.uk/download/2393
RDP	SEC Appendix Y - Registration Data Interface Code of Connection	1.16	Pursuant to Section E2.12 of the Code, having been requested to refresh or resubmit a file in accordance with clause 1.14 of this document a Registration Data Provider shall send the file to the DCC via the Registration Data Interface, in accordance with the Registration Data Interface Specification and the timings set out in clauses 1.17 or 1.18 below. On receipt of the file, the DCC shall upload the file as detailed in the Registration Data Interface Specification https://smartenergycodecompany.co.uk/download/2393
Panel	Smart Energy Code	Section E1.4	The Panel shall periodically request from the DCC any Registration Data reasonably required by the Panel in relation to the proper exercise of its duties, powers and functions, including the Registration Data required by the Panel to establish into which Party Category a Party falls. Where aggregated or anonymised data (or similar) is sufficient for the Panel's needs, the Panel shall request, and the DCC shall provide, the data in such format. https://smartenergycodecompany.co.uk/download/2473
DCC	Smart Energy Code	Section E1.5	The DCC shall provide to the Panel any Registration Data requested by the Panel in accordance with Section E1.4.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2473

7.8.2 Threshold Anomaly Detection

7.8.2.1 Introduction

TAD is one of the means of detecting whether a User System and / or DCC Systems have been Compromised. This detective control focuses on monitoring whether the number of Signed Pre-Commands that may affect the supply of energy to a premises as well as the number of Service Requests that ask for Personal Data in accordance with the Data Protection Act exceed a set threshold. In effect, this control checks whether the number of such Service Requests / Signed Pre-Commands has come from the expected source.

Users and the DCC are required to set ADTs for the number of each of the supply affecting Signed Pre-Commands as well as for the number of each of the Service Requests to which a corresponding Response contains 'personal' information sent within a set period of time. Users may also set Warning Thresholds in relation such Service Requests / Signed Pre-Commands sent over a period of time.

Both the number of Service Requests / Signed Pre-Commands and the period of time are set by the DCC and Users for their respective ADTs. During the set period of time, the DCC will monitor the number of Service Requests / Signed Pre-Commands it receives from the User.

In addition to these volume based ADTs, the DCC is required to monitor whether a specific supply affecting parameter, as set by the Security Sub-Committee, within each Signed Pre-Command is within a range set by the Security Sub-Committee. At the time of writing the BAD, this 'packet inspection' ADT has not been implemented in the DCC Systems and the process for managing it does not appear to be described in SEC Appendix AA – Threshold Anomaly Detection Procedures. It is assumed that the process for managing breaches of this ADT would be similar to those for the User and DCC set ADTs. The 'packet inspection' is expected to be implemented in DCC Release 1.3.

If the number of Service Requests / Signed Pre-Commands sent exceeds the Warning Threshold or the ADT, the DCC will notify the User of the Service Requests / Signed Pre-Commands that have exceeded the relevant threshold.

Except for Warning Thresholds, the Service Requests / Signed Pre-Commands that exceed the relevant ADT must be put in quarantine by the DCC. This means they are held in the DCC Systems, and are not sent to Devices. Users may then examine whether the Service Requests / Signed Pre-Commands are genuine and inform the DCC whether the DCC should send the corresponding Command to the Device or delete the Service Request / Signed Pre-Command from the DCC Systems. If the User does not notify the DCC within a set period of time, the Service Request / Signed Pre-Command will be deleted from the DCC Systems.

This process area describes how Users notify the DCC of the Warning Thresholds and ADTs they set, and the steps the DCC and Users take when they are breached.

The focus is on the relationship between the DCC and Users. The process does not describe the internal processes of the DCC or Users in deciding how to set their thresholds or investigating breaches.

7.8.2.2 Scope

This process area includes:

- Set Anomaly Detection Threshold
- Operate Anomaly Detection Threshold

7.8.2.3 Actors

- User
- DCC

7.8.2.4 Prerequisites

The User has nominated a SRO for the purpose of managing the TAD.

The DCC has provided guidance for Users on setting thresholds and a template for submission, and made these available through the SSI.

The DCC guidance includes input from the SSC on whether the way of setting the ADTs continues to provide an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems.

7.8.2.5 Process Description

7.8.2.5.1 Set Anomaly Detection Threshold

User Set

The User sets its Warning Thresholds and ADTs for the number of Service Request / Signed Pre-Commands the User is entitled to send in its User Role and the period of time for monitoring these thresholds. The setting of Warning Thresholds is optional.

If the User wishes to submit a Fast-Track Notification, it contacts the DCC before raising a DCC Service Management Service Request (SMSR) to explain why the Notification will be a Fast-Track Notification.

The User raises a SMSR via the SSI to notify the DCC of its Warning Thresholds and ADTs. The DCC receives the SMSR, creates an entry for that SMSR on the SSI, and provides an SMSR reference number to the User.

The User composes an ADT File and sends it to the DCC. (The ADT File is sent by email, and is Digitally Signed using an IKI Private Key associated with a File Signing. The SMSR reference number is in the subject of the email.) The User updates the status of the SMSR on the SSI.

The DCC receives the ADT File and applies the following checks:

- Checks the Cryptographic Protection applied to the ADT File;
- Confirms the validity of the Certificate used to check Cryptographic Protection;
- Checks the format of the ADT File; and
- For Fast-Track Notifications, assesses whether the justification provided is valid.

If any of the checks fail, the DCC does not process the request further, and updates the SMSR status on the SSI, and notifies the User.

If the checks are successful, the DCC checks that the User set the ADT and Warning Threshold consistently with guidance issued by DCC.

If this check fails, the DCC contacts the User (i.e. User's SRO) to confirm that the User wishes to have the submitted Warning Thresholds and ADTs applied.

- If the User wishes to have the Warning Thresholds and the ADTs applied, the DCC applies them within 72 hours from the receipt of the ADT File from the User (or within 24 hours if it is a Fast-Track Notification).
- If the User does not wish to have the Warning Thresholds and the ADTs applied, the User re-sets its Warning Thresholds and ADTs, and the process starts again from the User raising an SMSR via the SSI.

Once the Warning Thresholds and ADTs are applied, the DCC:

- Changes the SMSR status on the SSI to 'closed'; and
- Notifies the SSC of the ADTs that have been set by the User.

Once the Warning Thresholds and ADTs are applied, the User keeps them under review to ensure they continue to maintain its function effectively, taking account of any Security Sub-Committee feedback. Where they are no longer appropriate, the User sets new Warning Thresholds and ADTs.

DCC Set

The DCC sets ADTs at an aggregate level in relation to each SRV that requires an ADT.

Once the DCC sets the ADTs, it notifies the Security Sub-Committee.

Once the ADTs are applied, the DCC keeps them under review to ensure they continue to maintain its function effectively, taking account of any Security Sub-Committee feedback. Where they are no longer appropriate, the DCC sets new ADTs.

7.8.2.5.2 Operate Anomaly Detection Threshold

The DCC receives a Service Request / Signed Pre-Command from the User, and applies checks. This is described in Section 7.8.4 of the BAD. If these checks are successful, the DCC checks if the Service Request / Signed Pre-Commands is subject to TAD. If so, the DCC applies the Warning Thresholds to

the Service Request / Signed Pre-Command. If the Warning Threshold has been breached, the DCC continues processing the Service Request / Signed Pre-Command and does the following:

- The DCC logs which Service Requests / Signed Pre-Commands exceed the corresponding Warning Threshold.
- After a period of time, the DCC creates an SMSR on the SSI listing all Service Requests / Signed Pre-Commands that exceeded the Warning Threshold to date, and provides an SMSR reference number to the User.

The User receives the SMSR reference number. On the SSI, the User may view which Service Requests / Signed Pre-Commands exceeded the Warning Thresholds using the SMSR reference number. The User may investigate the reason for the breach and update the SMSR accordingly.

The DCC then applies, the following checks to the Service Request / Signed Pre-Command:

- Packet inspection ADT;
- DCC set ADT;
- User set ADT.

If any of the ADTs are breached, the DCC:

- Quarantines the Service Request / Signed Pre-Command and logs which Service Requests/Signed Pre-Commands have been quarantined as a result of exceeding which ADT; and
- Creates an DCC Service Management System (DSMS) on the SSI for each affected User, listing all Service Requests / Signed Pre-Commands that have been quarantined to date as a result of exceeding which ADT for that User, and provides an SMSR reference number to the User.

If the DCC set ADT has been breached, the DCC investigates the breach and assesses whether the Service Requests / Signed Pre-Commands must be deleted from the DCC Systems. If the Service Requests / Signed Pre-Commands must be deleted from the DCC Systems, the DCC deletes them, updates the status of the DSMS to 'closed' on the SSI and notifies the User. If the Service Requests / Signed Pre-Commands may be processed, the DCC updates the status of the DSMS and notifies the User.

The User may view (for 30 days from quarantine) and download (for 120 hours from quarantine) which Service Requests / Signed Pre-Commands exceeded the DCC ADT and have therefore been quarantined. If the User does not take any action, the DCC deletes the Service Requests / Signed Pre-Commands from its DCC Systems after 120 hours;

If the User wishes to take action, the User downloads the report, investigates and composes a QCA File to notify the DCC of whether each of the Service Request / Signed Pre-Command should be deleted or processed further by the DCC. The QCA File is Digitally Signed using an IKI Private

Key associated with a File Signing Certificate. The User sends the QCA File to the DCC. (The QCA File is sent by email, and the DSMS reference number is in the subject of the email.)

The DCC receives the QCA File, and within 24 hours of receipt applies the following checks:

- Checks the Cryptographic Protection applied to the QCA File;
- Confirms the validity of the Certificate used to check Cryptographic Protection; and
- Checks the format of the QCA File.

If the checks are successful, the DCC either deletes or processes the Service Requests / Signed Pre-Commands as instructed by the User, and updates the status of the DSMS to 'closed'.

7.8.2.6 Associated Process Area

#	Process Area
7.8.4	Service Request Processing
7.9.4	Manage Incidents

7.8.2.7 Governance

Actor	SEC Document	Clause	Text
7.8.2.5.1 Set Anomaly Detection Threshold			
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	2.1	Pursuant to Section G6.4 (b) of the Code, each User shall take into account any guidance issued by the DCC as to the appropriate level for their Anomaly Detection Thresholds (ADTs) giving regard to their Service Request forecast and expected pattern of demand for each Service Request. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	2.2	DCC shall: (a) provide guidance to support Users in setting appropriate ADT and Warning Thresholds; (b) provide a template for the User to provide its ADT and Warning Thresholds in the format set out in clause 6.3 of this document; and (c) provide the guidance and template referred to above via the Self Service Interface (SSI). https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	3.1	Prior to sending the DCC any Anomaly Detection Thresholds File, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC, where such reference number will be generated by the SSI automatically. https://smartenergycodecompany.co.uk/download/2263

Actor	SEC Document	Clause	Text
User	Smart Energy Code	Section G6.3	Each User which is an Eligible User in relation to any one or more individual Services listed in the DCC User Interface Services Schedule: (a) shall set Anomaly Detection Thresholds in respect of: (i) the total number of Critical Commands relating to each such Service; and (ii) the total number of Service Requests relating to each such Service in respect of which there are Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification; and (iii) may, at its discretion, set other Anomaly Detection Thresholds. https://smartenergycodecompany.co.uk/download/2479
User	Smart Energy Code	Section G6.4 (a) (b)	Where a User sets any Anomaly Detection Threshold in accordance with Section G6.3, it shall: (a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of its User Systems; (b) before doing so: (i) take into account any guidance issued by the DCC as to the appropriate level of the Anomaly Detection Threshold; and (ii) have regard in particular to the forecast number of Service Requests provided by the User to the DCC in accordance with Section H3.22 (Managing Demand for User Interface Services) https://smartenergycodecompany.co.uk/download/2479
User	Smart Energy Code	Section G6.4(c)	Where a User sets any Anomaly Detection Threshold in accordance with Section G6.3, it shall: (c) after doing so, notify the DCC of that Anomaly Detection Threshold. https://smartenergycodecompany.co.uk/download/2479
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	3.2	Each User shall use reasonable steps to organise its business processes in such a manner that obviates the need for it to rely on the use of Fast-Track Notifications. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly	3.3	Where a User wishes to submit a Fast-Track Notification it shall, prior to doing so, contact the Service Desk and provide a justification for why it is necessary for them to do so.

Actor	SEC Document	Clause	Text
	Detection Procedures		https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	3.4	A User shall, in each User Role in relation to which it is required (or elects) to set ADTs, provide an Anomaly Detection Thresholds File to the DCC via an email to the Service Desk. The email shall include: (a) the SMSR reference number in the subject line of the email; and (b) the Anomaly Detection Thresholds File (of the form set out in clause of this document), Digitally Signed by a Private Key associated with a File Signing Certificate and provided to an Authorised Responsible Officer (ARO) in accordance with the SMKI RAPP. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	3.5	The User shall update the SMSR corresponding to the Anomaly Detection Thresholds File submission on the SSI. On receipt of an SMSR and accompanying Anomaly Detection Thresholds File, the DCC shall: (a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; (b) check that the format of the Anomaly Detection Thresholds File is correct; and (c) for Fast-Track Notifications, assess whether the justification provided is valid. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	3.6	Following the checks above the DCC shall verify that the ADT and Warning Threshold values provided are consistent with guidance issued by DCC. Where the DCC considers this not to be the case it shall contact a Senior Responsible Officer (SRO) acting on behalf of the User, by telephone using the contact details held by the DCC. The DCC shall request confirmation from the SRO as to whether the submitted Anomaly Detection Thresholds File should be applied. The SRO shall either: (a) provide confirmation to the DCC to apply the ADT and Warning Thresholds that it has submitted in which case the DCC shall apply the ADT and Warning Thresholds included within the Anomaly Detection Thresholds File and close the relevant SMSR; or (b) resubmit Anomaly Detection Thresholds File having had further regard to the guidance. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA -	3.7	The DCC shall validate and process Anomaly Detection Thresholds File submissions and shall either apply the ADT

Actor	SEC Document	Clause	Text
	Threshold Anomaly Detection Procedures		and Warning Thresholds or reject the submission, in accordance with the timescales set out immediately below: (a) for a notification of an Anomaly Detection Thresholds File that is not a Fast-Track Notification, within 72 hours of receipt of an Anomaly Detection Thresholds File by the DCC; or (b) for a Fast-Track Notification, within 24 hours of receipt of an Anomaly Detection Thresholds File by the DCC. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	3.8	Where the ADT and Warning Thresholds have been successfully applied, the DCC shall update and close the relevant SMSR. Where any of the checks outlined at clause 3.5 fail, the DCC shall not apply the ADT and Warning Thresholds and shall update the SMSR to reflect this and notify the User of the reason for the failure. https://smartenergycodecompany.co.uk/download/2263
DCC	Smart Energy Code	Section G6.6	The DCC: (a) shall, for each individual Service listed in the DCC User Interface Services Schedule, set an Anomaly Detection Threshold in respect of : (i) the total number of Critical Commands relating to that Service; and (ii) the total number of Service Requests relating to that Service in respect of which there are Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification; (b) shall set an Anomaly Detection Threshold in respect of a data value that has been agreed with the Security Sub-Committee within each type of Signed PreCommand; and (c) may, at its discretion, set other Anomaly Detection Thresholds. https://smartenergycodecompany.co.uk/download/2479
	Smart Energy Code	Section G6.7	Where the DCC sets any Anomaly Detection Threshold in accordance with Section G6.6, it shall: (a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems; and (b) before doing so consult, and take into account the opinion of, the Security SubCommittee as to the appropriate level of the Anomaly Detection Threshold. https://smartenergycodecompany.co.uk/download/2479

Actor	SEC Document	Clause	Text
DCC	Smart Energy Code	Section G6.8	The DCC shall notify the Security Sub-Committee of: (a) each Anomaly Detection Threshold that it sets; and (b) each Anomaly Detection Threshold that is set by a User and notified to the DCC in accordance with Section G6.4(c). https://smartenergycodecompany.co.uk/download/2479
DCC	Smart Energy Code	Section G6.9	Where the DCC is consulted by a User in relation to an Anomaly Detection Threshold which that User proposes to set, the DCC shall: (a) provide to the User its opinion as to the appropriate level of that Anomaly Detection Threshold; and (b) in doing so, have regard to the need to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the User Systems of that User. https://smartenergycodecompany.co.uk/download/2479
DCC, Users	Smart Energy Code	Section G6.10	The DCC and each User shall, in relation to each Anomaly Detection Threshold that it sets: (a) keep the Anomaly Detection Threshold under review, having regard to the need to ensure that it continues to function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System and/or User Systems (as the case may be); (b) for this purpose have regard to any opinion provided to it by the Security Sub-Committee from time to time as to the appropriate level of the Anomaly Detection Threshold; and (c) where the level of that Anomaly Detection Threshold is no longer appropriate, set a new Anomaly Detection Threshold in accordance with the relevant provisions of this Section G6. https://smartenergycodecompany.co.uk/download/2479
7.8.2.5.2 Operate Anomaly Detection Threshold			
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.1	Where the number of communications has exceeded the Warning Threshold, the DCC shall raise an Incident and send an email notification to the User's registered contact address on the DSMS. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly	4.1	Where the number of communications has exceeded the Warning Threshold, the DCC shall raise an Incident and send an email notification to the User's registered contact address on the DSMS.

Actor	SEC Document	Clause	Text
	Detection Procedures		https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.2	Following any such notification, a User shall use the "View Service Management Incident" Interface Transaction within the SSI to obtain details on the Warning Threshold exceeded using the SMSR reference number provided within the email notification. Each User shall investigate, and then update and assign the Incident to the Service Desk using the "Update Service Management Incident" Interface Transaction within the SSI. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.3	Each User shall investigate, and then update and assign the Incident to the Service Desk using the "Update Service Management Incident" Interface Transaction within the SSI. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AB - Service Request Processing Document	12.1	The DCC shall apply Threshold Anomaly Detection where an Anomaly Detection Threshold has been established under Section G6 (Anomaly Detection Thresholds) in respect of the Service Request or Signed Pre-Command. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	12.2	Where the DCC applies Threshold Anomaly Detection to either a Service Request or a Signed Pre-Command and the check is failed, the DCC shall notify the User and quarantine the Service Request or Signed Pre-Command. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	12.3	Where the DCC has quarantined a Service Request or Signed Pre-Command it shall maintain such quarantine until: (a) such time as the relevant User instructs the DCC to process the Service Request or Signed Pre-Command, in which case the DCC shall continue to process the Service Request or Signed Pre-Command in accordance with the provisions of this Service Request Processing document; (b) the Service Request or Signed Pre-Command is confirmed by the User to be anomalous or to otherwise require deletion, in which case the DCC shall delete it from the DCC Systems; or (c) the Service Request or Signed Pre-Command is required to be deleted in accordance with the Threshold Anomaly Detection Procedures, in which case the DCC shall delete it from the DCC Systems.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.4	Where the DCC has quarantined communications in accordance with the Service Request Processing Document the DCC shall raise an Incident and send an email notification to the affected User's registered contact address on the DSMS to inform the User of the ADT that has been exceeded. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.5	The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event for audit purposes and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.6	Each User shall use the "View Service Management Incident" Interface Transaction within the SSI to obtain details on the ADT exceeded using the Incident reference number provided within the email notification. The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" Interface Transaction within the SSI, which shall include the list of quarantined communications in a CSV format. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.7	Each User shall investigate and resolve the ADT exceeded event. Each User shall provide an email to the Service Desk indicating the action to be taken on each of the quarantined communications. The email shall include: (a) the Incident reference number in the subject line of the email; and (b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix	4.8	Each User shall update the Incident using the "Update Service Management Incident" Interface Transaction

Actor	SEC Document	Clause	Text
	AA - Threshold Anomaly Detection Procedures		within the SSI and assign to the Service Desk for further action. The DCC shall: (a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and (b) check that the format of the data is correct. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.9	Upon successful validation of all of the above checks the DCC shall perform the actions on the quarantined communications, notify the User, update and close the Incident. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.9	Upon successful validation of all of the above checks the DCC shall perform the actions on the quarantined communications, notify the User, update and close the Incident. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.10	Where any of the above validation steps fail the DCC shall update the Incident, reassign it to the User and notify the User of the reason for the failure. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.11	Pursuant to Section G6.6 of the Code the DCC shall set ADTs. Where a DCC set ADT has been exceeded, the DCC shall: (a) quarantine the communication(s) that have exceeded the ADT; (b) raise an Incident in accordance with the Incident Management Policy; and (c) determine the reasons for the Incident and take appropriate remedial action. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.12	DCC shall contact the User(s) impacted by the event by raising an Incident to notify them that their communication(s) have been quarantined. At an appropriate point during the investigation, DCC shall advise Users of the action that should be taken in respect of quarantined communications, which will be one of the following: (a) that quarantined communications must be deleted;

Actor	SEC Document	Clause	Text
			(b) that the User may decide whether quarantined communications should be processed or deleted; or (c) that no action should be taken by the User in respect of quarantined communications, which will result in the quarantined communications being archived for 30 days and subsequently deleted by the DCC. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.13	Upon being advised of the action to be taken, Users shall submit an email and Quarantined Communications Action File which specifies actions in respect of each quarantined communication and shall, where relevant, correspond with the actions as advised by the DCC. Such email shall be submitted to the Service Desk and shall include: (a) the DSMS Incident reference number notified in the subject line of the email; and (b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.14	The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident. https://smartenergycodecompany.co.uk/download/2263
User	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.15	The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" Interface Transaction within the SSI which shall include the quarantined communications(s) in a CSV format. Each User shall update the Incident using the "Update Service Management Incident" Interface Transaction within the SSI and assign the Incident to DCC for further action. The DCC shall: (a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

Actor	SEC Document	Clause	Text
			(b) check that the format of the data is correct. https://smartenergycodecompany.co.uk/download/2263
DCC	SEC Appendix AA - Threshold Anomaly Detection Procedures	4.16	Within 24 hours of receipt of a Quarantined Communications Action File, the DCC shall validate that Quarantined Communications Action File and shall either: (a) where the checks are successful, perform the actions on the quarantined communications and notify the User of successful completion of the notified actions once completed, via the SSI; or (b) where the checks are unsuccessful, update and reassign the Incident and notify the User of the reason for the failure. https://smartenergycodecompany.co.uk/download/2263

7.8.3 Manage Schedule

7.8.3.1 Introduction

This process area describes how Users can create, read and delete schedules for Service Requests. In respect of Service Requests that can be scheduled, Users can specify the initial time and date for execution of corresponding Commands as well as the frequency at which execution is to recur on the specified Device. Over the specified period with the specified frequency the User will receive a Service Response from the DCC.

Schedules are typically used to receive readings from Devices. Service Requests which can be scheduled are always Non-Critical, as the process for sending corresponding Non-Critical Commands to Devices does not require any DCC-User interactions, unlike the process for sending Critical Commands.

7.8.3.2 Scope

This process area includes:

- Create Schedule
- Delete Schedule

This process area involves but does not specifically describe Read (Non-Device) - Read Schedule.

7.8.3.3 Inputs

- ‘Create Schedule’ Service Request (SRV 5.1)
- ‘
- ‘Delete Schedule’ Service Request (SRV 5.3)

7.8.3.4 Actors

- Supplier
- Export Supplier
- Network Operator
- Other Users
- DCC
- Smart Meter
- GPF

7.8.3.5 Process Description

7.8.3.5.1 Create Schedule

The User composes a 'Create Schedule' Service Request (SRV 5.1) and sends it to the DCC. With the Service Request, the User specifies the target Device ID, the SRV to be scheduled, the frequency of execution, the start and, if applicable, end date.

The DCC receives the Service Request and completes Non-Device Service Request processing. If the SRV to be scheduled is capable of being scheduled and all the other checks are successful, the DCC creates a schedule for the Device. The DCC assigns it a unique Schedule ID and stores it on its systems. The DCC sends a Service Response (SRV 5.1) to the User.

At the time specified in the schedule, the DCC composes a Service Request (without a Digital Signature from the User) of the type defined in the schedule. The DCC completes Non-Critical Service Request processing, creates a corresponding Command and sends it to the Device specified in the schedule.

The Device receives the Command, executes it and sends a Response to the DCC. The DCC receives the Response and sends a Service Response to the User.

7.8.3.5.2 Read (Non-Device) - Read Schedule

Once a Schedule has been created, the User may read it. To do that the User composes a 'Read Schedule' Service Request (SRV 5.2) and sends it to the DCC. This process is described in Section 7.4.1.6.3 of the BAD.

7.8.3.5.3 Delete Schedule

If a schedule or schedules that the User created are no longer required, the User can delete them. To do that, the User composes a 'Delete Schedule' Service Request (SRV 5.3) and sends it to the DCC. The User may either delete a single schedule on a Device, or delete all schedules on a Device.

The DCC receives the Service Request, completes Non-Device Service Request processing, deletes the schedule(s) and sends a Service Response to the User.

There are a number of other triggers for the DCC to delete schedules. They include:

- On CoT, the DCC deletes the schedules created by Other Users. For more detail, see Section 7.5.2.5.1 of the BAD;
- On CoS, the DCC deletes schedules created by the Losing Supplier. For more detail, see Section 7.7.1.5.4 of the BAD;
- When Devices are Decommissioned. For more detail, see Sections 7.6.1.6.8 and 7.6.2.5.5 of the BAD.

7.8.3.6 Associated Process Areas

#	Process Areas
7.4.1	Read
7.5.2	Change of Tenant
7.6.1	Replace Communications Hub
7.6.2	Remove and Decommission Devices
7.7.1	Transitional Change of Supplier

7.8.3.7 Governance

Actor	SEC Document	Clause	Text
7.8.3.5.1 Create Schedule			
DCC	Smart Energy Code	Section H3.12	The DCC shall only accept a Service Request for a Future-Dated Service or a Scheduled Service that has an execution date that is later than the time on the date at which the Service Request is received by the DCC. No User may request a Future-Dated Service that has an execution date of more than 30 days after the date on which the Service Request is sent to the DCC. https://smartenergycodecompany.co.uk/download/2483
User	SEC Appendix AD - DCC User Interface Specification v1.1	2.6.2.2	A User may send a Service Request to create a schedule which is maintained and executed to initiate the sending of repeating Commands to a specified Device at regular defined intervals of time. Such schedules are created using the Create Schedule Service Request 5.1 and are stored within the DCC Systems. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	2.6.2.2	A User may send a Service Request to create a schedule which is maintained and executed to initiate the sending of repeating Commands to a specified Device at regular defined intervals of time. Such schedules are created using the Create Schedule Service Request 5.1 and are stored within the DCC Systems. https://smartenergycodecompany.co.uk/download/4639
User	SEC Appendix AD - DCC User Interface Specification v1.1	2.6.2.2	Each User shall ensure that the number of active schedules they have created and which relate to any particular Device does not exceed 99 Schedules. https://smartenergycodecompany.co.uk/download/2279

Actor	SEC Document	Clause	Text
	SEC Appendix AD - DCC User Interface Specification v2.0	2.6.2.2	Each User shall ensure that the number of active schedules they have created and which relate to any particular Device does not exceed 99 Schedules. https://smartenergycodecompany.co.uk/download/4639
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.8.45.3	Response Code E050301 - The DSPScheduleID does not exist or it is not owned by the User submitting the Service Request Response Code W050301 - The User does not have any schedules created against the specified Device. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface Specification v2.0	3.8.45.3	Response Code E050301 - The DSPScheduleID does not exist or it is not owned by the User submitting the Service Request Response Code W050301 - The User does not have any schedules created against the specified Device. https://smartenergycodecompany.co.uk/download/4639
7.8.3.5.3 Delete Schedule			
DCC	SEC Appendix AB - Service Request Processing Document	14.1	The DCC shall not continue to process any Service Requests (or associated Pre-Commands or Signed Pre-Commands) where the services have been cancelled in accordance with Sections H3.18 to H3.20 (Cancellation of Future-Dated or Scheduled Services). https://smartenergycodecompany.co.uk/download/2271

7.8.4 Service Request Processing

7.8.4.1 Introduction

This process area explains how the DCC processes Service Requests received from Users. There are three types of processing the DCC undertakes. This depends on whether Service Requests result in corresponding Commands destined for Devices forming part of a SMS or whether they are for notifying the DCC of an activity. Where Service Requests result in corresponding Commands destined for Devices, the difference in processing also depends on whether corresponding Commands are supply affecting.

7.8.4.2 Scope

This process area coves three types of processing:

- Critical Service Request processing
- Non-Critical Service Request processing
- Non-Device Service Request processing

This process area involves but does not specifically describe:

- Obtain Commands for Local Delivery. This is described in Section 7.2.2.6.2 of the BAD.
- Send Commands Locally. This is described in Section 7.2.2.6.3 of the BAD.

7.8.4.3 Actors

- User
- DCC

7.8.4.4 Process Description

7.8.4.4.1 Non-Critical Service Request Processing

The User composes a Service Request and sends it to the DCC. The DCC receives the Service Request, and in parallel the DCC:

- Sends an Acknowledgement to the User; and
- Applies the following checks:
    - Verifies the Service Request;
    - Confirms that the Service Request has been sent by a User whose right to send that Service Request has not been suspended, and that such User is acting in a User Role which is an Eligible User Role for that Service Request;
    - Confirms that the SMI Status of the Device identified in the Service Request is: (i) 'Commissioned'; (ii) 'Installed not Commissioned'; (iii) 'Whitelisted'; or (iv) 'Pending';
    - Checks Cryptographic Protection for the Service Request;
    - Confirms Validity of the Certificate used to Check Cryptographic Protection for the Service Request; and
    - Confirms that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request for all times within any date range requested:
        - Where there is no such date range, at the specified time for execution; or
        - Where there is no date range and no date for execution is specified, at the time at which the check is being carried out.

If any of the checks fail, the DCC rejects the Service Request and informs the User.

If the checks are passed, the DCC may apply Anomaly Detection to the Service Request. If the Anomaly Detection check fails, the DCC quarantines the Service Request. This process is described in Section 7.8.2.5.2 of the BAD.

If the Anomaly Detection check is applied and is passed, the DCC creates a corresponding Command (this includes the application of the Message Authentication Code to the Command) and sends the Command to the User and the Device specified in the Service Request.

The Device receives the Command, and executes it, and sends a Response to the DCC. The DCC receives the Response, and sends a Service Response to the User.

7.8.4.4.2 Critical Service Request Processing

The User composes a Service Request and sends it to the DCC. The DCC receives the Service Request from the User. In parallel, the DCC does the following things:

- Sends an Acknowledgment to the User; and
- Applies the following checks:
    - Verifies the Service Request;
    - Confirms that the Service Request has been sent by a User whose right to send that Service Request has not been suspended, and that such User is acting in a User Role which is an Eligible User Role for that Service Request;
    - Checks Cryptographic Protection for the Service Request;
    - Confirms Validity of the Certificate used to Check Cryptographic Protection for the Service Request; and
    - Confirms that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request for all times within any date range requested:
        - Where there is no such date range, at the specified time for execution; or
        - Where there is no date range and no date for execution is specified, at the time at which the check is being carried out.

If any of the checks fails, the DCC rejects the Service Request and informs the User.

If the checks are passed, the DCC then Transforms the Service Request into a Pre-Command, and sends the Pre-Command to the User.

The User receives the Pre-Command and carries out the following checks:

- Checks Cryptographic Protection for the Pre-Command;
- Confirms validity of the Certificate used to Check Cryptographic Protection for the Pre-Command; and
- Correlates the Pre-Command.

Where Correlation of the Pre-Command demonstrates that it is substantively identical to the Service Request the User signs the Pre-Command, and sends the Signed Pre-Command to the DCC.

The DCC receives the Signed Pre-Command, and does the following things:

- Sends an Acknowledgement to the User; and
- Applies the following checks:
    - Verifies the Signed Pre-Command;
    - Confirms that the Signed Pre-Command has been sent by a User whose right to send that message has not been suspended, and that such User is acting in a User Role which is an Eligible User Role for a Service Request of the type corresponding with the Signed Pre-Command;
    - Checks Cryptographic Protection for the Signed Pre-Command; and
    - Confirms Validity of the Certificate used to Check Cryptographic Protection for the Signed Pre-Command.

If any of the checks fails, the DCC rejects the Signed Pre-Command and notifies the User.

If the checks are passed, the DCC applies Anomaly Detection to Signed Pre-Command. If the Anomaly Detection check fails, the DCC quarantines the Service Request. This process is described in more detail in Section 7.8.2.5.2 of the BAD.

If the Anomaly Detection check is passed, the DCC applies a Message Authentication Code to the Signed Pre-Command, and then sends the Command to the User and to the Device specified in the Service Request.

The Device receives the Command, executes it and sends a Response to the DCC. The DCC receives the Response and sends a Service Response to the User.

7.8.4.4.3 Non-Device Service Request Processing

The User composes a Service Request and sends it to the DCC. The DCC receives the Service Request from the User, and completes the following checks:

- Verifies the Service Request;
- Confirms that the Service Request has been sent by a User acting in a User Role which is an Eligible User Role for that Service Request;
- Confirms SMI Status (Commissioned, Installed-not-Commissioned, Whitelisted or Pending). This does not apply to the following Service Requests:
    - Update Inventory;
    - Read Inventory;
    - Request WAN Matrix;
    - Device Pre-Notification;

- CH Status Update- Install Success;
- CH Status Update- Install No SM WAN;
- CH Status Update- Fault Return; and
- CH Status Update- No Fault Return.

- Checks the Cryptographic Protection;
- Confirms the Validity of the Certificate used to Check Cryptographic Protection for the Service Request;
- Confirm User is or will be Eligible User. This does not apply to the following Service Requests:
  - Read Inventory, Request WAN Matrix;
  - Device Pre-Notification;
  - CH Status Update- Install Success;
  - CH Status Update- Install No SM WAN;
  - CH Status Update- Fault Return; and
  - CH Status Update- No Fault Return.

The DCC sends a Service Response to the User notifying whether or not the Service Request was successfully processed.

7.8.4.4.4 Obtain Commands for Local Delivery

The User determines the Service Requests required. In addition to these Service Requests, the User needs an 'Update HAN Device Log' Service Request (SRV 8.11) to add an HHT to the CHF Device Log. The process for requesting all these Service Requests for local delivery is the same for requesting Service Requests for delivery over the WAN. Instead the User, specifies to the DCC that the corresponding Commands are for local delivery. The only difference is instead of sending the corresponding Commands to Devices and to the Supplier, the DCC only sends them to the Supplier.

The process is as follows: the Supplier composes the Service Request specifying that the corresponding Command is for local delivery. The DCC receives the Service Request and completes either Critical or Non-Critical Service Request processing (depending on the Service Request). The DCC sends a corresponding Command to the Supplier. The DCC does not send it to the Device. This process is described in Section 7.2.2.6.2 of the BAD

7.8.4.4.5 Send Commands Locally

The Supplier receives the Commands and makes them available to be downloaded to the HHT.

To send these Commands to Devices using the HHT, the Installer establishes an InterPAN between the HHT and the CHF. The process is described in Section 7.2.2.6.3 of the BAD.

The HHT stores all Device Alerts and Responses received from the CHF. The CHF also maintains a buffer of all Device Alerts and Responses whilst the SM WAN is unavailable. These will be sent to the DCC once the WAN becomes available.

7.8.4.5 Associated Process Areas

#	Process Areas
7.2.2	Install and Leave
7.8.2	Threshold Anomaly Detection

7.8.4.6 Governance

Actor	SEC Document	Clause	Text
7.8.4.4.1 Non-Critical Service Request Processing			
DCC	SEC Appendix AB - Service Request Processing Document	6.1	Subject to Clause 16 (Obligations of the DCC: Non-Device Service Requests), where the DCC receives a Service Request from a User, the DCC shall send an Acknowledgement to the User. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.1 (a)-(k)	(a) Verify the Service Request; (b) confirm that the Service Request has been sent by a User whose right to send that Service Request has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for that Service Request; (c) in the case of Non-Critical Service Requests (other than an 'Update Firmware' Service Request or a 'CoS Update Security Credentials' Service Request), confirm that the SMI Status of the Device identified in the Service Request is: (i) 'commissioned'; (ii) 'installed not commissioned'; (iii) 'whitelisted'; or (iv) 'pending'; (d) Check Cryptographic Protection for the Service Request; (e) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Service Request; (f) subject to Clause 6.2, in the case of Non-Critical Service Requests, confirm (using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory) that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request: (i) for all times within any date range requested; (ii) where there is no such date range, at the specified time for execution; or (iii) where there is no date range and no date for execution is specified, at the time at which the check is being carried out; (g) in the case of a 'CoS Update Security Credentials' Service Request, confirm that the User ID contained within each of

Actor	SEC Document	Clause	Text
			the Organisation Certificates included within the Service Request is associated with the User submitting the Service Request and that the MPRN or MPAN included within the Service Request is Associated with the Device identified within the Service Request; (h) in the case of a 'Restore HAN Device Log' or a 'Restore Gas Proxy Function Device Log' Service Request, confirm that the Device Log Data to be restored originates from a Communications Hub Function or Gas Proxy Function that forms (or formed immediately prior to its replacement) part of a Smart Metering System for which the User making such Service Request is (or, immediately prior to its replacement, was) the Responsible Supplier; (i) in the case of an 'Update Firmware' Service Request, confirm that the Hash calculated across the Manufacturer Image contained within the Service Request is the same as the entry within the Certified Products List (as identified by the Device ID, information in the Smart Metering Inventory and the firmware version specified in the Service Request); (j) in the case of any Service Request that contains any Certificates, Confirm Validity of those Certificates; and (k) in the case of an 'Update HAN Device Log' Service Request requesting the addition of a Smart Meter to the Device Log of a Communications Hub Function confirm (using the Registration Data and the MPRN or MPAN in the Service Request) that the User sending the Service Request is a Responsible Supplier in respect of that MPRN or MPAN. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.2	The step set out at Clause 6.1(f) shall not apply in the following circumstances (and, where it is necessary to identify a Responsible Suppler, the DCC shall do so using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory): (a) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Smart Meter sends a 'Join Service' Service Request to join that Gas Smart Meter to a Gas Proxy Function; (b) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Proxy Function sends a 'Restore GPF Device Log' Service Request to restore the Device Log of that Gas Proxy Function; or (c) the Service Request has been sent by a User acting in the User Role of 'Other User'.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.4 (a)	Subject to Clauses 8 (Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and Corresponding Pre-Commands), 9 (Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests), 10 (User and DCC Obligations: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters) and 16 (Obligations of the DCC: Non-Device Service Requests), where all of the requirements of Clause 6.1 are satisfied in respect of a Service Request, the DCC shall Transform the Service Request https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.3	Where any of the checks in Clause 6.1 are not satisfied in respect of a Service Request, the DCC shall not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Service Request (and, save where Clause 6.1(d) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	13.1	Where the DCC is required to send a Command, it shall only apply any necessary Message Authentication Code to the relevant communication and send the resulting Command if: (a) Threshold Anomaly Detection has been applied to the associated Service Request or Signed Pre-Command (or, where in response to a Service Request from an Eligible User a Command is to be Digitally Signed by the DCC, that Command prior to the addition of a Message Authentication Code); and (b) either (i) the Threshold Anomaly Detection check is passed; or (ii) the User that sent the original Service Request or Signed Pre-Command has instructed DCC to process a quarantined Service Request or Signed Pre-Command in accordance with Clause 12.3(a). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	13.2	Where the requirements of Clause 13.1 are met, the DCC shall apply the required Message Authentication Code (as required by the GB Companion Specification) to the relevant communication to create a Command and send that Command to (as specified in the originating Service Request): (a) the relevant Device (provided that this option is only available in respect of Devices associated with Commissioned Communications Hub Functions); and/or (b) the User who sent the originating Service Request via the DCC User Interface.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2271
7.8.4.4.3 Critical Service Request Processing			
User	SEC Appendix AB - Service Request Processing Document	3.1	Where a User receives a Pre-Command from the DCC, the User shall: (a) Check Cryptographic Protection for the Pre-Command; (b) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Pre-Command; and (c) subject to the requirements of Clause 3.1(a) and (b) being satisfied, Correlate the Pre-Command. https://smartenergycodecompany.co.uk/download/2271
User	SEC Appendix AB - Service Request Processing Document	3.2	Where Correlation of the Pre-Command demonstrates that it is substantively identical to the Service Request that led to the Pre-Command, the User may: (a) Digitally Sign the GBCS Payload of the Pre-Command to create the GBCS Payload of an associated Signed Pre-Command; and (b) send the associated Signed Pre-Command with its appropriate wrapper and Digital Signature to the DCC. https://smartenergycodecompany.co.uk/download/2271
User	SEC Appendix AB - Service Request Processing Document	3.3	Where applicable, Users must comply with their obligations under Section G3.25 (Supply Sensitive Check). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.1	Subject to Clause 16 (Obligations of the DCC: Non-Device Service Requests), where the DCC receives a Service Request from a User, the DCC shall send an Acknowledgement to the User. (a) Verify the Service Request; (b) confirm that the Service Request has been sent by a User whose right to send that Service Request has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for that Service Request; (c) in the case of Non-Critical Service Requests (other than an 'Update Firmware' Service Request or a 'CoS Update Security Credentials' Service Request), confirm that the SMI Status of the Device identified in the Service Request is: (i) 'commissioned'; (ii) 'installed not commissioned'; (iii) 'whitelisted'; or (iv) 'pending'; (d) Check Cryptographic Protection for the Service Request; (e) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Service Request; (f) subject to Clause 6.2, in the case of Non-Critical Service Requests, confirm (using the Registration Data, the

Actor	SEC Document	Clause	Text
			Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory) that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request: (i) for all times within any date range requested; (ii) where there is no such date range, at the specified time for execution; or (iii) where there is no date range and no date for execution is specified, at the time at which the check is being carried out; (g) in the case of a 'CoS Update Security Credentials' Service Request, confirm that the User ID contained within each of the Organisation Certificates included within the Service Request is associated with the User submitting the Service Request and that the MPRN or MPAN included within the Service Request is Associated with the Device identified within the Service Request; (h) in the case of a 'Restore HAN Device Log' or a 'Restore Gas Proxy Function Device Log' Service Request, confirm that the Device Log Data to be restored originates from a Communications Hub Function or Gas Proxy Function that forms (or formed immediately prior to its replacement) part of a Smart Metering System for which the User making such Service Request is (or, immediately prior to its replacement, was) the Responsible Supplier; (i) in the case of an 'Update Firmware' Service Request, confirm that the Hash calculated across the Manufacturer Image contained within the Service Request is the same as the entry within the Certified Products List (as identified by the Device ID, information in the Smart Metering Inventory and the firmware version specified in the Service Request); (j) in the case of any Service Request that contains any Certificates, Confirm Validity of those Certificates; and (k) in the case of an 'Update HAN Device Log' Service Request requesting the addition of a Smart Meter to the Device Log of a Communications Hub Function confirm (using the Registration Data and the MPRN or MPAN in the Service Request) that the User sending the Service Request is a Responsible Supplier in respect of that MPRN or MPAN. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.2	The step set out at Clause 6.1(f) shall not apply in the following circumstances (and, where it is necessary to identify a Responsible Suppler, the DCC shall do so using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory): (a) an Import Supplier that is the Responsible Supplier

Actor	SEC Document	Clause	Text
			for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Smart Meter sends a 'Join Service' Service Request to join that Gas Smart Meter to a Gas Proxy Function; (b) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Proxy Function sends a 'Restore GPF Device Log' Service Request to restore the Device Log of that Gas Proxy Function; or (c) the Service Request has been sent by a User acting in the User Role of 'Other User'. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.4 (b)	Subject to Clauses 8 (Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and Corresponding Pre-Commands), 9 (Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests), 10 (User and DCC Obligations: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters) and 16 (Obligations of the DCC: Non-Device Service Requests), where all of the requirements of Clause 6.1 are satisfied in respect of a Service Request, the DCC shall Transform the Service Request and: (b) in the case of a Critical Service Request, send the Transformed Service Request to the User who submitted the Service Request. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	6.3	Where any of the checks in Clause 6.1 are not satisfied in respect of a Service Request, the DCC shall not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Service Request (and, save where Clause 6.1(d) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	7.1	Where the DCC receives a Signed Pre-Command from a User, the DCC shall provide an Acknowledgement to the User and (whether before or after such Acknowledgement is sent) apply the following checks: (a) Verify the Signed Pre-Command; (b) confirm that the Signed Pre-Command has been sent by a User whose right to send that message has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for a Service Request of the type corresponding with the Signed Pre-Command;

Actor	SEC Document	Clause	Text
			(c) Check Cryptographic Protection for the Signed Pre-Command; and (d) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Signed Pre-Command. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	7.3	Where any of the checks in Clause 7.1 are not satisfied in respect of a Signed Pre-Command, the DCC shall not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall: (a) reject the Signed Pre-Command; and (b) save where Clause 7.1(d) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface. https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	7.2	Subject to Clauses 14 (Obligations of the DCC: Orchestration of Service Requests), where all of the requirements of Clause 7.1 are satisfied, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	13.1	Where the DCC is required to send a Command, it shall only apply any necessary Message Authentication Code to the relevant communication and send the resulting Command if: (a) Threshold Anomaly Detection has been applied to the associated Service Request or Signed Pre-Command (or, where in response to a Service Request from an Eligible User a Command is to be Digitally Signed by the DCC, that Command prior to the addition of a Message Authentication Code); and (b) either (i) the Threshold Anomaly Detection check is passed; or (ii) the User that sent the original Service Request or Signed Pre-Command has instructed DCC to process a quarantined Service Request or Signed Pre-Command in accordance with Clause 12.3(a). https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request Processing Document	13.2	Where the requirements of Clause 13.1 are met, the DCC shall apply the required Message Authentication Code (as required by the GB Companion Specification) to the relevant communication to create a Command and send that Command to (as specified in the originating Service Request): (a) the relevant Device (provided that this option is only available in respect of Devices associated with Commissioned Communications Hub Functions); and/or (b) the User who sent the originating Service Request via the DCC User Interface.

Actor	SEC Document	Clause	Text
			https://smartenergycodecompany.co.uk/download/2271
7.8.4.4.3 Non-Device Service Request Processing			
DCC	SEC Appendix AB - Service Request Processing Document	16.1 (a) & (b)	16.1 Where the DCC receives a Non-Device Service Request from a User, the obligations of the DCC under this Appendix shall be modified as follows (and where a Non-Device Service Request is not specifically identified below, they shall be applied un-modified): (a) the DCC shall not send an Acknowledgement in respect of the Service Request; (b) the checks set out in Clause 6.1 shall be modified as follows: (i) the check set out in Clause 6.1(c) does not apply to the following Service Requests: (A) 'Update Inventory'; (B) 'Read Inventory'; (C) 'Request WAN Matrix'; (D) 'Device Pre-notification'; (E) 'Communications Hub Status Update- Install Success'; (F) 'Communications Hub Status Update - Install No SM WAN'; (G) 'Communications Hub Status Update – Fault Return'; and (H) 'Communications Hub Status Update – No Fault Return'; and (ii) the check set out in the Clause 6.1(f) does not apply to the following Service Requests: (A) 'Read Inventory'; (B) 'Request WAN Matrix'; (C) 'Device Pre-notification'; (D) 'Communications Hub Status Update- Install Success'; (E) 'Communications Hub Status Update - Install No SM WAN'; (F) 'Communications Hub Status Update – Fault Return'; and (G) 'Communications Hub Status Update – No Fault Return'; https://smartenergycodecompany.co.uk/download/2271
	SEC Appendix AB - Service Request Processing Document	16.1(c)	the DCC shall not, in any event, be required to apply Threshold Anomaly Detection in relation to Non-Device Service Requests; https://smartenergycodecompany.co.uk/download/2271
DCC	SEC Appendix AB - Service Request	16.1 (d)	where the checks set out in Clause 6.1 (as modified by this Clause 16) are satisfied, the DCC shall not Transform the Service Request (as would otherwise be required by Clause 6) and shall instead send the User a Service Response

Actor	SEC Document	Clause	Text
	Processing Document		notifying the User whether or not the Non-Device Service Request has been successful, and where successful: (i) in the case of any Non-Device Service Request that changes or creates information held (or intended to be reflected) on the DCC Systems (including the Smart Metering Inventory), update the information held on DCC Systems accordingly; and/or (ii) in the case of a 'Read Inventory' or 'Request WAN Matrix' Service Request, include within the Service Response the relevant information requested by the Service Request; (iii) in the case of a 'Device Pre-Notification' Service Request, add the relevant Device to the Smart Metering Inventory with an SMI Status of 'pending'; (iv) in the case of a 'Create Schedule' Service Request, (A) create a schedule of the Service Request type identified in the 'Create Schedule' Service Request; (B) include within the Service Response the identifier of any schedule that has been successfully created; (C) at each point in time set out in the schedule (and subject to the further arrangements set out in the DCC User Interface Specification), create a Service Request (without a Digital Signature from the User) of the appropriate type and in relation to the relevant Device (in each case as specified in the original 'Create Schedule' Service Request); (D) process the Service Requests referred to in (C) above in accordance with Clause 6.1 as if they had been received from the User that sent the original 'Create Schedule' Service Request, provided that the checks identified under Clause 6.1(c) and 6.1(d) do not apply; https://smartenergycodecompany.co.uk/download/2271

7.8.5 Error Processing

7.8.5.1 Introduction

This process area describes the error handling processes that the DCC has in place when managing communications between Users and SMSs.

7.8.5.2 Scope

This process area covers Error Processing.

This process area involves but does not specifically describe:

- Non-Critical Service Request processing. This is described in Section 7.8.4.4.1 of the BAD.
- Critical Service Request processing. This is described in Section 7.8.4.4.2 of the BAD.
- Non-Device Service Request processing. This is described in Section 7.8.4.4.3 of the BAD.

7.8.5.3 Actors

- User
- DCC
- Device

7.8.5.4 Process Description

7.8.5.4.1 Error Processing

In response to each Service Request / Signed Pre-Command the DCC receives from Users, the DCC sends the User an Acknowledgement. The Acknowledgement indicates either of the following:

- That the Service Request has been accepted by the DCC Systems (Code 200);
- That the Service Request has not been accepted by the DCC Systems and the problem needs to be resolved by the User (Code 200 and 300);
- That the DCC Systems are unable to accept the Service Request (Code 500 and 503).

For Code 500 and 503, the User raises an Incident. For more detail, see Section 7.9.4 of the BAD.

Once the Service Request / Signed Pre-Command has been accepted by the DCC System, the DCC processes it and at the end of the processing sends another Acknowledgement to the User. The Acknowledgement indicates either of the following:

- No action required to be taken by the User (Acknowledgement is prefixed with I for Information either I0 Success or I99 Acknowledgement);
- No action required to be taken by the User (Acknowledgment is prefixed with W for Warning);
- User needs to take action (Acknowledgment is prefixed with E for Error).

The Error Handling Strategy sets out the steps the User needs to take in relation to each Acknowledgment prefixed with an E.

A complete list of the Error handling response codes are detailed in the DUIS section 3.5.10

The outcome of this process is:

- The User makes the necessary changes and submits a valid Service Request; or
- Having satisfied itself that the original Service Request was valid, the User raises an Incident. This process is described in Section 7.9.4.5.1 of the BAD.

Errors may also occur in communications between the DCC and Devices and are managed as follows:

- For Future Dated Service Requests, the DCC checks whether the User is eligible for it on the execution date. If not, the DCC sends a DCC Alert to the User.

DCC Alert Code	Alert Name	Event	Trigger
N7	"DSP Scheduled" / "Future Dated Response Pattern (DSP)" access control failure	"DCC Scheduled" / "Future Dated Response Pattern (DSP)" access control failure (Authorisation, Device status)	User not eligible to send a Future Dated Response Pattern DSP Command.

- If the DCC receives no Response to a Command it has sent to a Device, it re-sends the Command.
- If the retry still produces no Response, the DCC waits for a period of time (the back-off period) before trying again.

The number of retries is configurable by the DCC. The retry period and the back-off period depend upon the mode of operation and are shown in the table below:

Table 13. Retry and back-off periods

Mode of Operation	Initial Retry Period	Back-Off Period	Final Retry Period
On Demand Request	Configurable period by the DCC (held within the DCC systems) based on the following factors: • DCC Target Response Time • HAN Transfer Time • Device Processing Time • Device Wakeup Time	N/A	N/A
Future Dated Response Pattern (Device)	2 hours	2 hours	Future Dated Response Pattern (Device) Target Response Time + 60 minutes
Future Dated Response Pattern (DSP)	2 hours	2 hours	Future Dated Response Pattern (DSP) Target Response Time + 60 minutes

DCC Scheduled	2 hours	2 hours	DCC Scheduled Target Response Time + 60 minutes

If following the retry and back off period there is still no Response and the number of allowed retries has been completed, the DCC sends a DCC Alert back to the User.

Table 14. DCC Error Alerts

DCC Alert Code	Alert Name	Event	Trigger
N10	"Future Dated Response Pattern (Device)" Command time-out	"Future Dated Response Pattern (Device)" Command time-out	"Future Dated Response Pattern (Device)" Command response not received from the Device within the Target Response Time from the ExecutionDateTime
N11	"DSP Scheduled" / "Future Dated Response Pattern (DSP)" Command time-out	"DCC Scheduled" / "Future Dated Response Pattern (DSP)" Command time-out	"DCC Scheduled" Schedule instance / "Future Dated Response Pattern (DSP)" Command not sent to or response not received from the Device within the Target Response Time from the ExecutionDateTime
N12	Failure to deliver Command to Device	Failure to deliver Command to Device	Failure to receive an acknowledgement notification from a CSP via the SM WAN for an "On Demand" or "Future Dated" Command
N13	Failure to receive Response from Device	Failure to receive Response from Device	Failure to receive a response from a Device for an "On Demand" Command or "Future Dated" Command Acknowledgement
N14	Sequenced Request Failure	Sequenced Request Failure	Previous Command in sequence failed or timed-out
N15	Sequenced Request received out of order	Sequenced Request received out of order	Preceding Request not received during "Wait Period"

7.8.5.5 Associated Process Areas

#	Process Areas
7.8.4	Service Request Processing
7.9.4	Manage Incidents

7.9 Manage Service

Manage Service describes the processes, functions and Services that the DCC has in place to support the provision of Communication Services. This functional area covers:

- Order and Return Communications Hub – this process area describes how Suppliers order CHs from the DCC, and how they can return them (whether due to faults, recall or other causes).
- Manage Service – this process area describes how the DCC manages demand for its Communication Services, what other functions the DCC has in place to support the provision of Communication Services, and how the DCC performance in relation to the provision of the Communication Services is measured.
- Manage Demand – this process area described how the DCC manages demand for Service Requests.
- Manage Incident – this process area describes how the DCC manages Incidents. The primary focus is not on the internal problem resolution of the different actors, but rather how responsibility for Incidents is allocated, managed and reported on, and how incidents are either closed, or become Problems for further work.
- No WAN Issues – this process area describes the process for dealing with instances of WAN unavailability.
- Recall Communications Hub – this process area describes the process for recalling CHs.
- Elective Communications Services – this process area describes how Parties go about requesting Elective Communications Services from the DCC.

7.9.1 Order and Return Communications Hub

The following section applies to both Single Band and Dual Band Communications Hubs.

7.9.1.1 Introduction

CHs form part of SMSs installed in the Energy Consumers premises by Suppliers. They are provided and owned by the DCC.

Ordering and returns of CHs is primarily managed through a CH Ordering System or an OMS provided by the DCC. Suppliers use this system to provide their CH Forecasts, submit and manage CH orders and manage their returns. The OMS is available via the SSI or a public internet link.

7.9.1.2 Scope

This process area includes:

- Order Communications Hub
- Communications Hub Status Update - Fault Return and No Fault Return

This process area involves but does not specifically describe:

- Install and Commission. This process is described in Section 7.2.1 of the BAD.
- Install and Leave. This process is described in Section 7.2.2 of the BAD.
- Replace Communications Hub. This process is described in 7.6.1 of the BAD.

7.9.1.3 Inputs

- 'Communications Hub Status Update – Fault Return' Service Request (SRV 8.14.3)
- 'Communications Hub Status Update – No Fault Return' Service Request (SRV 8.14.4)

7.9.1.4 Actors

- Supplier
- DCC
- Panel

7.9.1.5 Prerequisites

A Party created a CH Forecast covering the period of 24 months commencing with the sixth month after the end of the month in which the forecast is submitted to the DCC. A CH Forecast consists of the following:

- A forecast of the number of CHs that the Party requires to be delivered each month over the specified date range; and
- Each monthly forecast includes the aggregate number of CHs to be delivered each month, the number of CH to be delivered in respect of each Region. For the first 10 months for which the CH Forecast relates to, the number of CHs of each HAN Variant to be delivered in respect of each Region.

The Party submitted the CH Forecast to the DCC no later than the fifth Working Day prior to the last Working Day of each month via the CH Ordering System, or if forecast has not been submitted by the due date, the DCC makes certain assumptions about a Party's requirements. These assumptions are explained in SEC Section F5.6.

7.9.1.6 Process Description

7.9.1.6.1 Order Communications Hub

A Party submits a Communications Hub Order for CHs and CH Auxiliary Equipment via the CH Ordering System. A CH Order must:

- Be for a single Region, and specify which Region it relates to;
- Be for the Delivery Month;
- Be for one or more Delivery Locations;
- Specify the Delivery Date;
- Specify a Delivery Quantity for each Delivery Location;
- Specify the preferred date within the Delivery Month for each Delivery Location; and
- Specify the number of Communications Hub Auxiliary Equipment to be delivered to each Delivery Location.

Parties must ensure that its CH Order would not result in a requirement for the DCC to deliver a single Consignment that comprises only CH Auxiliary Equipment.

The DCC acknowledges the order, and within five Working Days checks the order against the current forecast and notifies the Party:

- If the order lies within the tolerances prescribed in the SEC, the order is considered compliant, and is accepted; or
- If the order lies outside the tolerances, the DCC may decide to accept it in full, accept it in part, or reject it.

The Party can cancel accepted orders, but the DCC may charge the Party for any costs incurred by cancellation.

The DCC delivers the order in accordance with the delivery requirements set out in Appendix H- CH Handover Support Materials.

The Party inspects the delivery, and may reject it if the delivery does not match the order, or the CH Products are damaged. The Party confirms acceptance or rejection through the CH Ordering System, and makes any rejected Consignments available for collection.

The Party confirms whether the delivery of CH Products has been made in compliance with the order within five Working Days after the applicable Delivery Date.

The DCC collects any rejected orders and makes arrangements to replace them.

7.9.1.6.2 Communications Hub Status Update – Fault Return and No Fault Return

CHs may be returned to the DCC in the following circumstances:

- At the Supplier's discretion (typically as a result of a fault found during installation, or following a CH replacement); or
- At the request of the DCC (typically a Product Recall or Technology Refresh).

Following the CH replacement, Suppliers may return the CH to the DCC at any time, but must do so within 90 days of its removal.

Where a Supplier identifies a potential CH fault, it may complete the CH Availability and Diagnostics Check procedure prior to raising an Incident with the DCC.

Where CHs are being returned at the request of the DCC, they must be returned by:

- The Supplier who ordered them (for CHs which have not been installed);
- The Lead Supplier (for CHs which are installed and not yet removed); or
- The Supplier who removed them (for CHs which have been removed).

The Supplier notifies the DCC that it intends to return a stated number of CHs on a specific date and to a specific location.

The notification is made by the Supplier either via the DCC Service Desk or through a Service Request (a 'Communications Hub Status Update – Fault Return' Service Request (SRV 8.14.3) or a 'Communications Hub Status Update – No Fault Return' Service Request (SRV 8.14.4)).

The Supplier composes a Service Request and sends it to the DCC. the DCC receives the Service Request, completes Non-Device Service Request processing and sends a Service Response. If the checks are successful, the DCC creates an individual record for each returned CH. For each returned CH, this contains all details received by the DCC from the Supplier within the Service Request or provided via the DCC Service Desk. This is made available to the Supplier within seven days after the return of the CH via the CH Ordering System.

The Supplier uses the CH Ordering System to request a Return Materials Authorisation (RMA). This includes the CHF identifier for each Device, Supplier contact details and a preferred DCC Return Location and Return Date. The preferred Return Date needs to be on a Working Day at least five Working Days following the date that the request for the RMA is submitted.

The DCC authorises the RMA, and returns a unique booking reference, including a delivery time slot, RMA reference and DCC contact details.

The Supplier physically returns the CH Products with a return Delivery Note which contains the following information:

- Booking reference for the return delivery as supplied by DCC;
- Return date and return Delivery Time;
- Party Signifier;

- DCC returns location;
- List of all CHF identifiers being returned; and
- (Where one or more pallets are to be returned), the pallet identifiers for each pallet being returned.

The DCC verifies that the return matches the record, and signs the return Delivery Note.

The DCC may choose to carry out CH Fault Diagnosis to confirm the reason code and responsibility. The following process takes place:

- The DCC notifies the Supplier within 10 days that it wishes to carry out CH Fault Diagnosis. If there is no notification received, the Supplier's reason code stands;
- The DCC completes CH Fault Diagnosis within 35 days, and reports to the Supplier. If there is no CH Fault Diagnosis within 35 days, the Supplier's reason code stands; and
- The Supplier has 35 days to respond to the DCC's report, otherwise the DCCs CH Fault Diagnosis stands.

The DCC compensates Suppliers for faults which are the responsibility of the DCC in accordance with the formula defined in the SEC. Either Party can ask the Panel to adjudicate in the event of a Dispute.

The DCC may choose to recondition any returned CHs, subject to any Data being removed before a delivery, or dispose of them.

The DCC provides the Panel and the Parties with a periodic report on the number of returned CH and the reasons for their return.

7.9.1.7 Associated Process Areas

#	Process Areas
7.2.1	Install and Commission
7.2.2	Install and Leave
7.6.1	Replace Communications Hub

7.9.1.8 Governance

Actor	SEC Document	Clause	Text
7.9.1.6.1 Order Communications Hub			
DCC	Smart Energy Code	Section F5.1	The DCC shall ensure that Communications Hub Device Models are made available to be ordered by Parties under this Section F5 such that the Parties can order Communications Hubs that provide for each and every combination of HAN Variant and WAN Variant; save that this Section F5 does not apply to Special Installation Mesh Communications Hubs. All references in this Section F5 to Communications Hubs shall be deemed to exclude Special Installation Mesh Communications Hubs

			https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F5.20	Subject to Section F5.23, the DCC shall make one or more systems (the CH Ordering System) available to other Parties, which Parties can access remotely (via such means, and subject to any security requirements, as are set out in the CH Support Materials). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F5.21	The DCC shall ensure that the CH Ordering System is available in advance of the time from which other Parties are obliged to submit Data via the CH Ordering System, and at all times thereafter (subject to Planned Maintenance undertaken in accordance with Section H8.3). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F5.22	The DCC shall ensure that the CH Ordering System allows each Party to: (a) submit details of its forecasts, orders and returns of Communications Hubs and/or Communications Hub Auxiliary Equipment, as required in accordance with this Section F5, Sections F6 (Delivery and Acceptance of Communications Hubs) and F8 (Removal and Return of Communications Hub), and the CH Support Materials; (b) view Data regarding the status of such submissions (but only its own submissions), and (where relevant) receive responses from the DCC regarding such submissions; and (c) view the SM WAN Coverage Database https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.2	For the purposes of this Section F5, a "Communications Hub Forecast" means an estimate of the future requirements of a Party for the delivery to it of Communications Hubs by the DCC, which: (a) is submitted by that Party to the DCC; (b) covers the period identified in Section F5.3; and (c) complies with the requirements of Section F5.4. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.3	Each Communications Hub Forecast shall cover the period of 24 months commencing with the sixth month after the end of the month in which the forecast is submitted to the DCC. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.4	Each Communications Hub Forecast shall: (a) comprise a forecast of the number of Communications Hubs that the Party requires to be delivered to it in each month of the period to which it relates; (b) set out that forecast for each such month by reference to: (i) the aggregate number of Communications Hubs to be delivered; (ii) the number of Communications Hubs to be

			delivered in respect of each Region; and (iii) (for the first 10 months of the period to which the forecast relates) the number of Communications Hubs of each HAN Variant to be delivered in respect of each Region; and (c) include such further information and be provided in such form as may be set out in the CH Handover Support Materials at the time of its submission. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.5	Each Supplier Party, and each other Party that intends to order Communications Hubs in the future, shall: (a) submit a Communications Hub Forecast to the DCC by no later than the 5th Working Day prior to the last Working Day of each month; (b) submit each Communications Hub Forecast via the CH Ordering System; (c) take reasonable steps to ensure that the information contained in each Communications Hub Forecast is accurate and up to date; and (d) ensure that it submits a forecast that will enable it to submit a Communications Hub Order that meets the requirements of Section F5.12. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F5.6	A Party that has not submitted a Communications Hub Forecast for a Region during a month in accordance with this Section F5 shall be deemed to have submitted a forecast which specified: (a) for the first 23 months of the period covered by the forecast, the same number of Communications Hubs as the Party forecast for the corresponding month in its previous forecast; (b) for the first 9 months of the period covered by the forecast, the same number of each HAN Variant as the Party forecast for the corresponding month in its previous forecast; (c) for the 10th month of the period covered by the forecast, the number of each HAN Variant that results from applying the same proportions of each HAN Variant as applies to the 9th month of the period pursuant to paragraph (b) above; and (d) for the 24th month of the period covered by the forecast, zero Communications Hubs. https://smartenergycodecompany.co.uk/download/2476
DCC	SEC Appendix H - CH Handover Support Materials	3.1	Following receipt of a Communications Hub Forecast or the deeming of a Communications Hub Forecast by the DCC in accordance with Section F5.6, the DCC shall notify via email to all OMS Accounts associated with that Party that the following information is available via the OMS: (a) a unique reference for the relevant Communications Hub Forecast; and (b) the associated date, which shall be: (i) where a Communication Hub Forecast has been submitted by a Party,

			the date of submission; or (ii) where the Communications Hub forecast has not been submitted by a Party, the date at which the DCC has deemed that forecast. https://smartenergycodecompany.co.uk/download/2333
Supplier	Smart Energy Code	Section F5.7	For the purposes of this Section F5, a "Communications Hub Order" means an order by a Party for the delivery to it of Communications Hubs and/or Communications Hub Auxiliary Equipment by the DCC, which: (a) is submitted by that Party to the DCC; and (b) satisfies the requirements of Section F5.8 https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.8	Each Communications Hub Order shall (subject to any further requirements set out in the CH Handover Support Materials): (a) relate to a single Region, and identify the Region to which it relates; (b) relate to the delivery of Communications Hubs and/or Communications Hub Auxiliary Equipment in the 5th month after the end of the month in which that Communications Hub Order is submitted to the DCC (the "Delivery Month"); (c) specify the addresses of the location or locations (each a "Delivery Location") at which the delivery of the Communications Hubs and/or Communications Hub Auxiliary Equipment is required, each of which locations must be in Great Britain but need not be in the Region to which the relevant Communications Hub Order relates; (d) specify, in accordance with Section F5.12, the number (if any) of Communications Hubs of each Device Model to be delivered to each Delivery Location (in each case, a "Delivery Quantity"); (e) specify the preferred date within the Delivery Month on which the delivery to each Delivery Location is required (provided that the actual delivery date within the Delivery Month for each Delivery Location (in each case, a "Delivery Date") shall be determined in accordance with the CH Handover Support Materials); (f) specify the number and type of the Communications Hub Auxiliary Equipment (if any) to be delivered to each Delivery Location; and (g) include such further information and be provided in such form as may be set out in the CH Handover Support Materials at the time of its submission. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.9	In respect of each Communications Hub Order submitted in respect of a Region, the Communications Hubs and/or Communications Hub Auxiliary Equipment to be delivered to each Delivery Location on each Delivery Date shall be a "Consignment".

			https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.10	In order for a Communications Hub Order to be a compliant order, the order must comply with the requirements of this Section F5.10. A Party is not obliged to submit a compliant order, but a non-compliant order may be amended by the DCC in accordance with Section F5.17. The requirements of this Section F5.10 are, for each Communications Hub Order submitted by a Party in respect of a Region, that the aggregate (for all Consignments) of the Delivery Quantities of each HAN Variant for the Delivery Month must be: (a) greater than or equal to the higher of: (i) 50% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 10th month prior to the start of the Delivery Month; and (ii) 80% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by the Party in the 7th month prior to the start of the Delivery Month; and (b) less than or equal to the lower of: (i) 120% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 7th month prior to the start of the Delivery Month; and (ii) 150% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 10th month prior to the start of the Delivery Month. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.11	For the purposes of Section F5.10, in calculating, by reference to earlier forecast numbers: (a) the minimum aggregate of the Delivery Quantities, any fractions of a number shall be rounded down; and (b) the maximum aggregate of the Delivery Quantities, any fractions of a number shall be rounded up. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F5.12	For each Party's Communications Hub Order relating to a Region, the aggregate of the Delivery Quantities (for all Device Models taken together) that may be specified for each Consignment may not (unless such number is zero) be less than the minimum delivery quantity set out in the CH Handover Support Materials at the time at which the relevant Communications Hub Order is submitted. https://smartenergycodecompany.co.uk/download/2476
Supplier	SEC Appendix H - CH Handover	3.4	A Party shall provide Delivery Locations on the OMS using the CH Ordering profile and shall provide and maintain the following information for each Delivery Location: (a) the full delivery address;

	Support Materials		(b) operating hours; and (c) the name, email address, and telephone number for a nominated contact in relation to Communications Hubs Orders. https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.5	The DCC shall ensure that the OMS allows each Party using the CH Ordering profile to select a maximum of two Delivery Locations for each Communications Hub Order. https://smartenergycodecompany.co.uk/download/2333
Party	Smart Energy Code	Section F5.15	Each Party shall submit its Communications Hub Orders via the CH Ordering System. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F5.13	Each Party other than the DCC: (a) may submit one Communications Hub Order in relation to each Region in any month; (b) shall submit a Communications Hub Order in relation to a Region in a month if the aggregate of the Delivery Quantities for one or more Device Models required for a compliant order in accordance with Section F5.10 is greater than zero; and (c) where it fails to submit an order where it is required to do so in accordance with Section F5.13(b), shall be deemed to have submitted a Communications Hub Order for a Delivery Quantity of Communications Hubs of each Device Model equal to the minimum aggregate Delivery Quantity required in respect of that Device Model for a compliant order in accordance with Section F5.10 (and the remaining details of such deemed order shall be determined by the DCC in accordance with the CH Handover Support Materials). https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F5.14	Each Party shall ensure that any Communications Hub Order which it elects or is required to submit in any month is submitted by no later than the 5th Working Day prior to the last Working Day of that month. https://smartenergycodecompany.co.uk/download/2476
DCC	SEC Appendix H - CH Handover Support Materials	3.6	Where, in accordance with Section F5.13(c), the DCC deems the quantities of Communications Hubs to be included in a Communications Hub Order for a Party, it shall inform via email notification to all OMS Accounts associated with that Party that a deemed order has been made and make available, via the OMS, details of the deemed quantity of each Device Model and of any Communications Hub Auxiliary Equipment. https://smartenergycodecompany.co.uk/download/2333

Party	SEC Appendix H - CH Handover Support Materials	3.7	Where a Party receives a notification in accordance with clause 3.6, that Party shall specify a Delivery Location or Delivery Locations for the Communications Hub Order within two Working Days and shall comply with, and provide the further information set out in, clauses 3.13 and 3.14. https://smartenergycodecompany.co.uk/download/2333
Party	SEC Appendix H - CH Handover Support Materials	3.8	Where a Party has not specified a Delivery Location or Delivery Locations, or provided the other information required, in accordance with clause 3.7, the DCC shall specify the Communications Hub Order Delivery Location or Delivery Locations using Delivery Locations provided for any previous orders and, specify the further information set out in, clauses 3.13 and 3.14. https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.9	Where the DCC has determined the Delivery Location(s) pursuant to clause 3.8 and the relevant Party has not notified the DCC within 30 days of the DCC's notification pursuant to clause 3.6, that the extant delivery details are correct, then the relevant Party shall be deemed to have requested cancellation of the Consignment or Consignments (and Section F5.19 shall be deemed to apply). The DCC shall notify that such a request has been deemed, via an email to all OMS Accounts associated with that Party. https://smartenergycodecompany.co.uk/download/2333
Party	SEC Appendix H - CH Handover Support Materials	3.10	When submitting a Communications Hub Order, each Party shall ensure that only such WAN Variants and Communications Hub Auxiliary Equipment are ordered as it may reasonably require to: (a) complete planned installations using the WAN Variants and Communication Hub Auxiliary Equipment that are indicated as required for the relevant Installation Location(s) on the SM WAN Coverage Database; (b) conform to the proportions of T1 Aerial Type and T2 Aerial Type estimated as necessary within the CH Supporting Information to provide for Mesh Communications Hub installations; and (c) maintain sufficient stock to resolve coverage Incidents and Communication Hub faults as described in the CH Installation and Maintenance Support Materials https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.11	Where a Party submits a Communications Hub Order for the Central Region or the South Region that results in greater than 10% of the total number of Communications Hubs in the Communications Hub Order being Mesh Communications Hubs, the DCC may request an explanation why the quantity of Mesh Communications Hubs ordered is required and where such an explanation is requested the Party shall provide the explanation via email promptly.

			https://smartenergycodecompany.co.uk/download/2333
Party	SEC Appendix H - CH Handover Support Materials	3.12	Each Party shall ensure that its Communications Hubs Order is such that it would not result in a requirement for the DCC to deliver a single Consignment that comprises only Communications Hub Auxiliary Equipment. https://smartenergycodecompany.co.uk/download/2333
Party	SEC Appendix H - CH Handover Support Materials	3.13	In addition to complying with the requirements set out in Section F5.8, for each Communications Hub Order that it submits, a Party shall: (a) request delivery to no more than two Delivery Locations per Region; (b) request delivery to each Delivery Location no more than once in any single week; and (c) specify a Delivery Date and associated Delivery Window that is within Working Hours. https://smartenergycodecompany.co.uk/download/2333
Party	SEC Appendix H - CH Handover Support Materials	3.14	A Party submitting a Communications Hub Order shall ensure that for each delivery that will result from that Communications Hub Order and in relation to the Region to which the Order relates: (a) the number of each WAN Variant is an integer multiple of the quantity of Communications Hubs that are contained in a carton, as specified in Annex B of this document; (b) the total number of Communications Hubs ordered is such that a pallet layer contains the total number of cartons for that pallet layer as specified in Annex B of this document; and (c) the total number of Communications Hubs is greater than or equal to the quantity of Communications Hubs contained in a complete standard pallet, as specified in Annex B of this document https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.15	The DCC shall package and load Communications Hubs as described in Annex D of this document. https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.16	The DCC shall make available to a Party via the CH Ordering System at least one contact telephone number and email address for the DCC which is relevant to each Communications Hub Order placed by that Party for the purposes of allowing a Party to request amendments to Delivery Locations, Delivery Dates, or Delivery Windows in relation to a Communications Hub Order that it has submitted. https://smartenergycodecompany.co.uk/download/2333

Party	SEC Appendix H - CH Handover Support Materials	3.17	A Party shall make available to the DCC via the CH Ordering System at least one contact telephone number and email address for that Party which is relevant to each of its Communications Hub Orders, which shall be used by the DCC for any email or telephone communications regarding the order. https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.18	For each Communications Hub Order, where the DCC identifies an opportunity for consolidation of a Party's Consignments into a single delivery vehicle, the DCC may request permission to amend a Communications Hub Order to enable such consolidation. The agreement of the Party to such a request shall not be unreasonably withheld https://smartenergycodecompany.co.uk/download/2333
DCC	Smart Energy Code	Section F5.16	Where the DCC receives a Communications Hub Order from a Party via the CH Ordering System, the DCC shall: (a) promptly acknowledge receipt of that order; and (b) within five Working Days of its receipt of the order, notify the Party either that: (i) the order satisfies the requirements of Section F5.8, is a compliant order in accordance with Section F5.10 and was submitted in accordance with Section F5.14 (and is therefore accepted); or (ii) the order does not satisfy some or all of the conditions in (i) above (and is therefore subject to Section F5.17). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F5.17	Where this Section F5.17 applies in respect of a Party's Communications Hub Order, the DCC shall (having regard to the nature, extent and effect of the Party's breach of this Section F5 and/or of the order's non-compliance under Section F5.10, and having regard to the requirements of the DCC Licence) take all reasonable steps to accommodate the order (in whole or part, or subject to amendments). The DCC shall, by the end of the month in which such order is received by the DCC, notify the Party (in each case giving reasons for its decision) that: (a) the order is accepted in its entirety; (b) the order is accepted in part or subject to amendment; or (c) the order is rejected. https://smartenergycodecompany.co.uk/download/2476
DCC	SEC Appendix H - CH Handover Support Materials	3.19	The notification that the DCC is required to provide pursuant to Section F5.16 shall be provided by the DCC via email to all OMS Accounts associated with that Party notifying that information is available via the OMS. Such information will consist of the following; (a) an OMS Order Reference; and (b) confirmation that the Communications Hub Order is: (i) compliant with the requirements of Section F5 (and therefore accepted without

			amendment); or (ii) not compliant with the requirements of Section F5. https://smartenergycodecompany.co.uk/download/2333
DCC	SEC Appendix H - CH Handover Support Materials	3.20	Where a notification has been made of the type set out in clause 3.19(b)(ii), the further notification that DCC is required to provide pursuant to Section F5.17 shall be provided by the DCC via email to all OMS Accounts associated with that Party notifying that information is available via the OMS. The information on the OMS shall state whether the Order is: (a) accepted, in full and is not subject to amendment; (b) accepted, in part or is subject to amendment; or (c) rejected; and in each case (d) the reason for the decision. https://smartenergycodecompany.co.uk/download/2333
Supplier	Smart Energy Code	Section F5.19	Each Party that has had a Communications Hub Order accepted by the DCC may cancel one or more of the Consignments arising from that Communications Hub Order; provided that the Party must notify the DCC of such cancellation at least 48 hours in advance of the Delivery Date for the Consignment. A Party which cancels one or more Consignments in accordance with this Section F5.19 shall be liable to reimburse the DCC for all reasonable costs and expenses incurred by the DCC as a result of such cancellation. The DCC shall notify the Party of such costs and expenses as soon as reasonably practicable after notice of the cancellation is given. Such compensation shall be included in the next Invoice to be produced by the DCC following its calculation. The DCC shall, where requested not less than 10 Working Days in advance of the Delivery Date, provide a nonbinding estimate of the costs and expenses it is likely to incur in the event that a Party opts to cancel a Consignment (such estimate to be provided not less than 5 Working Days in advance of the Delivery Date). The DCC shall take all reasonable steps to ensure the estimate is accurate. https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F6.1	The DCC shall ensure that the applicable numbers of Communications Hub Products are delivered in accordance with Valid Communications Hubs Orders to the relevant Delivery Location on the relevant Delivery Date during the relevant Delivery Window. https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F6.2	The DCC shall ensure that the Communications Hub Products are delivered in accordance with the delivery requirements set out in the CH Handover Support Materials. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.3	The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the

			Communications Hub Products are unloaded from the delivery vehicle at the Delivery Location in accordance with Good Industry Practice and the CH Handover Support Materials. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.4	Delivery of Communications Hub Products pursuant to this Code shall occur on removal of the Communications Hub Products from the delivery vehicle at the Delivery Location (subject to any additional requirements in the CH Handover Support Materials). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F6.9	The only grounds for non-compliance under Section F6.7 are that: (a) no delivery was made to the relevant Delivery Location on the relevant Delivery Date, or the delivery was made but contained fewer Communications Hub Products of the applicable Device Model or type than the DCC was obliged to deliver; (b) the delivery contained more Communications Hub Products of the applicable Device Model or type than the DCC was obliged to deliver to the relevant Delivery Location on the relevant Delivery Date; (c) the delivered Communications Hub Products are (or reasonably appear on a visual inspection to be) damaged or have been (or reasonably appear on a visual inspection to have been) tampered with (and such damage or tampering occurred prior to their delivery to the Party as described in Section F6.4); and/or (d) the Party is otherwise entitled to reject the Communications Hub Products in accordance with the CH Handover Support Materials. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F6.15	The Party which submitted the Communications Hub Order shall ensure that each of the DCC and its sub-contractors and its and their agents is allowed access to the Delivery Location for the purposes of exercising the DCC's rights and performing the DCC's obligations under this Section F6. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F6.7	The Party which submitted the Valid Communications Hub Order shall confirm whether or not a delivery of Communications Hub Products has been made in compliance with the order within five days after the applicable Delivery Date (such confirmation to be submitted in accordance with and contain the information specified in the CH Handover Support Materials and via the CH Ordering System). https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.8	Where a Party fails to submit a confirmation in accordance with Section F6.7, the Party shall be deemed to have

			confirmed that a delivery of Communications Hub Products has been made in compliance with the relevant order. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F6.10	Where a Party notifies the DCC under Section F6.7 that a delivery is non-compliant in accordance with Sections F6.9(b), (c) and/or (d), the Party thereby rejects the Communications Hub Products in question. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F6.11	Where Section F6.10 applies, the Party to which the rejected Communications Hub Products were delivered shall make those Communications Hub Products available for collection by the DCC in accordance with the CH Handover Support Materials. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.12	The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the rejected Communications Hub Products are loaded on to the DCC's vehicle in accordance with Good Industry Practice and the CH Handover Support Materials. Risk of loss or destruction of or damage to such Communications Hub Products shall transfer to the DCC on commencement of such loading (where loaded by the DCC) or on completion of such loading (where not loaded by the DCC). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F6.13	Where a Party notifies the DCC under Section F6.7 that a delivery is non-compliant in accordance with Sections F6.9(a), (c) and/or (d), the DCC shall ensure that replacement Communications Hub Products of the applicable Device Model or type and in the number necessary to make up the shortfall are delivered to the relevant Delivery Location as soon as reasonably practicable thereafter. https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F6.14	Where Section F6.13 applies, the DCC shall (via the CH Ordering System) notify the Party of the dates on which the DCC is able to deliver such replacement Communications Hub Products, and this Section F6 shall apply as if: (a) the replacement Communications Hub Products to be delivered pursuant to this Section F6.14 were the subject of a Valid Communications Hub Order; and (b) the date selected by the Party, out of the dates so notified by the DCC, was the Delivery Date for that order. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.15	The Party which submitted the Communications Hub Order shall ensure that each of the DCC and its sub-contractors and its and their agents is allowed access to the Delivery Location

			for the purposes of exercising the DCC's rights and performing the DCC's obligations under this Section F6. https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F6.16	The DCC shall ensure that each person that accesses a Delivery Location pursuant to Section F6.15 shall do so in compliance with Good Industry Practice and the site rules and reasonable instructions of the relevant Party (or its representatives). https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.17	Each Party which submits a Communications Hub Order may specify non-standard delivery instructions where and to the extent provided for in the CH Handover Support Materials. Subject to such Party agreeing to pay any applicable Charges, the DCC shall comply with such delivery instructions. https://smartenergycodecompany.co.uk/download/2476
Party	Smart Energy Code	Section F6.18	Where the Party which submitted a Valid Communications Hub Order breaches its obligations under this Section F6 and/or the CH Handover Support Materials and as a result the DCC is not able to deliver the Communications Hub Products in accordance with this Code, that Party shall be liable to reimburse the DCC for all reasonable costs and expenses incurred by the DCC as a result. The DCC shall notify the Party of such costs and expenses as soon as reasonably practicable after the event. Such compensation shall be included in the next Invoice to be produced by the DCC following its calculation. https://smartenergycodecompany.co.uk/download/2476
7.9.1.6.2 Communications Hub Status Update – Fault Return and No Fault Return			
Party who ordered the CH	Smart Energy Code	Section F8.1(a)	The DCC's rights under this Section F8.1 are in addition to (and separate from) the rights of the DCC (and the obligations of the other Parties) to remove and/or return Communications Hubs under other provisions of this Code (including pursuant to the Incident Management Policy and the CH Support Materials). The DCC has the right to request (in reliance on this Section F8.1) that Parties return to the DCC one or more Communications Hubs. Following receipt of such a request: (a) in respect of Communications Hubs that have been delivered but have not yet been installed at premises, the Party which ordered those Communications Hubs shall return them to the DCC; https://smartenergycodecompany.co.uk/download/2476
Lead Supplier for the CH	Smart Energy Code	Section F8.1(b)	The DCC's rights under this Section F8.1 are in addition to (and separate from) the rights of the DCC (and the obligations of the other Parties) to remove and/or return Communications Hubs under other provisions of this Code

			(including pursuant to the Incident Management Policy and the CH Support Materials). The DCC has the right to request (in reliance on this Section F8.1) that Parties return to the DCC one or more Communications Hubs. Following receipt of such a request: (b) in respect of Communications Hubs that have been installed at premises and not yet removed from that premises, the Lead Supplier for those Communications Hubs shall remove them from the premises and return them to the DCC (and this obligation shall apply whether or not such Lead Supplier is a User); and https://smartenergycodecompany.co.uk/download/2476
Supplier Party that removed the CH	Smart Energy Code	Section F8.1(c)	The DCC's rights under this Section F8.1 are in addition to (and separate from) the rights of the DCC (and the obligations of the other Parties) to remove and/or return Communications Hubs under other provisions of this Code (including pursuant to the Incident Management Policy and the CH Support Materials). The DCC has the right to request (in reliance on this Section F8.1) that Parties return to the DCC one or more Communications Hubs. Following receipt of such a request: (c) in respect of Communications Hubs that have been removed from a premises and not yet returned to the DCC, the Supplier Party that removed the Communications Hub from the premises shall return them to the DCC. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.3	Each Supplier Party that: (a) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, is entitled to remove that Communications Hub from the premises at which it is installed (but must install a replacement Communications Hub unless the Communications Hub Function is Withdrawn); (b) Decommissions a Communications Hub Function, shall remove the Communications Hub of which the Communications Hub Function forms part from the premises at which it is installed; and (c) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, may also be obliged under another provision of this Code to remove a Communications Hub, including where it is obliged to do so in accordance with the Incident Management Policy or the CH Support Materials. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.4	Where a Supplier Party removes a Communications Hub from a premises, it shall do so in accordance with the CH Installation and Maintenance Support Materials

			https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.5	Where a Communications Hub is removed by a Supplier Party from a premises at which it was previously installed, then the risk of loss or destruction of or damage to that Communications Hub shall vest in that Supplier Party as set out in Section F7.4(a) (Risk in the Communications Hubs following Installation). https://smartenergycodecompany.co.uk/download/2476
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.1	A Supplier Party may remove a Communications Hub from an ICHIS compliant host that is powered. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.2	Where a Supplier Party removes a Communications Hub and any associated Communications Hub Auxiliary Equipment, the Supplier Party shall do so in accordance with the procedures set out in Annex A of this document. https://smartenergycodecompany.co.uk/download/2336
Supplier	Smart Energy Code	Section F8.6	Where a Communications Hubs is removed by a Supplier Party from a premises at which it was previously installed, the Supplier Party shall return the Communications Hub to the DCC within 90 days after the date of its removal. This obligation to return a Communications Hub only applies where the Communications Hub Function which forms part of that Communications Hub has at any time had an SMI Status of 'installed not commissioned' or 'commissioned'. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.7	A Party that wishes to return a Communications Hub to the DCC shall be entitled to do so at any time. A Party that ceases to be a Party shall return to the DCC all the Communications Hubs that have been delivered to that Party and not yet installed at premises or reported as lost or destroyed. https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F8.8	The DCC shall publish on the CH Ordering System the following information: (a) the addresses of no more than two locations in respect of each Region to which Communications Hubs can be returned (which locations must be in Great Britain), making clear which Device Models may be returned to which locations; (b) the operating hours of each such location during which returns can be made (which operating hours must be reasonable); and

			(c) any changes to the information required to be published under (a) and (b) above, for which at least four months' advance notice must be given (unless the Panel approves a shorter period). https://smartenergycodecompany.co.uk/download/2476
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.3	Following the removal of a Communications Hub, as a result of a suspected or actual fault in the Communications Hub the Supplier Party shall notify the DCC of its removal by submitting a Service Request in accordance with clauses 9.4 or 9.5 as applicable within five (5) Working Days of the date of removal. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.4	Where the Communications Hub has been removed due to physical damage, the Supplier Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return) indicating the appropriate fault return type and reason as specified in the DCC User Interface Specification (DUIS). https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.5	Where a Communications Hub is removed in accordance with clause 8.8, the Supplier Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return) indicating the appropriate fault return type as specified in the DUIS. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.6	Where a Communications Hub is removed and clause 9.4 and 9.5 do not apply, and the Supplier Party wishes to return the Communications Hub, the Supplier Party shall submit a Service Request 8.14.4 (Communications Hub Status Update – No Fault Return) indicating the appropriate return type as specified in Section F9, within five (5) Working Days of the date of removal. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.7	Where either: (a) a Communications Hub is to be returned prior to installation pursuant to clause 3.4; or (b) the DCC has requested the return of a Communications Hub in accordance with Section F8.1(b) of the Code or the Supplier Party is required to return pursuant to Section F8.6 of the Code; the Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return). https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I -	9.8	Where a Communications Hub is to be returned prior to installation pursuant to Section F8.7(a) of the Code, the

	CH Installation and Maintenance Support Materials		responsible Party shall submit a Service Request 8.14.4 (Communications Hub Status Update – No Fault Return). https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	9.9	In the event that a Party is not able to submit a Service Request in accordance with clauses 9.4, 9.5, 9.6, 9.7 or 9.8 that Party shall contact the Service Desk https://smartenergycodecompany.co.uk/download/2336
Supplier	Smart Energy Code Materials	Section F8.9	A Party required or opting to return one or more Communications Hubs to the DCC shall: (a) notify the DCC of the number of Communications Hubs to be returned, of the location to which they are to be returned (being one of the locations published for the relevant Region in accordance with Section F8.8), of the date on which they are to be returned, and of any further information required in accordance with the CH Installation and Maintenance Support Materials; (b) return those Communications Hubs to the location and on the date notified in accordance with (a) above during the applicable operating hours for that location published in accordance with Section F8.8; (c) otherwise comply with the return requirements set out in the CH Installation and Maintenance Support Materials; and (d) be liable to pay the applicable Charges in the event that it returns one or more Communications Hubs to the wrong returns location. https://smartenergycodecompany.co.uk/download/2476
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.5	To return a Communications Hub a Party shall request a Returns Material Authorisation (RMA) once that Party has notified the DCC by either having: (a) submitted Service Request 8.14.3 or Service Request 8.14.4 in respect of the Communications Hub to be returned; or (b) contacted the Service Desk. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.6	The requesting Party shall ensure that the request for an RMA is: (a) made via the CH Ordering System; and (b) includes: (i) the CHF Identifier for each Communications Hub to be returned under that RMA, as previously notified to the DCC in accordance with clause 10.5 (ii) the contact name, email address, and telephone number to be used by the DCC to contact the Party in relation to that RMA; (iii) the preferred DCC Returns Location; and (iv) a preferred Return

			Date, which shall be on a Working Day at least five (5) Working Days following the date that the request for the RMA is submitted. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	10.7	Following acceptance of an RMA request, the DCC shall: (a) confirm authorisation to the submitting Party using the contact details provided; (b) provide the Party with the following information via the Order Management System using either the 'CH Ordering' or 'CH Delivery and Returns' OMS profiles or via notification to the contact details provided: (i) a unique booking reference; (ii) confirmed timeslot for delivery; (iii) RMA reference; and (iv) any changes to the DCC contact details for the purposes of the return; and (c) request any additional information as may be reasonably required to facilitate the logistics of the return in accordance with good industry practice. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.8	A Party shall ensure that all Communications Hubs returned to the DCC are in packaging of equivalent standard to that in which a Communications Hub of that Device Model was originally packaged, not exceeding the maximum number of Communications Hubs per carton and cartons per pallet set out in the CH Handover Support Materials. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.9	A Party may return aerials or other equipment to DCC within a Communications Hub return delivery and must ensure that any aerials or other equipment returned to the DCC are in packaging of equivalent standard to that in which the aerials or other equipment was originally packaged. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.10	Where a Communications Hub has been subject to environmental or biological contamination, the Party shall: (a) where it is safe to do so, place the Communications Hub in appropriately sealed packaging such that DCC can clearly identify the nature of the contamination without removing or unsealing such packaging; or (b) where safe return of a contaminated Communications Hub is not possible, safely and securely dispose of the Communications Hub. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and	10.11	Where the Party does not return a Communications Hub within 90 days pursuant to Section F8.6 of the Code, the Communications Hub shall be deemed to be lost or stolen and the DCC shall prevent that Communications Hub from connecting to the SM WAN.

	Maintenance Support Materials		https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.12	The Party shall ensure that the Communications Hub delivery is accompanied with a Return Delivery Note that contains, as a minimum, the following information: (a) booking reference for the return delivery as supplied by DCC pursuant to clause 10.7; (b) return date and return delivery time; (c) Party Signifier; (d) DCC Returns Location; (e) list of all CHF Identifiers being returned; and (f) (where one or more pallets are to be returned), the pallet identifiers for each pallet being returned. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	10.14	The Party shall notify the DCC if there are any known issues that mean the delivery will be late, stating the reason for the delay and the expected time of arrival. The Party shall take all reasonable steps to make such notification a minimum of 5 Working Hours prior to the return delivery booking time. The DCC shall take all reasonable steps to accommodate a revised return delivery booking time and shall confirm to the Party that the DCC is either: (a) able to accept the late return delivery; or (b) unable to accept the return delivery. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	10.13	The DCC shall provide the Party with a printable RMA label for each return delivery via the OMS (using the CH Ordering or CH Delivery and Returns profile) immediately following authorisation. The Party shall securely attach the corresponding RMA label on each pallet and each carton (where a carton is not part of a pallet) and each Communications Hub (where a Communications Hub is not part of a pallet or carton) for each return delivery https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	10.16	Prior to signing the Return Delivery Note, the DCC may carry out the following; (a) assessment of pallets delivered against those recorded under the RMA request; (b) checks between CHF Identifiers received against those listed under the RMA request; and (c) checks that the number of Communications Hubs returned match the number of CHF Identifiers listed in the RMA request. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH	10.19	Where requested to do so the DCC shall sign and retain a copy of the Return Delivery Note.

	Installation and Maintenance Support Materials		https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	10.17	The DCC may reject any returned Communications Hubs where unloading them would present a health and safety risk. Where the DCC rejects the return delivery, the Party shall be required to request a new RMA and rearrange the return delivery following the relevant procedures set out in clauses 10.5 to 10.15 of this document. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	10.18	Following the checks performed pursuant to clause 10.16, the DCC shall record any discrepancies between the return delivery and the Return Delivery Note. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	11.1	The DCC shall create an individual record for each returned Communications Hub on receipt of Service Request 8.14.3, 8.14.4 or any return notified through the Service Desk. For each returned Communications Hub this record shall contain all details received by DCC from the Party within the Service Request or provided via the Service Desk and other supporting information as set out in Annex D, and shall be made available by the DCC to the Party that returned the Communications Hub within seven (7) days after the return of the Communications Hubs via the CH Ordering System. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	11.2	Where the DCC intends to undertake any CH Fault Diagnosis, the DCC shall update the relevant record, as described in Annex D of this document, indicating that further analysis is required, in accordance with Section F9.9 of the Code. The DCC shall make this information available and notify the Party that returned the Communications Hub within ten (10) days after the return of the Communications Hubs or notification of its loss or destruction pursuant to Section F9.9, of this revision. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance	11.3	In the event that a Party is not able to access the record created in accordance with clause 11.1, that Party may contact the Service Desk in order to access the record, which the DCC shall enable. https://smartenergycodecompany.co.uk/download/2336

	Support Materials		
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	11.4	The DCC shall undertake CH Fault Diagnosis using visual and electronic analysis of returned Communications Hubs, as set out in clauses 11.5 and 11.6. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	11.5	The DCC may undertake the following visual inspections of a returned Communications Hub and shall subsequently update the information in the record created pursuant to 11.1 to include the results from this analysis: (a) check for any physical damage to any part of the Communication Hub including, but not limited to, the outer casing, external interfaces and connectors; (b) check to identify any loose internal components and for evidence that such components were previously connected correctly; (c) check for any evidence of tampering; and (d) check for any evidence of exposure to adverse environmental conditions including, but not limited to, water, condensation, smoke, chemicals, pests, etc. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	11.6	Where the Communications Hub is not deemed to be physically damaged in accordance with clause 11.5, the DCC may undertake the electronic diagnostic tests described in Annex C of this document and shall subsequently update the information in the record created pursuant to 11.1 to include the results from this analysis. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	11.7	Pursuant to Section F9.11, where the DCC disputes the reason given by a Party for the return of a Communications Hub, the DCC shall provide the Party which returned the Communications Hub with a report. The DCC shall provide this report by updating the relevant Fault Analysis Report record maintained for each returned Communications Hub, as set out in Annex D of this document, with the results of the Fault Analysis and make this available via the CH Ordering System and notify the Party that returned the Communications Hub. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and	11.8	Where the DCC provides a Fault Analysis Report and the Party does not object in accordance with Section F9.13 of the Code, no further action is required by the Party and the DCC shall update the 'Returns Record Status' field to "Closed"

	Maintenance Support Materials		https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	11.9	Where the Party wishes to notify the DCC of their objection pursuant to Section F9.14 of the Code it shall do so via the Service Desk. https://smartenergycodecompany.co.uk/download/2336
Supplier	Smart Energy Code	Section F8.10	The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the returned Communications Hubs are unloaded from the vehicle in which they have been returned, and that they are unloaded in accordance with Good Industry Practice and the CH Installation and Maintenance Support Materials. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.11	Risk of loss or destruction of or damage to returned Communications Hubs shall transfer to the DCC on commencement of such unloading (where unloaded by the DCC) or on completion of such unloading (where not unloaded by the DCC). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F8.12	The DCC shall ensure that each Party (and its sub-contractors and its and their agents) is allowed access to the locations published pursuant to Section F8.8 for the purposes of exercising the Party's rights and performing the Party's obligations under this Section F8. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.13	The relevant Party shall ensure that any person that accesses a location pursuant to Section F8.14 shall do so in compliance with Good Industry Practice and the site rules and reasonable instructions of the DCC (or its representatives). https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.17	Where a Communications Hub has been lost or destroyed (save where such loss or destruction occurs while the risk of loss or destruction was the responsibility of the DCC), the following Party shall notify the DCC of such loss or destruction (via the CH Ordering System): (a) where such loss or destruction occurs prior to completion of the Communications Hub's installation at a premises by a Supplier Party, the Party that ordered that Communications Hub; (or, in the case of Special Installation Mesh Communications Hubs, the Supplier Party which took delivery of the Communications Hub).

			(b) where such loss or destruction occurs after completion of such installation and before commencement of the Communications Hub's removal from a premises by a Supplier Party, the Supplier Party responsible under the Incident Management Policy for resolving the relevant Incident; or (c) where such loss or destruction occurs after commencement of the Communications Hub's removal from a premises by a Supplier Party, the Supplier Party which undertook such removal. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F8.18	Where a Communications Hub is lost or destroyed following completion of its installation at a premises by a Supplier Party and before commencement of its removal from a premises by a Supplier Party, then the Supplier Party that is obliged to notify the DCC of such loss or destruction under Section F8.17(b) shall be deemed to bear the risk of such loss or destruction as described in Section F7.4(b) (Risk in the Communications Hubs following Installation Installation). https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.1	The reason for the return of each returned Communications Hub, or for its loss or destruction, shall be determined in accordance with this Section F9. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.2	The Party which returns a Communications Hub to the DCC shall specify the reason for the Communications Hub's return. The Party which notifies the DCC of a Communications Hub's loss or destruction shall specify the reason it was lost or destroyed. In any such case, such Party shall specify the reason in accordance with the CH Support Materials. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.3	The reason specified by the relevant Party pursuant to Section F9.2 shall be subject to any contrary determination in accordance with this Section F9. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.4	The reason for the return of a Communications Hub, as finally determined in accordance with this Section F9, shall be used to determine the applicable category of responsibility (as described in Section F9.4), which is then used for the purposes of calculating the Charges (or adjustments to the Charges in accordance with this Section F9) https://smartenergycodecompany.co.uk/download/2476

Supplier	Smart Energy Code	Section F9.5	The reasons that apply for the purposes of this Section F9 are as follows: (a) that the Communications Hub Function which forms part of the Communications Hub has been Withdrawn from a Non-Domestic Premises; (b) return of a Communications Hub to the DCC due to a Special Second-Fuel Installation; (c) return of a Communications Hub to the DCC due to a Special WAN-Variant Installation; (d) loss or destruction of or damage to a Communications Hub, which occurred while the relevant Party was responsible for such risk and which was caused otherwise than by a breach of this Code by the DCC or a CH Defect; (e) return of a Communications Hub to the DCC, other than where another reason under this Section F9.5 applies; (f) that the Communications Hub has a CH Defect; (g) loss or destruction of or damage to a Communications Hub caused by a breach of this Code by the DCC; (h) rejection of a Communications Hub in accordance with Section F6.10 (Rejected Communications Hub Products); and (i) return of a Communications Hub to the DCC where requested by the DCC under Section F8.1 (Product Recall / Technology Refresh). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F9.7	The DCC has the right to examine and test returned Communications Hubs and to investigate the cause of any damage to or loss or destruction of Communications Hubs to verify whether the reason given by a Party pursuant to Section F9.2 is correct (being CH Fault Diagnosis). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F9.8	The DCC shall undertake CH Fault Diagnosis in accordance with the process for the same described in the CH Installation and Maintenance Support Materials (which may include sampling and extrapolation of results based on sampling). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F9.9	The DCC shall, within 10 days after the return of Communications Hubs or notification of their loss or destruction by a Party, notify that Party (via the CH Ordering System) if the DCC intends to undertake any CH Fault Diagnosis in respect of those Communications Hub. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.10	In the absence of a notification in accordance with Section F9.9, the reason given by a Party in accordance with Section F9.2 in respect of the Communications Hubs in question shall be deemed to be correct https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F9.11	Provided the DCC has first given notice in accordance with Section F9.9, where the DCC disputes the reason given by a

			Party pursuant to Section F9.2 in respect of any Communications Hubs, the DCC shall provide to the Party a report setting out the DCC's analysis of why the reason given by the Party is not correct. https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F9.12	Where the DCC does not provide a report to the Party in accordance with Section F9.11 within 35 days after the DCC's notice to a Party under Section F9.9, the reason given by the Party in accordance with Section F9.2 in respect of the Communications Hubs in question shall be deemed to be correct. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.13	Unless the Party notifies the DCC of the Party's objection to the DCC's analysis within 35 days after receipt of a report in accordance with Section F9.11, the analysis set out in the report shall be deemed to be correct. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F9.14	Where the Party notifies the DCC of an objection within the time period required by Section F9.13, then either of them may refer the matter to the Panel for determination (which determination shall be final and binding for the purposes of this Code). Where the Panel is unable to determine the reason for a Communications Hub's return, then the reason given by the relevant Party under Section F9.2 shall be deemed to be correct. https://smartenergycodecompany.co.uk/download/2476

7.9.2 Manage Service

7.9.2.1 Introduction

The DCC is responsible for providing Users with a range of Services. These include: CH related Services, Enrolment Services, Core Communication Services, Local Command Services, Elective Communication Services and SMKI Services. The DCC provides some of these Services via the DCC User Interface. These DCC Services are defined as DCC User Interface Services and relate to the processing of Service Requests.

This process area covers the DCC User Interface Services. The CH related services are covered in Section 7.9.1 of the BAD, while the SMKI Services in Section 7.7 of the BAD.

The DCC is required to provide the Services in accordance with Service Management Standards. This includes:

- Maintaining DCC Systems and managing internal system changes;
- Managing internal system and Parse and Correlate Software releases;

- Having in place Business Continuity and Disaster Recovery arrangements; and
- Having in place an Incident Management process. This process is described in Section 7.9.4 of the BAD.

To support the provision of the Services, the DCC has in place the following functions:

- A SSI; and
- A Service Desk.

To support the provision of the DCC User Interface Services, the DCC is also required to:

- Obtain Registration Data for the purpose of checking eligibility for some of the DCC User Interface Services. This process is described in Section 7.8.1 of the BAD; and
- Provide Parse and Correlate Software to Users to enable Users to covert Service Responses and Alerts into the format set out in the Message Mapping Catalogue and confirm that any Pre-Command the User receives is the same as the corresponding Service Request the User sent to the DCC.

DCC performance is measured by Code Performance Measures (CPM). This is in addition to the DCC obligations relating to Demand Management described in Section 7.9.3 of the BAD.

7.9.2.2 Scope

This process area includes:

- Manage Service
- Self Service Interface
- Service Desk
- Performance Standards and Reporting

This process area excludes:

- Business Continuity and Disaster Recovery
- Parse and Correlate Software

7.9.2.3 Actors

- Users
- Parties
- RDP
- DCC

7.9.2.4 Process Description

7.9.2.4.1 Manage Service

The DCC undertakes maintenance of the DCC Systems to avoid Service disruption. It does this through:

- Scheduling planned maintenance, and limiting its duration;
- Sharing with Parties, RDPs and the Panel its maintenance plans;
- Accommodating changes to the plan proposed by Parties, RDPs or the Panel where possible; and
- Where unplanned maintenance is required, notifying Parties, RDPs and the Panel, and keeping them informed of progress.

Where the DCC is proposing to change the DCC Systems, the DCC:

- Assesses the impact upon Parties and RDPs, and if there is a material risk of disruption, consult with them and the Panel; and
- Allows Parties and RDPs to get involved with testing the change prior to implementation.

The DCC manages releases to the DCC Systems and / or the Parse and Correlate Software in accordance with the DCC Release Management Policy. This policy is available from the DCC website[23], and:

- Is consistent with the Service Management Standards;
- Includes a mechanism for setting priorities;
- Defines a 7-step release model
- Defines periods of change-freeze; and
- Defines periods of notice to be given to Users prior to implementation.

The DCC consults with Parties, RDPs and the SEC Panel before making any changes to the Policy.

7.9.2.4.2 Self-Service Interface

The DCC provides a SSI, which allows Users to access a range of functionality on-line. Users can access the SSI using the SSI Code of Connection via the DCC Gateway. SEC Appendix AH - Self-Service Interface Design Specification provides further detail.

The functionalities available via the SSI include:

[23] https://www.smartdcc.co.uk/media/362370/dcc_releasemanagementpolicy_v1.0_baselined_-_published_20160331.pdf

- The SMI;
- A record of the Service Requests and Signed Pre-Commands sent by that User, and of the Acknowledgments, Pre-Commands, Service Responses and Alerts received by that User in the last 3 months;
- A record of the 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests sent by any User in the last 3 months;
- The Incident Management Log (IML);
- The CH Order Management System;
- The WAN checker; and
- Any additional information made available by the DCC.

7.9.2.4.3 Service Desk

The DCC provides a Service Desk contactable via the SSI, email and through a dedicated telephone number.

The Service Desk can be used by Parties and RDPs to resolve queries relating to the Services (provided that Users use the SSI in the first instance). Parties make enquiries to the Service Desk by submitting SMSR.

The Service Desk can be used by Incident Parties that are not Users to raise Incidents (or by Users, where the Incident Management Log is not available via the SSI).

The DCC is required to ensure the Service Desk is available at all times, and provide alternative arrangements (a different telephone number and email address) where the usual Service Desk is not available.

7.9.2.4.4 Performance Standards and Reporting

The DCC is subject to six CPM covering Service Requests (On-Demand and Future Dated), Alerts, Incidents and SSI availability.

Each CPM has a Target Service Level and Minimum Service Level.

The Service Levels are calculated monthly as follows:

- The percentage of Service Requests or Alerts completed within the Target Response Time (Target Response Times are specific to each SRV, and vary depending upon whether the Service Request is On-Demand or Future Dated. Target Response Times are defined in the SEC Appendix E – DCC User Interface Services Schedule. The method of measuring the Target Response Time is defined in Section 3.7 of SEC Appendix AD – DCC User Interface Specification;
- The percentage of Incidents closed within the Target Resolution Time; and

- The percentage of time the SSI is available within the Target Availability Period.

Table 15. Performance Standards

No.	Code Performance Measure	Performance Measurement Period	Target Service Level	Minimum Service Level
1	Percentage of On-Demand Service Responses delivered within the applicable Target Response Time.	monthly	99%	96%
2	Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time.	monthly	99%	96%
3	Percentage of Alerts delivered within the applicable Target Response Time.	monthly	99%	96%
4	Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.	monthly	100%	85%
5	Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 3, 4 or 5 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.	monthly	90%	80%
6	Percentage of time (in minutes) when the Self-Service Interface is available to be accessed by all Users during the Target Availability Period.	monthly	99.5%	98%
7	Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.	monthly	99%	96%
8	Percentage of documents stored on the SMKI	monthly	99%	96%

	Repository delivered within the applicable Target Response Time for the SMKI Repository Service.			

The DCC provides a monthly report to the Panel, Users, the Authority, and (on request) the Secretary of State, identifying those measures which are below the Service Level and:

- Where the measure is below the Target Service Level, provide a reason.
- Where the measure is below the Minimum Service Level, explain the steps taken to prevent recurrence.
- Provide an anticipated reduction in DCC costs as a result of a failure to meet the Service Level.

7.9.2.5 Governance

Actor	SEC Document	Clause	Text
7.9.2.4.1 Manage Service			
DCC	Smart Energy Code	Section H3.1	The DCC shall maintain the DCC User Interface in accordance with the DCC User Interface Specification, and make it available via DCC Gateway Connections to Users to send and receive communications in accordance with the DCC User Interface Specification and the DCC User Interface Code of Connection. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H3.2	The DCC shall ensure that the DCC User Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.1	The DCC shall provide the Services in a manner that is consistent with: (a) the Service Management Standards; or (b) any other methodology for service management identified by the DCC as being more cost efficient than the Service Management Standards, and which has been approved by the Panel for such purpose. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.2	The DCC shall (insofar as is reasonably practicable) undertake Maintenance of the DCC Systems in such a way as to avoid any disruption to the provision of the Services (or any part of them) https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.3	Without prejudice to the generality of Section H8.2, the DCC shall (unless the Panel agrees otherwise): (a) undertake Planned Maintenance of the DCC Systems only between 20.00 hours and 08.00 hours; (b) limit Planned Maintenance of the Self-Service Interface to no more than four hours in any month; and (c) limit Planned Maintenance of the DCC Systems generally (including of the SelfService Interface) to no more than six hours in any month. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.4	At least 20 Working Days prior to the start of each month, the DCC shall make available to Parties, to Registration Data Providers and to the Technical Architecture and Business Architecture Sub-Committee a schedule of the Planned Maintenance for that month. Such schedule shall set out (as a minimum) the following: (a) the proposed Maintenance activity (in reasonable detail);

			(b) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity; (c) the time and duration of each such Maintenance activity; and (d) any associated risk that may subsequently affect the return of normal Services. https://smartenergycodecompany.co.uk/download/2483
Panel	Smart Energy Code	Section H8.5	The Panel may (whether or not at the request of a Party) request that the DCC reschedules any Planned Maintenance set out in a monthly schedule provided pursuant to Section H8.4. In making any such request, the Panel shall provide the reasons for such request to the DCC in support of the request. The DCC will take all reasonable steps to accommodate any such request. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.6	As soon as reasonably practicable after the DCC becomes aware of any Unplanned Maintenance, the DCC shall notify the Technical Architecture and Business Architecture Sub-Committee, Parties and (insofar as they are likely to be affected by such Unplanned Maintenance) Registration Data Providers of such Unplanned Maintenance (and shall provide information equivalent to that provided in respect of Planned Maintenance pursuant to Section H8.4). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.7	During the period of any Planned Maintenance or Unplanned Maintenance, the DCC shall provide Parties and (insofar as they are likely to be affected by such maintenance) Registration Data Providers with details of its duration and the expected disruption to Services to the extent they differ from the information previously provided. https://smartenergycodecompany.co.uk/download/2483
DC	Smart Energy Code	Section H8.8	Where the DCC is proposing to make a change to DCC Internal Systems, the DCC shall: (a) undertake an assessment of the likely impact upon: (i) Parties in respect of any potential disruption to Services; and/or (ii) RDPs in relation to the sending or receipt of data pursuant to Section E (Registration Data), that may arise as a consequence of the Maintenance required to implement the contemplated change; (b) where such assessment identifies that there is a Material Risk of disruption to Parties and/or RDP's, consult with Parties and/or RDPs (as applicable) and with the Technical Architecture and Business Architecture Sub-Committee regarding such risk;

			(c) provide the Parties and RDPs the opportunity to be involved in any testing of the change to the DCC Internal Systems prior to its implementation; and (d) undertake an assessment of the likely impact of the contemplated change upon the security of the DCC Total System, Smart Metering Systems, and the Systems of Parties and/or RDPs. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.9	The DCC shall ensure that it plans, schedules and controls the building, testing and deployment of releases of IT updates, procedures and processes in respect of the DCC Internal Systems and/or the Parse and Correlate Software in accordance with a policy for Release Management (the "DCC Release Management Policy"). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.10	The DCC shall ensure that the DCC Release Management Policy: (a) defines the scope of the matters that are to be subject to the policy in a manner consistent with the Service Management Standards; (b) includes a mechanism for setting priorities for different types of such matters; (c) defines periods of change-freeze where no such matters may be implemented; and (d) defines periods of notice to be given to Parties and RDPs prior to the implementation of such matters. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.11	The DCC shall make the DCC Release Management Policy available to Parties, RDPs and the Technical Architecture and Business Architecture Sub-Committee. The DCC shall consult with Parties, RDPs and the Technical Architecture and Business Architecture Sub-Committee before making any changes to the DCC Release Management Policy https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.12	The DCC's obligation under Section H8.11 is in addition to its obligations in respect of Planned Maintenance and changes to DCC Internal Systems to the extent that the activity in question involves Planned Maintenance or changes to DCC Internal Systems. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H15.1	The DCC shall maintain each DCC Gateway Connection and make it available subject to and in accordance with the provisions of this Section H15. https://smartenergycodecompany.co.uk/download/2483

DCC	Smart Energy Code	Section H15.2	The DCC shall ensure that each DCC Gateway Connection is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section L4.1	The DCC shall maintain the SMKI Service Interface in accordance with the SMKI Interface Design Specification and make it available, for sending and receiving communications in accordance with the SMKI Code of Connection, via DCC Gateway Connections, to: (a) Authorised Subscribers; and (b) (where applicable) Parties for the purpose of undertaking SMKI Entry Process Testing. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L4.2	The DCC shall ensure that the SMKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3): (a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and (b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L6.1	The DCC shall maintain the SMKI Repository Interface in accordance with the SMKI Repository Interface Design Specification and make it available, via DCC Gateway Connections, to: (a) the Parties and RDPs; (b) the Panel (or the Code Administrator on its behalf); and (c) the SMKI PMA (or the Code Administrator on its behalf), to send and receive communications in accordance with the SMKI Repository Code of Connection and (where applicable) for the purpose of SMKI Entry Process Testing. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L6.2	The DCC shall ensure that the SMKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3): (a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and (b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing https://smartenergycodecompany.co.uk/download/2503

DCC	Smart Energy Code	Section L13.10	The DCC shall maintain the DCCKI Service Interface in accordance with the DCCKI Interface Design Specification and make it available, to DCCKI Authorised Subscribers, for sending and receiving communications in accordance with the DCCKI Code of Connection. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L13.11	The DCC shall ensure that the DCCKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3): (a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and (b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L13.24	The DCC shall maintain the DCCKI Repository Interface in accordance with the DCCKI Repository Interface Design Specification and make it available to the Parties and to RDPs to send and receive communications in accordance with the DCCKI Repository Code of Connection and (where applicable) for the purpose of Entry Process Testing. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L13.25	The DCC shall ensure that the DCCKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3): (a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and (b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing. https://smartenergycodecompany.co.uk/download/2503
7.9.2.4.3 Service Desk			
DCC	Smart Energy Code	Section H 8.13	Each User shall take reasonable steps to access the information it needs, and to seek to resolve any queries it may have, via the Self-Service Interface in the first instance. A User shall only contact the Service Desk where it cannot reasonably obtain the information it needs, or resolve its query, via the Self-Service Interface. https://smartenergycodecompany.co.uk/download/2483
Party	Smart Energy Code	Section H8.14	A Party that is not a User will be unable to access the Self-Service Interface, but may contact the Service Desk. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.19	The DCC shall ensure that a team of its representatives (the Service Desk) is available to be contacted as follows: (a) the Service Desk shall be contactable via the following means (to be used by Parties and Registration Data Providers, to the extent available to them, in the following order of

			preference, save as otherwise provided for in the Incident Management Policy): (i) the Self-Service Interface; (ii) a dedicated email address published on the DCC Website; and (iii) a dedicated telephone number published on the DCC Website; (b) the Service Desk can be used by Parties to seek resolution of queries relating to the Services (provided that Users shall seek resolution via the Self-Service Interface in the first instance); and (c) the Service Desk can be used by Incident Parties that are not Users to raise Incidents (or by Users, where the Incident Management Log is not available via the Self-Service Interface, to raise or provide information in respect of Incidents), which the DCC shall then reflect in the Incident Management Log. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.20	The DCC shall ensure that the Service Desk is available at all times, and shall provide alternative arrangements (a different telephone number and email address) where the usual Service Desk in not available. Where a different telephone number and email address is to be used, the DCC shall publish details of the alternative number and address at least 20 Working Days in advance. https://smartenergycodecompany.co.uk/download/2483
7.9.2.4.2 Self-Service Interface			
DCC	Smart Energy Code	Section H8.15	The DCC shall maintain and keep up-to-date an interface (the Self-Service Interface) which: (a) complies with the specification required by the Self-Service Interface Design Specification; (b) is made available to Users in accordance with the Self-Service Interface Code of Connection via DCC Gateway Connections; and (c) allows each User to access the information described in Section H8.16 as being accessible to that User (and also allows other Users to access that information to the extent permitted by the first User in accordance with the Self-Service Interface Design Specification). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.16	The Self-Service Interface must (as a minimum) allow the following categories of User to access the following: (a) the Smart Metering Inventory, which shall be available to all Users and capable of being searched by reference to the following (provided that there is no requirement for the DCC to provide information held on the inventory in respect of Type 2 Devices other than IHDs):

			(i) the Device ID, in which case the User should be able to extract all information held in the inventory in relation to (I) that Device, (II) any other Device Associated with the first Device, (III) any Device Associated with any other such Device; and (IV) any Device with which any of the Devices in (I), (II) or (III) is Associated; (ii) the MPAN or MPRN, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meter to which that MPAN or MPRN relates, or in relation to any Device Associated with that Smart Meter or with which it is Associated; (iii) post code and premises number or name, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked to that postcode and premises number or name, or in relation to any Device Associated with those Smart Meters or with which they are Associated; (iv) the UPRN (where this has been provided as part of the Registration Data), in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked by that UPRN, or in relation to any Device Associated with those Smart Meters or with which they are Associated; (b) a record of the Service Requests and Signed Pre-Commands sent by each User, and of the Acknowledgments, Pre-Commands, Service Responses and Alerts received by that User (during a period of no less than three months prior to any date on which that record is accessed), which shall be available only to that User; (c) a record, which (subject to the restriction in Section I1.4 (User Obligations)) shall be available to all Users: (i) of all 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests in relation to each Smart Meter (or Device Associated with it) that were sent by any User during a period of no less than three months prior to any date on which that record is accessed; and (ii) including, in relation to each such Service Request, a record of the type of the Service Request, whether it was successfully processed, the time and date that it was sent to the DCC, and the identity of the User which sent it; (d) the Incident Management Log, for which the ability of Users to view and/or amend data shall be as described in Section H9.4 (Incident Management Log); (e) the CH Order Management System, which shall be available to all Users; (f) the following information in respect of the SM WAN, which shall be available to all Users (and which shall be capable of interrogation by post code and postal outcode): (i) whether a Communications Hub Function installed in a premises at any given location: (A) is expected to be able to connect to the SM WAN;

			(B) is expected to be able to connect to the SM WAN from a particular date before 1 January 2021, in which case the date shall be specified; or (C) cannot be confirmed as being able to connect to the SM WAN before 1 January 2021; (ii) any known issues giving rise to poor connectivity at any given location (and any information regarding their likely resolution); and (iii) any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM WAN; (g) additional information made available by the DCC to assist with the use of the Services and diagnosis of problems, such as service status (including information in respect of Planned Maintenance and Unplanned Maintenance) and frequently asked questions (and the responses to such questions), which shall be available to all Users; and (h) anything else expressly required by a provision of this Code. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.17	Without prejudice to the requirements of Sections H8.16(b) and (c), to the extent that the Self-Service Interface does not allow a User to access a record of the information referred to in those Sections in respect of the preceding 7 years, then: (a) subject (in the case of the information referred to in Section H8.16(c)) to the restriction in Section I1.4 (User Obligations), that User shall be entitled to request such information from the DCC; and (b) the DCC shall provide such information to that User as soon as reasonably practicable following such request. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H8.18	The DCC shall ensure that the Self-Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3). https://smartenergycodecompany.co.uk/download/2483
7.9.2.4.4 Performance Standards and Reporting			
DCC	Smart Energy Code	Section H13.1	Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period): https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H13.2	The DCC may modify the Reported List of Service Provider Performance Measures where it has: (a) undertaken reasonable consultation with the Parties regarding the proposed modification;

			(b) given due consideration to, and taken into account, any consultation responses received; and (c) provided to the Panel, the Parties, the Authority and (on request) the Secretary of State a statement of its reasons for the modification together with copies of any consultation responses received, and as soon as reasonably practicable following any such modification, the DCC shall provide an up-to-date copy of the Reported List of Service Provider Performance Measures to the Panel, the Parties, the Authority and (on request) the Secretary of State https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H13.3	Prior to agreeing any changes to the DCC Service Provider Contracts that will alter the Service Provider Performance Measures, the DCC shall: (a) undertake reasonable consultation with the Panel and Parties regarding such changes; (b) give due consideration to, and take into account, any consultation responses received; and (c) provide to the Panel, the Parties, the Authority and (on request) the Secretary of State a statement of its reasons for proposing to agree such changes. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H13.4	The DCC shall, within 25 Working Days following the end of each Performance Measurement Period, produce a report setting out the Service Levels achieved in respect of each Performance Measure. Such report must identify: (a) those Performance Measures (if any) for which the Service Level was less than the Target Service Level and/or the Minimum Service Level; (b) where a Service Level is less than the Target Service Level, the reason for the Service Level achieved; (c) where a Service Level is less than the Minimum Service Level, the steps the DCC is taking to prevent the re-occurrence or continuation of the reason for the Service Level achieved; and (d) any anticipated reductions in the DCC's Internal Costs and/or External Costs (as both such expressions are defined in the DCC Licence) arising as a consequence of the DCC Service Providers failing to achieve the Target Service Levels in respect of the Service Provider Performance Measures. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H13.5	A copy of the report produced pursuant to Section H13.4: (a) shall be provided by DCC, immediately following its production, to the Panel, the Parties, the Authority and (on request) the Secretary of State; and (b) may be provided by the Panel, at its discretion, to any other person

			https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H13.6	The DCC shall: (a) establish and periodically review the Performance Measurement Methodology in accordance with Good Industry Practice and in consultation with the Panel, the Parties and the Authority; and (b) as soon as reasonably practicable following any modification which it may make to the Performance Measurement Methodology, provide an up to date copy of the Performance Measurement Methodology to the Panel, the Parties, the Authority and (on request) the Secretary of State. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section L8.1	The DCC shall undertake the following activities within the following time periods (each such time period being, in respect of each such activity, the "Target Response Time" for that activity): (a) in response to a single Certificate Signing Request, sending to an Eligible Subscriber either an Organisation Certificate or Device Certificate within 30 seconds of receipt of the Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface; and (b) in response to a Batched Certificate Signing Request, sending to an Eligible Subscriber the number of Device Certificates that were requested: (i) where the receipt of the Batched Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface occurred between the hours of 08:00 and 20:00 on any day, by no later than 08:00 on the following day; or (ii) where the receipt of the Batched Certificate Signing Request from that Eligible Supplier over the SMKI Service Interface did not occur between the hours of 08:00 and 20:00, within 24 hours of the time of that receipt. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.2	For the purposes of Section L8.1, a "Batched Certificate Signing Request" is a single communication containing Certificate Signing Requests for the Issue of more than one but no more than 50,000 Device Certificates. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.3	For the purposes of Section L8.1, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Interface Design Specification. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.4	The DCC shall send to a Party, an RDP, the Panel or the SMKI PMA (as the case may be) a copy of any document or information stored on the SMKI Repository within 3 seconds of

			receipt of a request for that document from that person or body over the Repository Interface (and that time period shall be the "Target Response Time" for that activity) https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.5	For the purposes of Section L8.4, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Repository Interface Design Specification. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.6	Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period): https://smartenergycodecompany.co.uk/download/2503
DCC	SEC Appendix AD - DCC User Interface Specification v1.1	3.7	For the purposes of supporting the measurement of Target Response Times (as per Section H3), the concepts of 'receipt' and 'sending' are to be interpreted by Users and the DCC in the following manner. The DCC shall operate the DCC User Interface such that; • For the Transform and Non-Device Services the DCC Systems shall record the date and time of receipt of the Request from the User at the Message Gateway and the date and time of sending of the Service Response to the User at the Message Gateway. • For the Send Command Service the DCC Systems shall record at the Message Gateway the date and time of receipt of the Service Request from the User by the Send Command Service and then subsequently record at the Message Gateway the date and time of Sending of the Service Response to the User's Receive Response Service. • For Device Alerts the DCC Systems shall record the date and time of receipt of the Alert from the Communication Hub and the date and time of sending the Device Alert to the User's Receive Response Service. • For DCC Alerts the DCC Systems shall record at the Message Gateway the date and time of sending of the DCC Alert to the User's Receive Response Service. https://smartenergycodecompany.co.uk/download/2279
	SEC Appendix AD - DCC User Interface	3.7	For the purposes of supporting the measurement of Target Response Times (as per Section H3), the concepts of 'receipt' and 'sending' are to be interpreted by Users and the DCC in the

	Specification v2.0		following manner. The DCC shall operate the DCC User Interface such that; • For the Transform and Non-Device Services the DCC Systems shall record the date and time of receipt of the Request from the User at the Message Gateway and the date and time of sending of the Service Response to the User at the Message Gateway. • For the Send Command Service the DCC Systems shall record at the Message Gateway the date and time of receipt of the Service Request from the User by the Send Command Service and then subsequently record at the Message Gateway the date and time of Sending of the Service Response to the User's Receive Response Service. • For Device Alerts the DCC Systems shall record the date and time of receipt of the Alert from the Communication Hub and the date and time of sending the Device Alert to the User's Receive Response Service. • For DCC Alerts the DCC Systems shall record at the Message Gateway the date and time of sending of the DCC Alert to the User's Receive Response Service. https://smartenergycodecompany.co.uk/download/4639

7.9.3 Manage Demand

7.9.3.1 Introduction

The DCC provides a range of services to Users through its physical infrastructure and IT systems. This includes, but is not limited to, Communication Services that the DCC provides through the DCC User Interface and SMKI Services that the DCC provides through the SMKI Interface. The role of the DCC in providing these Services include processing of Service Requests, Responses, Alerts and CSR.

Under the current arrangements, the DCC system capacity needs to meet Users' projected demand for the DCC User Interface Services and SMKI Services. User demand is based on forecasts from Users.

The current arrangements are not considered to be effective and efficient by the DCC as User demand can vary quite significantly while the DCC maximum capacity is fixed. Currently, the DCC is not permitted to prioritise the processing of messages or put in place any other demand management measures in the event that the volume of messages outstrips capacity. The DCC is currently required to meet the Target Response Times in respect of all communications provided that they are within the forecast provided by the Users.

This process description focuses on the relationship between the DCC and the Users. This process description does not describe the internal processes of Users in determining their forecasts, or the DCC processes for determining the required capacity to meet User demand.

7.9.3.2 Scope

This process area includes Manage Forecasts.

7.9.3.3 Actors

- Users
- Authorised Subscribers
- DCC
- Panel

7.9.3.4 Process Description

7.9.3.4.1 Manage Forecasts

SRV Forecasts

By the 15th Working Day of January, April, July and October, each User provides the DCC with a forecast of the number of Service Requests that the User will send in each of the 8 months following the end of the month in which the forecast is provided.

The forecast breaks down the total number of Service Requests by reference to each Service listed in the DCC User Interface Services Schedule and the category of Service (i.e. Future Dated, On Demand or Scheduled).

The DCC monitors and records actual Service Requests sent by each User, by Service Request and in total.

By the 10th Working Day following the end of each month, the DCC provides:

- Each User with a report that sets out the number of Service Requests sent by that User during that month (in total and by Service Request), and comparing the actual numbers sent against forecast.
- Each User with a report setting out the current value for every Monthly Service Metric for that User and a comparison of the current value against the relevant Monthly Service Threshold; and
- The Panel with a report that sets out:
    - The number of Service Requests sent by all Users during that month (in total and by Service Request), and comparing the actual numbers sent against forecast.
    - Where the number of Service Requests sent by any User during that month is less than or equal to 90% or greater than or equal to 110% of the User's most recent monthly forecast, the identity of the User and the number of Service Requests they sent. (In total and by Service Request).

- Where the measured value of any Monthly Service Metric for any User and that month is greater than or equal to 110% of Monthly Service Threshold, the identity of the User and the values of the Monthly Service Metrics during that month.

The Panel will publish the reports provided to it on the Website. (The Panel may decide not to publish one or more parts of a report concerning under-forecasting or over-forecasting if the Panel considers this was reasonable).

The DCC will not be considered to be in breach of its Target Response Times if total Service Requests sent by all Users exceeds 110% of the current forecast for that month. (Provided that the DCC takes reasonable steps to achieve the Target Response Times.)

CSR Forecast

By the 15th Working Day of March, June, September and December each Authorised Subscriber provides the DCC with a forecast of the number of CSRs that the Authorised Subscriber will send in each of the 8 months following the end of the month in which the forecast is provided.

The forecast will contain a breakdown of the total number of CSRs in respect of Device Certificates between those which request the issue of a single Device Certificate and those which are Batched CSRs.

The DCC monitors and records the number of CSR sent by each Authorised Subscriber in total.

By no later than the 10th Working Day following the end of each month, the DCC provides:

- Each Authorised Subscriber with a report that sets out the number of CSRs sent by that Authorised Subscriber in respect of Device Certificates during that month (in total and broken down between those which request the issue of a single Device Certificate and those which are Batched Certificate Signing Requests, and comparing the actual numbers sent against the forecast.

- The Panel with a report that sets out:

    - The aggregate number of CSRs in respect of Device Certificates sent by all Authorised Subscribers collectively during that month (in total and broken down between those which request the issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers sent against the forecast.

    - Where the number of CSRs in respect of Device Certificates sent by any Authorised Subscriber during that month is greater than or equal to 110% of the Authorised Subscriber's most recent monthly forecast, the identity of each such Authorised Subscriber and the number of CSRs in respect of Device Certificates sent by each such Authorised Subscriber (in total and broken down between those which request the issue of a single Device Certificate and those which are Batched).

The Panel publishes the reports provided to it on the Website. (The Panel may decide not to publish one or more parts of a report concerning under-forecasting or over-forecasting if the Panel considers this was reasonable).

The DCC is not be considered to be in breach of its Target Response Times if the aggregate CSRs in respect of Device Certificates sent by all Authorised Subscribers exceeds 110% of the current forecast for that month. (Provided that the DCC takes reasonable steps to achieve the Target Response Times).

7.9.3.5 Governance

Actor	SEC Document	Clause	Text
7.9.3.4.1 Manage Forecasts			
User	Smart Energy Code	Section H3.22	By the 15th Working Day of the months of January, April, July and October, each User shall provide the DCC with a forecast of the number of Service Requests that the User will send in each of the 8 months following the end of the month in which such forecast is provided. Such forecast shall contain a breakdown of the total number of Service Requests by reference to each Service listed in the DCC User Interface Services Schedule and the category of Service (i.e. Future Dated, On Demand or Scheduled). https://smartenergycodecompany.co.uk/download/2483
Party	Smart Energy Code	Section H3.22A	A Party that is not a User but expects to submit Service Requests to the DCC at any time during any period referred to in Section H3.22 shall comply with Section H3.22 as if it were a User https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H3.23	The DCC shall monitor and record the aggregate number of Service Requests sent by each User in total, and also the aggregate number of Service Requests sent by each User in respect of each Service listed in the DCC User Interface Services Schedule. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H3.24	By no later than the 10th Working Day following the end of each month, the DCC shall provide: (a) each User with a report that sets out the number of Service Requests sent by that User during that month (in total and broken down by reference to each Service listed in the DCC User Interface Services Schedule), and comparing the actual numbers sent against the numbers most recently forecast for the applicable month; (b) each User with a report setting out the current value (calculated at the end of the previous month) for every Monthly Service Metric for that User and a comparison of the current value against the relevant Monthly Service Threshold; and (c) a report to the Panel that sets out:

Actor	SEC Document	Clause	Text
			(i) the aggregate number of Service Requests sent by all Users collectively during that month (in total and broken down by reference to each Service listed in the DCC User Interface Services Schedule), and comparing the actual numbers for that month sent against the numbers most recently forecast for the applicable month; (ii) where the number of Service Requests sent by any User during that month is less than or equal to 90% or greater than or equal to 110% of the User's most recent monthly forecast for the applicable month, the identity of each such User and the number of Service Requests sent by each such User (in total and broken down by reference to each Service listed in the DCC User Interface Services Schedule); and (iii) where the measured value of any Monthly Service Metric for any User and that month is greater than or equal to 110% of Monthly Service Threshold, the identity of that User and the values of such Monthly Service Metrics during that month. https://smartenergycodecompany.co.uk/download/2483
Panel	Smart Energy Code	Section H3.25	The Panel shall publish the reports provided to it pursuant to Section H3.24(c) on the Website. The Panel may decide not to publish one or more parts of a report concerning under-forecasting or over-forecasting as referred to in Section H3.24(c)(ii) where the Panel considers that the under-forecasting or over-forecasting was reasonable in the circumstances (including where it arose as a result of matters beyond the User's reasonable control). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H3.26	The DCC shall, on or around each anniversary of the date on which it first started providing Services over the DCC User Interface, review (and report to the Panel on) each Monthly Service Metric and associated Monthly Service Threshold to establish whether they are still an appropriate mechanism to illustrate User behaviour that may utilise a significant element of the capacity requirements of the Services. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H3.28	The DCC shall not be considered to be in breach of this Code with regard to the obligation to achieve Target Response Times if, during the month in question, the aggregate Service Requests sent by all Users exceeds 110% of the aggregate demand most recently forecast for that month by all Users pursuant to Section H3.22 (provided that the DCC shall nevertheless in such circumstances take reasonable steps to achieve the Target Response Times). https://smartenergycodecompany.co.uk/download/2483

Actor	SEC Document	Clause	Text
User	Smart Energy Code	Section L8.7	Each Party which is an Authorised Subscriber in accordance with the Device Certificate Policy shall: (a) as soon as reasonably practicable after becoming an Authorised Subscriber; and (b) subsequently by the 15th Working Day of the months of March, June, September and December in each year, provide the DCC with a forecast of the number of Certificate Signing Requests that the Authorised Subscriber will send in each of the 8 months following the end of the month in which such forecast is provided. Such forecast shall contain a breakdown of the total number of Certificate Signing Requests in respect of Device Certificates between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.8	The DCC shall monitor and record the aggregate number of Certificate Signing Requests sent by each Authorised Subscriber in total. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.9	By no later than the 10th Working Day following the end of each month, the DCC shall provide: (a) each Authorised Subscriber with a report that sets out the number of Certificate Signing Requests sent by that Authorised Subscriber in respect of Device Certificates during that month (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers sent against the numbers most recently forecast for the applicable month; and (b) (in so far as there were one or more Parties or RDPs which were Authorised Subscribers during the applicable month) a report to the Panel that sets out: (i) the aggregate number of Certificate Signing Requests in respect of Device Certificates sent by all Authorised Subscribers collectively during that month (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers for that month sent against the numbers most recently forecast for the applicable month; and (ii) where the number of Certificate Signing Requests in respect of Device Certificates sent by any Authorised Subscriber during that month is greater than or equal to 110% of the Authorised Subscriber's most recent monthly forecast for the applicable month, the identity of each such Authorised Subscriber and the number of Certificate Signing Requests in respect of Device Certificates sent by each such

Actor	SEC Document	Clause	Text
			Authorised Subscriber (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched https://smartenergycodecompany.co.uk/download/2503

Panel	Smart Energy Code	Section L8.10	The Panel shall publish each report provided to it pursuant to Section L8.9(b) on the Website, save that the Panel may decide not to publish one or more parts of a report concerning under-forecasting as referred to in Section L8.9(b)(ii) where the Panel considers that the under-forecasting was reasonable in the circumstances (including where it arose as a result of matters beyond the Authorised Subscriber's reasonable control). https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.11	The DCC shall, as soon as is reasonably practicable, submit a Modification Proposal containing rules that it considers appropriate to enable the prioritisation by the DCC of Certificate Signing Requests in respect of Device Certificates sent over the SMKI Service Interface in circumstances in which the aggregate demand for the Issue of Device Certificates cannot be satisfied within the applicable Target Response Times. https://smartenergycodecompany.co.uk/download/2503
DCC	Smart Energy Code	Section L8.12	The DCC shall not be considered to be in breach of this Code with regard to the obligation to achieve the Target Response Times set out at Section L8.1 if, during the month in question, the aggregate Certificate Signing Requests in respect of Device Certificates sent by all Authorised Subscribers exceeds 110% of the aggregate demand most recently forecast for that month by all Authorised Subscribers pursuant to Section L8.7 (provided that the DCC shall nevertheless in such circumstances take reasonable steps to achieve the Target Response Times) https://smartenergycodecompany.co.uk/download/2503

7.9.4 Manage Incidents

7.9.4.1 Introduction

Incidents are actual or potential interruptions to the DCC Total System. Problems are the underlying cause of one or more Incidents. This process area describes the processes operated by the DCC to manage Incidents and resolve Problems.

The focus is on the relationship between the DCC and Users, and the communications and handoffs between them.

The majority of Incidents and Problems are expected to be raised, viewed and updated via the SSI.

7.9.4.2 Scope

This process area includes:

- Manage Incident

- Manage Problem

7.9.4.3 Actors

- Users
- RDP
- DCC – in this context, internal DCC function managing communication with Incident and Interested Parties
- DCC Service Desk – in this context, internal DCC function managing Incidents

In this context User, RDPs and the DCC are acting as:

- Incident Parties; or
- Interested Parties.

7.9.4.4 Prerequisites

Users and RDPs have provided the DCC with a list of individuals who can raise an Incident and communicate with the DCC regarding the Incident.

7.9.4.5 Process Description

7.9.4.5.1 Manage Incident

Raising Incidents

Users

A User (the Incident Party) identifies an issue.

The Incident Party checks[24] the following:

- The issue is with Devices;
- The issue is with its own internal systems;
- The issue is a Known Error with an existing workaround from the DCC;
- The issue can be resolved by sending an SRV to the DCC.

If any of the checks determine that the issue lies with one of the above or can be resolved by sending an SRV to the DCC, the process stops here and the Incident Party takes appropriate action as per their internal business processes.

[24] Users may choose to interrogate the SMS or run their own diagnostics on their internal systems to determine where the issue lies. The DCC Service Users SharePoint, accessible from the DCC website, provides further guidance.

If the issue lies elsewhere and the Incident Party cannot resolve it by sending an SRV to the DCC, the Incident Party checks the SSI to ensure that:

- The Incident has not been raised already; and
- The DCC has not issued a Service Alert for this issue.

If either of these exists, the process stops here. If neither exists, the Incident Party raises an Incident and specifies the category.

RDP

A RDP (the Incident Party) identifies an issue regarding the provision of Data to or by the DCC. The Incident Party checks that the issue does not reside within the RDP Systems or processes.

If the issue is not down to the RDP Systems or processes, the Incident Party raises an Incident. The Incident Party can ask the DCC to raise an Incident on its behalf or raise an Incident themselves. The Party raising the Incident specifies the category.

DCC

The DCC (the Incident Party) identifies an issue. The Incident Party raises an Incident via the DCC Service Desk and specifies the category.

- For category 1 Incidents (Major Incidents or Major Security Incidents), as defined in SEC Appendix AG - Incident Management Policy, the Incident Party raises it with the DCC Service Desk.
- For category 2-5 Incidents, the Incident Party uses the SSI to raise the Incident in IML. (If SSI unavailable, the Incident Party may use email or telephone to raise the Incident with the DCC Service Desk).

The DCC Service Desk or Incident Party records the following Data in the IML:

- Contact name
- Contact organisation
- Contact details
- Organisation's Incident reference number (where available)
- Date and time of occurrence
- MPxN or Device ID (where appropriate)
- Summary of Incident
- Business impact

The categorisation of the Incident determines both the Target Initial Response Time and the Target Resolution Time as laid out in the table below:

Table 16. Target Response Times and Target Resolution Times for Incidents

Category	Target Response Time	Target Resolution Time
1	10 minutes	4 hours
2	20 minutes	24 hours
3	45 minutes	72 hours
4	3 hours	5 days
5	1 day	10 days

The DCC Service Desk assesses the information in the IML to confirm whether:

- It is an Incident; and
- Whether is the DCC is responsible for resolving the Incident.

If the first check fails, the DCC Service Desk:

- Contacts the Incident Party, providing the details to enable the Incident Party to raise and manage the Incident within their own systems; and
- Sets the Incident status to 'Closed'.

If the second check fails, the DCC Service Desk:

- Contacts the Incident Party; and
- Assigns the Incident to the Incident Party and sets the Incident status to 'pending'.

The DCC Service Desk assesses the information in the IML, and does the following:

- Categorises an Incident using information in the Incident Management Log;
- Prioritises an Incident by considering the Incident Category and the time remaining until the Target Resolution Time, as defined in the Incident Management Policy;
- Assigns the appropriate Incident Party to resolve it and update the status of the Incident to 'pending'; and
- Identifies Interested Parties for the Incident.

The Incident Party reviews the information in the IML.

If the Incident Party believes that the Incident has been updated to an incorrect Incident Category by the DCC or the Incident Party disagrees with the allocation, it notifies the DCC.

The DCC updates the IML as required. If the Incident has been incorrectly assigned, the DCC reassigns it to another Incident Party.

The Incident Party notifies all Interested Parties that are likely to be affected by the Incident. If the Incident is a Major Security Incident, the DCC notifies the Panel and the Security Sub-Committee.

The Incident Party takes steps to resolve the Incident and logs any progress in the IML.

Incident resolution and closure

When the Incident Party resolves the Incident (or it subsequently determines that is not an Incident), it notifies the DCC Service Desk.

The DCC Service Desk does the following things:

- Updates the status of the Incident in the IML to 'resolved'; and
- Notifies the Incident Party and other Interested Parties and the Incident Party resolving the Incident of the IML status change.

The Incident Party that resolved the Incident, Incident Parties, Interested Party check whether the Incident has been resolved.

- If the Incident is resolved to their satisfaction, the process stops here.
- If the Incident is not resolved satisfactorily, the Party notifies the DCC Service Desk. The DCC Service Desk assesses the information provided. If it disagrees, it notifies the Party, and the process stop here. The Party may raise an Incident. If the DCC agrees, the DCC Service Desk reassigns the Incident and changes its status in the IML.

For Category 1 Incidents only; within 2 Working Days of resolution of the Incident, the DCC notifies the Panel of the nature and cause of the Incident and actions taken to resolve it.

For Category 1 Incidents only; within 20 Working Days of resolution of the Incident, the DCC provides a report to the Panel and the Authority summarising the nature and cause of the incident as well as a review of the effectiveness of the process resolution process.

7.9.4.5.2 Manage Problem

The DCC opens a Problem in the IML:

- When a Category 1 Incident has been resolved;
- When an Incident is closed with a Workaround, or
- When the DCC has identified a re-occurring Incident.

The DCC then carries out the Root Cause Analysis. If the DCC establishes the Root Cause, it reclassifies the Problem as a 'Known Error'. If the Root Case is not established, the Problem remains classified as a 'Problem'.

The DCC periodically issues a report listing open Problems to Incident Parties and the Panel, setting out for each open Problem:

- The date opened;
- Problem classification;
- Problem status;
- Target closure date;
- Anticipated costs for investigation and resolution of the Problem;
- Anticipated timescales for the closure of a Problem;
- Likely impact on the DCC business, and its effects on Incident Parties of closing a Problem and continuing with a workaround, highlighting instances where implementing a permanent solution may not be the recommended approach, and
- The reason for any target closure date change.

The DCC continues to analyse Problems in a priority set by Incident Parties and the Panel.

The DCC closes the Problem if:

- The permanent fix has been applied;
- An enhanced and acceptable workaround is in place; or
- The DCC is asked not continue investigations by the Panel.

7.9.4.6 Governance

Actor	SEC Document	Clause	Text
7.9.4.5.1 Manage Incident			
Incident Party	SEC Appendix AG - Incident Management Policy	2.1.3	Before raising an Incident with the DCC the Incident Party shall take all reasonable steps to: a) where appropriate, confirm that the issue does not reside within the HAN, or the Smart Meter, or other Devices which the Incident Party is responsible for operating; b) confirm that the issue does not reside within the Incident Party's own systems and processes; c) follow the guidance set out in the self-help material made available by the DCC, including checking for Known Errors and the application of any workarounds specified; and

Actor	SEC Document	Clause	Text
			d) where the party is a User and to the extent that this is possible, use the SSI or submit a Service Request to resolve the Incident in accordance with Section H9.2. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.1.4	In the event that the activities in clause 2.1.3 have been completed and an Incident is to be raised with the DCC, where it has access to the Self-Service Interface, the Incident Party shall check on the Self Service Interface to establish whether an Incident has already been raised or a Service Alert issued for this issue and: a) in the event that the Incident Party can reasonably determine that an Incident or Service Alert for this issue exists, the Incident Party shall notify the Service Desk who shall register the Incident Party as an Interested Party within the Incident Management Log; b) in the event that the Incident Party cannot identify an existing Incident or Service Alert they shall progress to clause 2.2 to raise an Incident. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.1.1	Before raising an Incident the DCC shall take all reasonable steps to ensure an Incident does not already exist for the issue https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.1.2	Pursuant to Section E2.13, prior to the DCC raising an Incident regarding the provision of Registration Data by a Registration Data Provider, the DCC shall take all reasonable steps to confirm that the issue does not reside within the DCC System or processes. https://smartenergycodecompany.co.uk/download/2295
RDP	SEC Appendix AG - Incident Management Policy	2.1.5	Prior to raising an Incident regarding the provision of data to and by the DCC, the Registration Data Provider shall take all reasonable steps to confirm that the issue does not reside within the Registration Data Provider's systems and processes. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.2.2	Where an Incident Party believes that an Incident ought to be treated as a Category 1 Incident (see clause 2.4.4), the Incident Party shall call the Service Desk as soon as reasonably practicable. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident	2.2.3	An Incident Party shall raise what it considers to be Category 2, 3, 4 and 5 Incidents as set out in clause 1.4.10 and provide information as set out in clause 2.3.1, subject

Actor	SEC Document	Clause	Text
	Management Policy		to Section H8.19(a). https://smartenergycodecompany.co.uk/download/2295
DCC, Incident Party	SEC Appendix AG - Incident Management Policy	2.3.1	When raising an Incident, the DCC or Incident Party shall provide the following information: a) Contact name; b) Contact Organisation; c) Contact details; d) Organisation's Incident reference number (where available); e) Date and time of occurrence; f) MPxN or Device ID (where appropriate); g) Summary of Incident; h) Business impact; and i) Results of initial triage and diagnosis including references to existing Incidents, where appropriate, and details of investigations performed to satisfy pre-requisites set out in clause 2.1. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.4.1	The DCC shall assign an Incident Category to an Incident raised by an Incident Party based on the information available at the time the Incident is recorded in the Incident Management Log. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.4.2	The DCC shall assign an Incident Category to an Incident raised by the DCC using information available to the DCC at the time the Incident is recorded in the Incident Management Log. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.4.3	The DCC shall progress the resolution of Incidents in priority order. The DCC shall determine the priority of an Incident by considering the Incident Category and the time remaining until the Target Resolution Time, as defined in clause 2.4.4. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	1.4.10	The DCC and Incident Parties shall each ensure that information regarding Incidents and Problems is recorded and kept up to date in the Incident Management Log as follows: a) for Major Incidents, the Incident Party shall comply with clause 2.2.2 b) the Incident Party shall use the Self Service Interface where it is able to do so and the DCC shall ensure that

Actor	SEC Document	Clause	Text
			information provided in this way is automatically added to the Incident Management Log c) where the Incident Party is unable to use the Self Service Interface, it shall provide information to the Service Desk by email or by phone and the Service Desk shall ensure that this information is entered into the Incident Management Log d) when an Incident is submitted by email and the Incident Party does not provide the required information as detailed in clause 2.3, the Service Desk shall return an email to the Incident Party requesting the missing information and the Incident shall not be recorded in the Incident Management Log until the required information has been received by the Service Desk e) the Service Desk shall enter information that the DCC originates into the Incident Management Log f) the resolver shall ensure all actions to resolve the Incident are recorded in the Incident Management Log g) In regard to items a) – f) above, the DCC and Incident Parties shall each ensure that information is as complete as is possible and is entered into the Incident Management Log as soon as is reasonably practicable. https://smartenergycodecompany.co.uk/download/2295
Incident Party (Optional)	SEC Appendix AG - Incident Management Policy	2.4.5	If an Incident Party believes an Incident has been allocated an incorrect Incident Category by the DCC or has been subsequently updated to an incorrect Incident Category by the DCC, it may invoke the escalation process set out in clause 2.9. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.4.6	The DCC may change the Incident Category of an Incident if more information becomes available. The DCC shall provide to Interested Parties, through a Nominated Individual, details of why the Incident Category has been changed. The DCC shall update the Incident Management Log with the revised Incident Category. https://smartenergycodecompany.co.uk/download/2295
DCC Service Desk	SEC Appendix AG - Incident Management Policy	2.5.1	The Service Desk shall manage Incidents recorded in the Incident Management Log through the Incident lifecycle. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG	2.5.2	The DCC shall assess the Incident and assign resolution activities to the appropriate resolver in accordance with

Actor	SEC Document	Clause	Text
	- Incident Management Policy		Section H9.2, and the resolver may be the DCC or an Incident Party. https://www.smartenergycodecompany.co.uk/docs/default-source/sec-documents/sec-5.8/sec-appendix-ag---incident-management-policy.pdf?sfvrsn=3/SEC Appendix AG - Incident Management Policy#2.5.2-Incident_Management https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.5.3	In the event that Incident resolution activities are assigned to a Registration Data Provider at a time which falls outside of the Registration Data Provider's hours of operation, and where the DCC has classified the Incident as a Category 1 or 2, the DCC shall contact the Registration Data Provider via its out-of-hours facility as provided in accordance with the clause 1.4.6. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.5.4	In the event that Incident resolution activities are assigned to a Registration Data Provider at a time which falls outside of the Registration Data Provider's hours of operation and the DCC has classified the Incident as a Category 3, 4 or 5, the DCC shall contact the Registration Data Provider when their business operations commence on the next Working Day. In such instances the time during which the Registration Data Provider was not able to be contacted shall be disregarded for the purpose of calculating the resolution time for the Incident https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.5.6 (a)	When assigning an Incident to an Incident Party where the DCC requires the Incident Party to diagnose or confirm resolution of an Incident, the DCC shall: a) engage with the Incident Party by a reasonable mechanism; https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.5.6 (b)	When assigning an Incident to an Incident Party where the DCC requires the Incident Party to diagnose or confirm resolution of an Incident, the DCC shall: (b) set the Incident status to pending https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.5.6 (c)	When assigning an Incident to an Incident Party where the DCC requires the Incident Party to diagnose or confirm resolution of an Incident, the DCC shall: (c) assign the activity to the Incident Party, and the resolution time shall not include the period of time

Actor	SEC Document	Clause	Text
			for which the activity is so assigned https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.5.5	Pursuant to H9.8(a), the resolver assigned to an Incident shall perform the appropriate steps to resolve the Incident in accordance with H9.8, and shall record information as set out in clause 1.4.10. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.5.7	The Incident Party shall, using a reasonable mechanism, confirm to the DCC when all activities requested pursuant to clauses 2.5.5 are complete, providing details of steps taken, which the Service Desk shall ensure are included in the Incident Management Log. The DCC shall then reassign the Incident or update the status in the Incident Management Log to resolved, as appropriate, based on the information received. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.5.9	If an Incident Party identifies that an Incident has been assigned to it but it should not be responsible for resolving it, the Incident Party shall advise the Service Desk, providing supporting information, and the DCC shall investigate and re-assign as appropriate https://smartenergycodecompany.co.uk/download/2295
DCC Service Desk	SEC Appendix AG - Incident Management Policy	2.5.8	Where an Incident has been investigated but has subsequently been determined not to be an Incident: a) the Service Desk shall contact the Incident Party that raised the Incident through a Nominated Individual and provide the relevant information that the DCC holds to enable the Incident Party to raise and manage the Incident within its own system; and b) the Service Desk shall set the status of the Incident in the Incident Management Log to closed. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.5.10	The DCC shall collate and make available to Network Parties and the Panel data related to the time taken to resolve Incidents associated with the exchange of data pursuant to Section E of the Code, where the DCC is responsible for resolving the Incident but in order to do so, activity must be undertaken by a Registration Data Provider. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident	2.6.1	The Service Desk shall take all reasonable steps using information available from the Live Services including Incident data, as appropriate, to identify Interested

Actor	SEC Document	Clause	Text
	Management Policy		Parties for an Incident. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.6.2	The DCC shall inform the Interested Parties identified by the DCC of the Incident through a Nominated Individual. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.7.1	Throughout the lifecycle of the Incident, the DCC, via the Service Desk, shall communicate updates to the Incident Party or other identified Interested Parties. These communications may be via email, phone call and/or via updates to the Incident Management Log. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.2	An Incident that the DCC is responsible for resolving shall be resolved by the DCC in accordance with the Target Resolution Times set out in the categorisation matrix in clause 2.4. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.3	The Service Desk and the resolver shall each record details of all steps they have each taken to resolve the Incident in the Incident Management Log, as set out in clause 1.4.10. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.4	The Service Desk shall notify the Incident Party and/or other Interested Parties and the resolver via email when the DCC sets the Incident status to resolved. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.4	The Service Desk shall notify the Incident Party and/or other Interested Parties and the resolver via email when the DCC sets the Incident status to resolved. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.5	If the Incident is resolved through the application of a workaround, the Service Desk shall either raise a new Problem or the Incident shall be associated with an existing Problem where one exists. https://smartenergycodecompany.co.uk/download/2295
Incident Party, Interested Parties, resolver	SEC Appendix AG - Incident Management Policy	2.12.6 (a)	If it does not consider that the Incident is resolved, the Incident Party, resolver or an Interested Party shall respond to the Service Desk via email or phone call within 3 Working Days, unless a longer period has been agreed by the Service Desk, such agreement to not be unreasonably withheld. In so doing, the relevant party

Actor	SEC Document	Clause	Text
			shall provide supporting information as to why they consider the Incident not to be resolved. Then, a) If the Service Desk receives, with supporting information, a response detailing that the Incident is not resolved, the Service Desk will change the status from resolved and reassign the Incident for investigation in accordance with H9; or https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.6 (a)	If it does not consider that the Incident is resolved, the Incident Party, resolver or an Interested Party shall respond to the Service Desk via email or phone call within 3 Working Days, unless a longer period has been agreed by the Service Desk, such agreement to not be unreasonably withheld. In so doing, the relevant party shall provide supporting information as to why they consider the Incident not to be resolved. Then, a) If the Service Desk receives, with supporting information, a response detailing that the Incident is not resolved, the Service Desk will change the status from resolved and reassign the Incident for investigation in accordance with H9; or https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.6 (b)	If it does not consider that the Incident is resolved, the Incident Party, resolver or an Interested Party shall respond to the Service Desk via email or phone call within 3 Working Days, unless a longer period has been agreed by the Service Desk, such agreement to not be unreasonably withheld. In so doing, the relevant party shall provide supporting information as to why they consider the Incident not to be resolved. Then, b) If a response is not received from the Incident Party within the aforementioned time frame the Service Desk shall close the Incident. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.12.7	In the event that the Incident Party requires subject matter expert advice before confirming closure and the subject matter expert is unavailable, the Incident Party may contact the Service Desk via email or phone call to request that the closure period be extended. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.8	In the event that the Incident is the result of an intermittent issue the Service Desk shall apply what it reasonably deems to be an appropriate closure period based on the frequency of the occurrences of the issue, and shall close the Incident after this period has

Actor	SEC Document	Clause	Text
			elapsed without any further occurrences. The Service Desk shall record this in the Incident Management Log. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.12.9	After the Incident has been resolved, the Service Desk may raise a Problem and link it to the Incident https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.13.1	The Incident Party that originally raised an Incident may only re-open it if it was closed with a workaround and one of the following circumstances occurs: a) the workaround fails; or b) the workaround deteriorates to a point that it affects normal business operations. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.13.2	If a Problem associated with an Incident has been closed, it shall not be possible to re-open the Incident. In this case, the Incident Party shall raise a new Incident. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.14.1	If a previous Incident reoccurs after it has been closed in line with the procedures in this Incident Management Policy, the Incident Party shall raise a new Incident, in accordance with the provisions set out above. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.14.2	The DCC may identify re-occurring Incidents by performing trending, correlation and incident matching. Confirmed re-occurrences may be progressed through Problem management https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.14.3	An Incident Party may identify a re-occurring incident and may notify the DCC. In so doing, the Incident Party shall provide all related Incident reference numbers to the DCC who may progress the issue through Problem management, as set out in clause 3. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.2	Once an Incident has been reported to the Service Desk pursuant to clause 2.2.2, the Service Desk shall perform initial triage on the Incident. The Major Incident management process and/or the DCC security team shall be engaged to progress and resolve the Incident where triage confirms that the DCC believes that the Incident should be treated as a Category 1 Incident, unless the

Actor	SEC Document	Clause	Text
			circumstances set out in 2.10.7 apply https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.4	The DCC shall notify all Incident Parties that are likely to be affected by such Major Incident by a reasonable means in accordance with Section H9.11. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.5	On resolution of the Major Incident, the DCC shall raise a Problem to confirm the Root Cause. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.6	The DCC shall make the details from the Problem available to Interested Parties. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.7	Where a Major Incident has been logged and investigated but then turns out to be an Incident which the DCC is not responsible for resolution (as set out in H9.2(b) then the Service Desk shall: a) Contact the appropriate Incident Party through a Nominated Individual; b) assign the Incident to the Incident Party c) set the Incident status to pending https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.8 (a)	Where a Major Incident has been investigated but turns out not to be an Incident: a) the Service Desk shall contact the Incident Party that raised the Incident through a reasonable mechanism and provide the details to enable the Incident Party to raise and manage the incident within their own system https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.8 (b)	Where a Major Incident has been logged and investigated but turns out not to be an Incident: b) the Service Desk shall set the status of the Incident to closed. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.11	The Incident Party shall notify the Panel and Security Subcommittee, in accordance with Section G3, and, pursuant to section H9, the DCC if: a) it detects a security Incident within its environment of which the DCC needs to be informed; b) any potential Security Incident it detects appears to

Actor	SEC Document	Clause	Text
			relate to the DCC Total System. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.10.12	The DCC shall notify the Panel and Security Subcommittee, in accordance with Section G2, and, pursuant to Section H9, inform an Incident Party by an appropriate mechanism if: a) any Security Incident occurs that is identified in the SEC as requiring notification to the Incident Party or the Panel and Security Subcommittee; or b) a Security Incident indicates a breach of the provisions of a Code of Connection. https://smartenergycodecompany.co.uk/download/2295
Incident Party	SEC Appendix AG - Incident Management Policy	2.11.1 (a)	In the event that a Major Incident is assigned to an Incident Party other than the DCC: a) the Incident Party may request that the DCC provides reasonable assistance. When this is requested the DCC shall provide reasonable assistance to the Incident Party responsible for resolving the Incident in accordance with Section H9.12(a) and https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.11.1 (a)	In the event that a Major Incident is assigned to an Incident Party other than the DCC: a) the Incident Party may request that the DCC provides reasonable assistance. When this is requested the DCC shall provide reasonable assistance to the Incident Party responsible for resolving the Incident in accordance with Section H9.12(a) and https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	2.11.1 (b)	(b) as part of such reasonable assistance, the DCC may disseminate the information to Incident Parties if requested by the Incident Party, using the Self Service Interface and other mechanisms as appropriate. https://smartenergycodecompany.co.uk/download/2295
DCC	Smart Energy Code	Section G2.11	The DCC shall, on the occurrence of a Major Security Incident in relation to the DCC Total System, promptly notify the Panel and the Security Sub-Committee. https://smartenergycodecompany.co.uk/download/2479
User	Smart Energy Code	Section G3.5	Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, promptly notify the Panel and the Security Sub-Committee. https://smartenergycodecompany.co.uk/download/2479

Actor	SEC Document	Clause	Text
Incident Party	Smart Energy Code	Section H9.6	Where an Incident Party becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed): (a) (where the Incident Party is a User) to the extent such Incident is reasonably capable of being resolved via the Self-Service Interface or via a Service Request which that User has the right to send, then the User shall exercise such rights with a view to resolving the Incident; or (b) (where the Incident Party is an RDP) to the extent such Incident is reasonably capable of being resolved by re-submitting a subset of Registration Data in accordance with the Registration Data Interface Documents, then the RDP shall re-submit such Data; or (c) where neither paragraph (a) nor (b) above apply (or to the extent the Incident is not resolved despite compliance with paragraph (a) or (b) above), then the Incident Party shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident) via the Self-Service Interface (or, in the case of non-Users, the Service Desk). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H9.7	Where the DCC becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed), then the DCC shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H9.8	Where an Incident has been added to the Incident Management Log (or reopened) pursuant to Section H9.6 or H9.7, then (until such time as that Incident is closed) the DCC and each relevant Incident Party shall each take all the steps allocated to them under and in accordance with the Incident Management Policy in respect of an Incident of the relevant type, so as to: (a) in the case of Incidents for which a Incident Party is responsible, resolve the Incident as soon as reasonably practicable; or (b) in the case of Incidents for which the DCC is responsible, resolve the Incident in accordance with the applicable Target Resolution Time. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H9.9	Where a Problem has been assigned to the DCC or an Incident Party, then (until such time as that Problem is closed) the DCC and each relevant Incident Party shall each take all the steps allocated to it under and in accordance with the Incident Management Policy so as to

Actor	SEC Document	Clause	Text
			close the Problem in accordance with priority for resolution and closure set out in the Incident Management Policy. https://smartenergycodecompany.co.uk/download/2483
Incident Party	Smart Energy Code	Section H9.10	Where an Incident Party identified as responsible for resolution of an Incident, and where that Incident Party considers (or should reasonably have considered) that the Incident constitutes a Major Incident, then such Incident Party shall notify the DCC of such fact (in accordance with the Incident Management Policy). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H9.11	Where the DCC becomes aware of a Major Incident, the DCC shall notify all Incident Parties that are likely to be affected by such Major Incident (in accordance with the Incident Management Policy). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H9.12	In the event of a Major Incident: (a) where the DCC is responsible for resolving that Incident, each Incident Party shall provide the DCC with all reasonable assistance as the DCC may request; and (b) where an Incident Party is responsible for resolving that Incident, the DCC and all other Incident Parties shall provide all reasonable assistance to the Incident Party responsible for resolving that Incident as such Incident Party may request, (in each case) in relation to the resolution of that Incident, including as set out in the Incident Management Policy. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H9.13	Within two Working Days following resolution of a Major Incident, the DCC or the Incident Party responsible for resolving that Major Incident shall provide a summary report to the Panel in respect of that Major Incident. Such summary report must include (as a minimum): (a) the nature, cause and impact (and likely future impact) of the Major Incident (including, where the DCC is responsible for resolving the Major Incident, details of the impact of the Major Incident had on provision of the Services and over what period, and details of any Data that may have been lost); and (b) the action taken in the resolution of the Major Incident. https://smartenergycodecompany.co.uk/download/2483

Actor	SEC Document	Clause	Text
DCC	Smart Energy Code	Section H9.14	Within 20 Working Days following resolution of a Major Incident, the DCC or Incident Party responsible for resolving that Major Incident shall conduct a review regarding that Major Incident and its resolution, and shall report to the Panel and the Authority (and, on request, the Secretary of State) on the outcome of such review. Such report must include (as a minimum): (a) a copy of the summary report produced in respect of the Major Incident pursuant to Section H9.13; (b) where the DCC is responsible for resolving the Major Incident) any Services which were not restored within the Target Resolution Time for the Major Incident; (c) (where the DCC is responsible for resolving the Major Incident) where any Services were not restored within the Target Resolution Time, the reason why this was the case and the steps the DCC is taking to prevent the re-occurrence of such an event; (d) a review of the response to the Major Incident and its effectiveness; (e) any failures by Incident Parties to comply with their obligations under Energy Licences and/or this Code that caused or contributed to the Major Incident or its consequences; (f) (where the DCC is responsible for resolving the Major Incident) whether there is likely to be a reduction (and, to the extent reasonably capable of being determined at that time, the amount of the anticipated reduction) in the DCC's External Costs (as defined in the DCC Licence) arising as a consequence of the DCC Service Providers failing to achieve a restoration of any Services within the Target Resolution Time; and (g) any Modifications that could be made to this Code to mitigate against future Incidents and/or their consequences. https://smartenergycodecompany.co.uk/download/2483
	Smart Energy Code	Section H9.15	The Panel shall make each report produced by the DCC pursuant to Section H9.14 available to the other Parties, subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices. https://smartenergycodecompany.co.uk/download/2483
7.9.4.5.2 Manage Problem			
DCC	Smart Energy Code	Section H9.5	Where an Incident refers to a Problem, the DCC or any Incident Party may request that the person assigned responsibility for the Problem supplies to the DCC or Incident Party making the request reasonable information regarding the Problem,

Actor	SEC Document	Clause	Text
			provided that information in respect of any other Incident shall only be supplied to an Incident Party where that Incident Party would be allowed access to that information in accordance with Section H9.4. https://smartenergycodecompany.co.uk/download/2483
DCC	SEC Appendix AG - Incident Management Policy	3.1.1	The DCC shall open a Problem in the Incident Management Log in the following circumstances: a) when a Major Incident has been resolved; b) when an Incident is closed with a workaround applied; or c) when the DCC has identified a re-occurring Incident. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	3.1.2	The DCC shall allocate a reasonable initial timescale for carrying out the Root Cause Analysis to enable the re-classification of the Problem as a Known Error. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	3.2.1	The DCC shall periodically issue and make available a report listing open Problems to Incident Parties and the Panel. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	3.2.2	The report shall set out for each open Problem: a) date opened; b) Problem classification; c) Problem status; d) the target closure date; e) the anticipated costs (in DCC's reasonable opinion) for the investigation and resolution of the Problem, where appropriate; f) the anticipated timescales for the closure of a Problem; g) the likely impact on the DCC's business, and its effects on Incident Parties of closing a Problem and continuing with a workaround, highlighting instances where implementing a permanent solution may not be the recommended approach; and h) the reason for any target closure date change. https://smartenergycodecompany.co.uk/download/2295
DCC, Interested Party	SEC Appendix AG - Incident Management Policy	3.2.3	Following the issuing of such a report, the DCC shall discuss with Incident Parties the prioritisation and preferred timescales for the progression of each Problem. Following discussion, and taking respondents' views into account, the DCC will determine the prioritisation and

Actor	SEC Document	Clause	Text
			preferred timescales for the progression of each Problem. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	3.2.4	If a Problem investigation or resolution requires a change to the SEC a Modification Proposal shall be raised and submitted by the DCC. https://smartenergycodecompany.co.uk/download/2295
DCC, Interested Party	SEC Appendix AG - Incident Management Policy	3.3.2	Following the application of a permanent fix, the DCC shall discuss the outcome with Interested Parties before closing the Problem. https://smartenergycodecompany.co.uk/download/2295
DCC	SEC Appendix AG - Incident Management Policy	3.3.4	The DCC shall only close a Problem once one of the following conditions has been met and the DCC has discussed this with Interested Parties that: a) the permanent fix has been applied; or b) an enhanced and acceptable workaround is in place; or c) the DCC will not continue investigations https://smartenergycodecompany.co.uk/download/2295

7.9.5 No WAN Issues

7.9.5.1 Introduction

Most premises covered by the roll-out obligation will have WAN coverage. This process area describes the steps that the Supplier may take when WAN is not available.

Three scenarios are considered:

- WAN coverage will not be available for the premises
- WAN coverage is available but is not available during installation
- WAN is temporarily unavailable

7.9.5.2 Scope

This process area includes:

- Statement of Service Exemption.
- Temporary loss of WAN Connectivity

This process area involves but does not specifically describe:

- Read (Non-Device) – Request WAN Matrix. This process is described in Section 7.4.1.6.3 of the BAD;

- Manage Incidents. This process is described in Section 7.9.4.5.1 of the BAD;
- Install and Leave. This process is described in Section 7.2.2 of the BAD.

7.9.5.3 Actors

- Supplier
- DCC
- Smart Meter
- SIMCH
- Installer

7.9.5.4 Process Description

7.9.5.4.1 Read (Non-Device) – Request WAN Matrix

The Supplier plans the installation, taking into account the availability of the WAN Coverage in the premises. The Supplier either composes a 'Request WAN Matrix' Service Request (SRV 12.1) and sends it to the DCC or looks up the SSI to check the WAN Coverage Database. This process is described in more detail in Section 7.4.1 of the BAD.

7.9.5.4.2 Statement of Service Exemption

Some premises may never get an adequate WAN coverage, typically because of environmental factors. These premises are covered by a Statement of Service Exemption maintained by the DCC and available to Parties.

Where no WAN coverage is expected, the Supplier checks whether there is a Statement of Service Exemption in place which covers the premises. If yes, the Supplier would not be expected to offer Smart Meters to the Energy Customer.

7.9.5.4.3 Install and Leave

If no Statement of Service Exemption exists, and the WAN will become available at a later date, the Supplier may:

- If the installation is for a new supply, or to replace a faulty meter, complete Proactive Install and Leave. This is process is described in Section 7.2.2 of the BAD; or
- Wait with the installation until the WAN becomes available.

If WAN coverage exists for the premises, the Supplier arranges the installation. If the WAN is not available on the installation day, the Supplier may follow the Install and Leave process (Reactive Install and Leave). For more detail see Section 7.2.2 of the BAD.

The DCC has 90 days from the receipt of a 'Communications Hub Status Update - Install No SM WAN' Service Request (SRV 8.14.2) to resolve the lack of SM WAN coverage, and is expected to clear 99% of Incidents in that time.

The exact resolution will vary depending upon the nature of the problem, and whether the premises are in the Northern, Central or Southern Regions, but the most likely options are:

- Await completion of the relevant Network Enhancement Plan[25];
- Installation of a T3 Aerial*; or
- Installation of a Special Installation Mesh Communications Hub (SIMCH)*

* these options apply in the Southern and Central Regions only.

If the DCC determines that a special installation is required, it notifies the Supplier. The Supplier may request help from the DCC.

The Supplier is responsible for:

- Gaining the Energy Consumers consent;
- Planning and organising the site visit with the DCC's field engineers; and
- Installing the SIMCH.

The DCC is responsible for:

- Providing the SIMCH; or
- Providing and installing the T3 Aerial.

In the event that the special installation work does not provide WAN coverage, the Supplier is responsible for deciding whether to remove the equipment or leave it in place.

Whilst waiting for the WAN coverage issue to be resolved, the Supplier may choose to continue with the Install and Leave process, or abort the installation. If the Energy Consumer changes Suppliers during this time, there is currently no decision on who remains the Incident Party in this circumstance.

7.9.5.4.4 Manage Incidents

There may be temporary interruptions to the WAN availability once installation is complete. If this happens, the Supplier raises an Incident. This process is described in Section 7.9.4.5.1 of the BAD.

7.9.5.5 Associated Process Areas

#	Process Areas

[25] In some cases, the DCC may determine the most cost-effective solution is to install Mesh CHs in adjacent premises, allowing the WAN signal to "leapfrog" between CH. This may require multiple suppliers to work together and – in the worst case – require existing working CH to be replaced with Mesh CH.

7.2.2	Install and Leave
7.2.1	Install and Commission
7.4.1	Read
7.9.4	Manage Incidents

7.9.5.6 Governance

The BEIS Response[26] clarified that under the Reactive Install and Leave scenario, the establishment of the HAN should not be an absolute requirement, and that Proactive Install and Leave is only permissible in the case of new connections and where the WAN is to arrive by 2020. BEIS will amend licence conditions to clarify when cases of Reactive and Proactive Install and Leave will count towards Suppliers' rollout obligations.

Actor	SEC Document	Clause	Text
7.9.5.4.3 Install and Leave			
DCC	Smart Energy Code	Section F7.18	Where a Communications Hub is installed at a premises in accordance with this Code but does not connect to the SM WAN, and the SM WAN Coverage Database indicated (at any time during the 30 days prior to the date of installation) that the SM WAN is (or would be) available in the area in which the premises is located on the installation date, then the DCC shall (within 90 days after having been notified in accordance with the CH Installation and Maintenance Support Materials): (a) provide a response to the installing Supplier Party that either (i) confirms that the SM WAN is now available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN; or (ii) provides reasons why the SM WAN is not so available; and (b) (subject to Section F7.20) ensure that, in the case of at least 99% of all Communications Hubs for which the DCC is required to give such a response in each calendar quarter, the SM WAN is made available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN (but excluding for this purpose those locations where SM WAN connectivity is affected by problems with access pursuant to Section F7.5 which arise otherwise than as a result of the DCC's breach of this Code). F7 https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F7.19	Where a Communications Hub is installed at a premises in accordance with this Code but does not connect to the SM WAN (in circumstances where Section F7.18 does not apply), and the SM WAN Coverage Database is updated after installation to indicate that the premises is within an area in which the SM WAN is available, then (provided the DCC has

[26] Smart Meters Rollout Strategy Government Response

			been notified of the installation in accordance with the CH Installation and Maintenance Support Materials) the DCC shall (within 90 days after such update occurs): (a) provide a response to the Supplier Party which installed the Communications Hub that either (i) confirms that the SM WAN is now available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN; or (ii) provides reasons why the SM WAN is not so available; and (b) (subject to Section F7.20) ensure that, in the case of at least 99% of all Communications Hubs for which the DCC is required to give such a response in each calendar quarter, the SM WAN is available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN (but excluding for this purpose those locations where SM WAN connectivity is affected by problems with access pursuant to Section F7.5 which arise otherwise than as a result of the DCC's breach of this Code). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F7.20	Until 1 January 2021, Sections F7.18(b) and F7.19(b) do not apply to Communications Hubs installed at premises within a geographic area that is subject to a Network Enhancement Plan. Such Communications Hubs shall, until 1 January 2021, be excluded from the calculations under Sections F7.18(b) and F7.19(b). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F7.21	Within a reasonable period of time following each calendar quarter that ends prior to 1 January 2021, the DCC shall produce a report which identifies: (a) any new Network Enhancement Plans that have been created during that quarter, any Network Enhancement Plans that were completed during that quarter, and any ongoing Network Enhancement Plans; and (b) for each such Network Enhancement Plan: (i) an overview of the geographic area that is subject to the plan; (ii) the premises (by postcode) that fall within that area; and (iii) the scheduled date for completion of the planned works (or, where applicable, the actual date of completion). https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F7.22	A copy of the report produced under Section F7.21 shall be provided by the DCC to the Parties, the Panel, the Authority and (on request) the Secretary of State. https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F7.5	Where the CH Installation and Maintenance Support Materials require the DCC to undertake works on behalf of a

			Supplier Party, and where such works require the consent or agreement of any person other than the Supplier Party or the DCC (including where the consent or agreement of the Energy Consumer and/or any landlord or other owner of premises is required), then that Supplier Party shall ensure that such consent or agreement is obtained in advance (and the DCC shall provide all information reasonably requested by the Supplier Party in relation to it obtaining such consent or agreement). https://smartenergycodecompany.co.uk/download/2476
Supplier	Smart Energy Code	Section F7.6	A Supplier Party responsible under Section F7.5 for obtaining a consent or agreement in relation to works shall take reasonable steps to obtain such consent or agreement in a form that permits the installation, operation, repair, modification, replacement and removal of the equipment https://smartenergycodecompany.co.uk/download/2476
DCC	Smart Energy Code	Section F7.7	Where the DCC attends any premises and/or undertakes any works in reliance on a consent or agreement obtained (or required to be obtained) by a Supplier Party under Section F7.5, the DCC shall do so: (a) as the contractor of that Supplier Party; (b) in accordance with Good Industry Practice, the applicable consent or agreement obtained pursuant to Section F7.5 (and notified to the DCC), and the site rules and reasonable instructions of the owner and/or occupier of the relevant premises; (c) in compliance with all Laws and/or Directives applicable to the Supplier Party or its representatives (and notified to the DCC), including the requirements of the Supplier Party's Energy Licence concerning Supplier Party representatives who attend premises; and (d) in compliance with all reasonable requests of the Supplier Party. https://smartenergycodecompany.co.uk/download/2476
Supplier, DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.1	Where DCC identifies that resolution of an Incident relating to the ability to connect to the SM WAN requires work to be undertaken at a premises, the DCC shall notify the Supplier Party that raised the Incident accordingly. Such notification shall include details of the potential work required. The Supplier Party that raised the Incident may request that the DCC undertakes such work at the premises and the DCC shall be required to undertake such work, subject to the provisions of Section F7.5 – F7.7 of the Code. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH	6.2	Where a Supplier Party requires the DCC to undertake work at the premises, the Supplier Party shall update the Incident

	Installation and Maintenance Support Materials		accordingly. The Supplier Party shall update the Incident with the following information when it is available: (a) confirmation that consent for the work to be carried out has been obtained in accordance with Section F7.5 and F7.6 of the Code; (b) the date and time at which the DCC should attend the relevant premises to carry out the work where; (i) the Supplier Party shall ensure that the date shall be a Working Day, and the time shall be between 09:00 and 17:00; (ii) the Supplier Party shall ensure that the date is no less than five (5) Working Days after the date of this update; and (c) contact details that the DCC should use to confirm attendance prior to the agreed date and time or in the event that further liaison with the Supplier Party is required (d) details of the reasoning for the need for DCC to attend. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.3	Following the updates made pursuant to clause 6.2, the DCC shall subsequently update the Incident to provide contact details for its field force engineers at least one full Working Day prior to the date and time set for attendance at the relevant premises. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.4	The DCC shall take all reasonable steps to attend the relevant premises at the specified date and time to undertake the work in accordance with Section F7.7 of the Code and shall notify the Supplier Party immediately where a delay to arrival is likely. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.5	Where the DCC fails to meet the appointment, the DCC shall provide a list of reasonable options for revised dates and times from which the Supplier Party may select. Where the Supplier Party selects one of the potential dates and times offered by the DCC the provisions of clause 6.4 shall apply to that new date and time. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.6	Where, in the Central Region and South Region, the DCC attends the relevant premises and identifies that T3 Aerial Type is required to resolve an Incident, the DCC shall: (a) provide a T3 Aerial Type and any other equipment required to achieve connectivity between the Communications Hub and the SM WAN; and (b) undertake such authorised work as is required to install such aerial and any additional required equipment.

			https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.7	Where, in the Central Region and South Region, the DCC attends the relevant premises and identifies that a Special Installation Mesh Communications Hub is required to resolve an Incident, the Supplier Party shall install a Special Installation Mesh Communications Hub provided by the DCC (as further set out in the CH Handover Support Materials) by following the fitting procedure set out in Annex A.1 of this document. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.8	Following completion by the Supplier Party of the fitting procedure set out in Annex A.1 of this document for a Special Installation Mesh Communications Hub, the DCC shall: (a) provide an aerial and any other equipment required to connect the Special Installation Mesh Communications Hub to the SM WAN; and (b) undertake such work as is required to install such aerial or other equipment. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	6.9	Where successful connection to the SM WAN is indicated, following installation of either: (a) a Special Installation Mesh Communications Hub, aerial and any additional required equipment: or (b) a T3 Aerial Type; the Supplier Party shall complete the procedure set out in clause 4.6. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	6.10	Where successful connection to the SM WAN is not achieved, following installation of a Special Installation Mesh Communications Hub, aerial and any additional required equipment, the Supplier Party may either: (a) follow the fault handling procedure in accordance with clauses 8.3 to 8.6; (b) leave the Special Installation Mesh Communications Hub installed without establishing a connection to the SM WAN by following the CH No SM WAN Installation Procedure; or (c) remove the Special Installation Mesh Communications Hub in accordance with the process set out in Annex A of this document, in which case: (i) the DCC shall remove the aerial and other equipment installed in accordance with 6.8(b); (ii) the Supplier Party shall return the Special Installation Mesh Communications Hub to the DCC in accordance with clause 10.1 and in accordance with Section F7.4A; (iii) the Supplier Party shall update the existing Incident with details of the steps that have been undertaken within three (3) Working Days; and

			(iv) a notification shall be deemed not to have occurred for the purposes of Section F7.18. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	6.11	Where a successful connection to the SM WAN is not achieved, following installation of a T3 Aerial Type and any additional required equipment, and where the DCC has decided not to require the Supplier to install a Special Installation Mesh Communications Hub, the Supplier Party may either: (a) follow the fault handling procedure in accordance with clauses 8.3 to 8.6; (b) leave the Communications Hub installed and connected to the T3 Aerial Type without establishing a connection to the SM WAN by following the CH No SM WAN Installation Procedure; or (c) in accordance with any instruction from DCC, restore the Communications Hub aerial to its previous state, in which case: (i) the DCC shall remove the T3 Type Aerial and other equipment installed in accordance with 6.8(b); (ii) the Supplier Party shall update the existing Incident with details of the steps that have been undertaken within three (3) Working Days; and (iii) a notification shall be deemed not to have occurred for the purposes of Section F7.18. https://smartenergycodecompany.co.uk/download/2336
DCC	SEC Appendix I - CH Installation and Maintenance Support Materials	6.12	No Party other than the DCC may install, repair or remove T3 Type Aerials and other equipment installed in accordance with clause 6.8(b), without first seeking permission from DCC (save that such a Party may take action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property). https://smartenergycodecompany.co.uk/download/2336
7.9.5.4.4 Manage Incidents			
Supplier	SEC Appendix I - CH Installation and Maintenance Support Materials	8.12	Where a Supplier Party determines that, having undertaken the relevant Communications Hub Fault Handling Procedure, no fault exists with a Communications Hub, but no SM WAN connection is achieved, that Supplier Party shall raise or update an Incident in accordance with the Incident Management Policy to inform DCC of a local SM WAN connectivity issue, subject to clause 8.13. https://smartenergycodecompany.co.uk/download/2336
Supplier	SEC Appendix I - CH Installation and	8.13	Prior to informing DCC of a local SM WAN connectivity issue a Supplier Party shall: (a) ensure that the power supply to the Communications Hub is maintained following the completion of the fault handling procedure;

	Maintenance Support Materials		(b) verify that the Communications Hub Status Information does not indicate any fault other than failure to connect to the SM WAN; and (c) ensure that the Communications Hub is fitted with a security seal. https://smartenergycodecompany.co.uk/download/2336

7.9.6 Recall Communications Hub

7.9.6.1 Introduction

Devices forming part of Enrolled SMSs may be recalled, typically because they may have a recognised defect.

The SEC does not cover any processes associated with recalling Devices other than the CH. The responsibility for recalling CH sits with the DCC.

7.9.6.2 Scope

This process area includes recalls of CHs.

7.9.6.3 Actors

- Suppliers
- Parties
- DCC

7.9.6.4 Process Description

7.9.6.4.1 Recall Communications Hub

The DCC recalls a CH, and informs the Supplier.

Parties will be compensated by the DCC for the reasonable costs and expenses they incur:

- In taking any corrective actions; and / or
- In notifying consumers and other Parties of the planned corrective action.

7.9.6.5 Associated Process Areas

#	Process Areas
7.6.1	Replace Communications Hub
7.9.1	Order and Return Communications Hub

7.9.6.6 Governance

Actor	SEC Document	Clause	Text
7.9.6.4.1 Recall Communications Hub			

DCC	Smart Energy Code	Section F 9.23	Where the reason for a Communications Hub's return is determined in accordance with this Section F9 to have been a Product Recall or Technology Refresh, then the DCC shall (notwithstanding Section M2.8 (Exclusion of Other Liabilities)) be liable to each other Party for the reasonable costs and expenses incurred by that Party in: (a) any corrective action taken by that Party in accordance with this Code or other Laws and/or Directives (including any withdrawal or recall activities); and/or (b) notifying or warning Energy Consumers of any corrective action taken by the DCC and/or any other Party (and providing Energy Consumers with relevant information regarding such corrective action). https://smartenergycodecompany.co.uk/download/2476

7.9.7 Elective Communication Services

7.9.7.1 Introduction

DCC Users may request Communication Services in respect of additional functionality of Devices that form part of Enrolled SMSs from the DCC. This process area describes the process for requesting such Services.

7.9.7.2 Actors

- User
- DCC

7.9.7.3 Prerequisites

Devices to which communications will be sent form part of an Enrolled SMS.

7.9.7.4 Process Description

7.9.7.4.1 Request Elective Communications Services

A Party requests an evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service. If following the evaluation, the Party wishes to proceed, it requests a formal offer from the DCC to provide the Elective Communication Service.

The DCC makes an offer (unless it is not required to do pursuant to Condition 17 of the DCC Licence), and includes the following in the offer:

- details of the Charges that would apply to the Elective Communication Service determined in accordance with the Charging Methodology;
- where the proposed Charges have been calculated on the assumption that one or more other Parties accept offers, two alternative sets of Charges, one of which is contingent on acceptance of all the other such offers and one of which is not; and

- include an offer by the DCC to enter into a Bilateral Agreement.

The Bilateral Agreement needs to describe the Elective Communication Service in the same way as the Core Communication Services.

Once the DCC has commenced provision of the Elective Communication Service, the DCC notifies the Code Administrator of the date on which the Service commenced.

Within 6 months of starting to provide the Elective Communication Service, the DCC provides to the Code Administrator:

- a brief description of the Elective Communication Service;
- the frequency with which, and the period during which, it is provided; and
- the Target Response Time for it.

The Code Administrator publishes the details provided on the website, and reports to the Panel on whether the DCC has provided details.

7.9.7.5 Commentary

The SEC requires that the Elective Communication Services are defined in a manner consistent with the description of the Core Communication Services in the SEC. The applicable definitions state that Critical Service Requests are defined as such in SEC Appendix AD – DCC User Interface Specification, while Non-Critical can be inferred from SEC Appendix E – DCC User Interface Services Schedule. However, SEC Appendix E – DCC User Interface Services Schedule does not define which SRVs are Critical, which may imply that all SRVs are Non-Critical. To clarify this inconsistency, a minor change to the definition of Non-Critical Service Requests is needed.

7.9.7.6 Governance

Actor	SEC Document	Clause	Text
7.9.7.4.1 Request Elective Communications Services			
Party	Smart Energy Code	Section H7.4	Notwithstanding Section E7.2, any Party may request an initial evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service (a "Preliminary Assessment"). https://smartenergycodecompany.co.uk/download/2483
Party	Smart Energy Code	Section H7.5	Requests for a Preliminary Assessment shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC. https://smartenergycodecompany.co.uk/download/2483

Actor	SEC Document	Clause	Text
Party	Smart Energy Code	Section H7.7	Any Party that has requested a Preliminary Assessment and obtained a response as described in Section H7.6(b) may request a more detailed evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service (a "Detailed Evaluation"). https://smartenergycodecompany.co.uk/download/2483
Party, DCC	Smart Energy Code	Section H7.8	Requests for a Detailed Evaluation shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC. Following receipt of any such request (or purported request), the DCC shall: (a) where the request is incomplete or the DCC reasonably requires further information in order to assess the request, notify the Party that this is the case and provide reasonable assistance to the Party in re-submitting its request; (b) once the DCC has received all the information it reasonably requires in order to assess the request, confirm the applicable Charges payable in respect of the Detailed Evaluation; and (c) once the Party has agreed to pay the applicable Charges, provide the Detailed Evaluation to the requesting Party (in accordance with the time period prescribed by Condition 17 of the DCC Licence). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart DCC Licence	17.7	The Licensee, on receiving a request from any SEC Party ("the Requester") for the provision of Elective Communication Services under or pursuant to the SEC, must deliver to the Requester as soon as is reasonably practicable, and in any event within 14 days after receiving the request, either: (a) an initial evaluation of the technical feasibility and the likely scale of the cost of satisfying that request for such provision; or (b) notification that the initial evaluation indicates that a further and more detailed evaluation of the request is required. https://epr.ofgem.gov.uk/Content/Documents/Smart%20DCC%20Limited%20-%20Smart%20Meter%20Communication%20Consolidated%20Licence%20Conditions%20-%20Current%20Version.pdf

Actor	SEC Document	Clause	Text
Party	Smart Energy Code	Section H7.9	Any Party that has requested a Preliminary Assessment in respect of a proposed Elective Communication Service, and obtained a response as described in Section H7.6(a), may request a formal offer for that proposed Elective Communication Service. https://smartenergycodecompany.co.uk/download/2483
Party	Smart Energy Code	Section H7.10	Any Party that has requested and obtained a Detailed Evaluation in respect of a proposed Elective Communication Service may request a formal offer for that proposed Elective Communication Service https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H7.11	Following a request pursuant to Section H7.9 or H7.10, the DCC shall (in accordance with the time period prescribed by Condition 17 of the DCC Licence): (a) make an offer to provide the Elective Communication Service in question; or (b) notify the Party that the DCC is not willing to make such an offer (provided that the DCC may only do so where the DCC is not obliged to make such an offer in accordance with Condition 17 of the DCC Licence). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart DCC Licence	17.8	Where paragraph 17.7(a) is applicable, and insofar as the Requester wishes to proceed with the request, the Licensee must offer within 28 days (except where the Requester agrees to a longer period, or where the Authority otherwise consents) to enter into an Agreement for Services with the Requester on such terms as may be agreed. https://epr.ofgem.gov.uk/Content/Documents/Smart%20DCC%20Limited%20-%20Smart%20Meter%20Communication%20Consolidated%20Licence%20Conditions%20-%20Current%20Version.pdf
DCC	Smart Energy Code	Section H7.12	An offer to provide the Elective Communication Service made by the DCC pursuant to this Section H7 shall: (a) include details of the Charges that would apply to the Elective Communication Service, as determined in accordance with the Charging Methodology; (b) where the proposed Charges have been calculated (in accordance with the Charging Methodology) on the assumption

Actor	SEC Document	Clause	Text
			that one or more other Parties accept offers made pursuant to this Section H7, provide for two alternative sets of Charges, one of which is contingent on acceptance of all the other such offers and one of which is not; and (c) include an offer by the DCC to enter into a Bilateral Agreement with the Party requesting the Elective Communication Service. https://smartenergycodecompany.co.uk/download/2483
Party, DCC	Smart Energy Code	Section H7.13	Each Bilateral Agreement must: (a) be based on the Specimen Bilateral Agreement, subject only to such variations from such specimen form as are reasonable in the circumstances; (b) not contradict or seek to override any or all of this Section H or Sections G (Security), I (Data Privacy), J (Charges), L (Smart Metering Key Infrastructure) or M (General); (c) where reasonably necessary in accordance with the Charging Methodology, provide for Charges that include or comprise a standing charge that is payable by the recipient of the Elective Communication Service regardless of whether or not the Elective Communication Service is requested or provided; (d) where reasonably necessary in accordance with the Charging Methodology, require the recipient of the Elective Communication Service to pay compensation to DCC in the event of the early termination of the Bilateral Agreement (except in the case of termination as envisaged by Section H7.13(e)); (e) allow the recipient of the Elective Communication Services to terminate the Bilateral Agreement without paying compensation to the extent that such compensation is intended to recover investments made for the purposes of providing the Elective Communication Service where (and to the extent that) the DCC subsequently offers a Service listed in the DCC User Interface Services Schedule that relies upon such investments (and each Bilateral Agreement must provide for disputes regarding this provision to be subject to an initial Panel determination, but to ultimately be determined by arbitration); and (f) where reasonably necessary, require the recipient of the Elective Communication Services to provide credit support in

Actor	SEC Document	Clause	Text
			respect of its obligation to pay the compensation referred to in Section H7.13(d). https://smartenergycodecompany.co.uk/download/2483
Party, DCC	Smart Energy Code	Section H7.14	The parties to each Bilateral Agreement shall ensure that the Bilateral Agreement describes the Elective Communication Services in a manner consistent with the description of the Core Communication Services in this Code, including so as to identify (to the extent appropriate) equivalents of the following concepts: Service Requests; Non-Device Service Requests; Pre-Commands; Signed Pre-Commands; Commands; Services Responses; Alerts; and Target Response Times. To the extent that an Elective Communication Service comprises equivalents of such concepts, references to such concepts in this Code shall be construed as including the equivalent concepts under each Bilateral Agreement (and the DCC and the relevant User under the Bilateral Agreement shall comply with Sections H3 (DCC User Interface) and H4 (Processing Service Requests) in respect of the same). For the purposes of each Elective Communication Service (unless the Panel otherwise determined on a User's application): (a) the applicable Service Request shall be deemed to be a Critical Service Request, unless it results only in the sending of a Command to a Device that would arise were a Non-Critical Service Request listed in the DCC User Interface Service Schedule to be requested; (b) the applicable Service Request (and any associated Pre-Command) shall be deemed to contain Data that requires Encryption, unless it contains only Data described in the GB Companion Specification as capable of being sent without Encryption. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H7.15	Elective Communication Services shall be provided in accordance with this Code and the applicable Bilateral Agreement. In the event of any inconsistency between this Code and a Bilateral Agreement, the provisions of this Code shall prevail. https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H7.16	The DCC shall not agree to any variations to a Bilateral Agreement that would cause that agreement to become inconsistent with the requirements of this Section H7. https://smartenergycodecompany.co.uk/download/2483

Actor	SEC Document	Clause	Text
Party	Smart Energy Code	Section H7.17	Where the requirements of Condition 20 of the DCC Licence are met, a Party that has requested an offer for a proposed Elective Communication Service may refer a dispute regarding such request to the Authority for determination under and in accordance with that Condition. https://smartenergycodecompany.co.uk/download/2483
Authority	Smart DCC Licence	20.1	This condition provides for the Authority to determine any dispute arising between the Licensee and any person about the terms on which certain Services are offered to be provided under or pursuant to the requirements of Condition 17 (Requirements for the provision of Services). https://epr.ofgem.gov.uk/Content/Documents/Smart%20DCC%20Limited%20-%20Smart%20Meter%20Communication%20Consolidated%20Licence%20Conditions%20-%20Current%20Version.pdf
DCC	Smart Energy Code	Section H7.18	Once the DCC has commenced provision of an Elective Communication Service pursuant to a Bilateral Agreement, the DCC shall notify the Code Administrator of the date on which the provision of such service commenced (but shall not provide any details regarding such agreement to the Code Administrator). https://smartenergycodecompany.co.uk/download/2483
DCC	Smart Energy Code	Section H7.19	The DCC shall, on or around the date falling six months after it commenced provision of an Elective Communication Service pursuant to a Bilateral Agreement, provide to the Code Administrator the following details: (a) a brief description of the Elective Communication Service; (b) the frequency with which, and (where stated) the period during which, the Elective Communication Service is to be provided; and (c) the Target Response Time within which the Elective Communication Service is to be provided. https://smartenergycodecompany.co.uk/download/2483
Code Administrator	Smart Energy Code	Section H7.20	The Code Administrator shall arrange for the publication on the Website of the details provided to it pursuant to Section H7.19. The Code Administrator shall monitor and report to the Panel on whether the DCC has provided details pursuant to Section H7.18 in

Actor	SEC Document	Clause	Text
			respect of Elective Communication Services of which the Code Administrator is notified under Section H7.18. https://smartenergycodecompany.co.uk/download/2483

Appendix A - Glossary

Term	Acronym	Meaning
Accumulated Debt Register		has the meaning given to that expression in the Communications Hub Technical Specifications.
Acknowledgement		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Active Power Import		means the import of Active Power measured by Electricity Smart Meter.
Ad Hoc Device CSR Web Service Interface		means the system-to-system interface provided to the SMKI for the purposes of SMKI Subscribers refreshing Device Certificates following a Device CSR for the respective Device being approved through a Batch or Ad Hoc CSR to the SMKI Portal.
Ad-Hoc Device Certificate Signing Request	Ad-Hoc DCSR	means a CSR for a Device Certificate that is not part of a Batched Certificate Signing Request.
Alerts		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Anomaly Detection Threshold	ADT	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Anomaly Detection Threshold File	ADT File	means a CSV file submitted by a User for the purposes of notification of ADT and Warning Thresholds to be applied by the DCC.
Arm		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
ARO Nomination Form		has the meaning given to that expression in SEC Appendix D, Annex A.
Association		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Assurance Certificate		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Assurance Certificate Bodies	ACB	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Authentication		has the meaning given to that expression in the Great Britain Companion Specification.
Authorised Responsible Officer	ARO	means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP
Authorised Subscriber		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Authorised Subscriber Application Form		has the meaning given to that expression in SEC Appendix D, Annex A.
Authority		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Auxiliary Load Control Switches	ALCS	has the meaning given to that expression in the Great Britain Companion Specification.
Batched Certificate Signing Request	Batched CSR	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Batched Device CSR Web Service Interface		means the system-to-system interface provided to the SMKI for the purposes of SMKI Subscribers refreshing Device Certificates following a Device CSR for the respective Device being approved following the submission of a Batched Certificate Signing Request.
Block Counters		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Block Pricing		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Business Architecture		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Business Architecture Document	BAD	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Business Architecture Model	BAM	means the Business Architecture Model, a diagrammatic representation of the Business Architecture.
Business Continuity and Disaster Recovery		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Certification Authority Certificates		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Certificate Based Key-Establishment	CBKE	has the meaning given to that expression in the Great Britain Companion Specification.
Certificate Revocation List	CRL	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Certificate Revocation Request	CRR	has the meaning given to that expression in SEC Appendix B.
Certificate Signing Request	CSR	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Certificate Signing Request	CSR	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Certification Path Validation		has the meaning given to that expression in the Great Britain Companion Specification.
Certified Products List	CPL	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
CH Fault Diagnosis		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
CH Order Management System		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
CH Ordering System		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Change of Supplier	CoS	means the process by which a Supplier becomes the Responsible Supplier for a Metering Point.
Change of Tenant	CoT	means the process by which Energy Suppliers maintain their records of which consumers are occupants of which premises.
Check Cryptographic Protection		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
CHF Identifier		has the meaning given to that expression in the Communications Hub Technical Specifications.
Code of Connection		means one of the following Subsidiary Documents: DCC Gateway Connection Code of Connection; DCC User Interface Code of Connection; Registration Data Interface Code of Connection; Self Service Interface Code of Connection; SMKI Code of Connection; SMKI Repository Code of Connection; DCCKI Code of Connection; DCCKI Repository Code of Connection.
Code Performance Measures	CPM	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Command		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Commercial Product Assurance	CPA	means a Product Assurance Scheme required by the SEC.
Commissioned		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communication Hub Function	CHF	has the meaning given to that expression in Great Britain Companion Specification.
Communication Services		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Communications Hub	CH	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communications Hub Auxiliary Equipment	CH Auxiliary Equipment	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communications Hub Availability and Diagnostics Check	CH Availability and Diagnostics Check	means the process described in Section 5 of SEC Appendix I- CH Installation and Maintenance Support Materials.
Communications Hub Forecast	CH Forecast	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communications Hub Order	CH Order	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communications Hub Order Management System	CH OMS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communications Hub Products	CH Products	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Communications Hub Technical Specifications	CHTS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Compromise		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Confirm Validity		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Consignment		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Consumer Access Device	CAD	has the meaning given to that expression in the Great Britain Companion Specification.
Consumption Data		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Contingency Private Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Contingency Public Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Contingency Symmetric Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Core Communications Service		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
COSEM		Companion Specification for Energy Metering.
CoS Party		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
CPA Certificate		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Credit Mode		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Critical National Infrastructure	CNI	means the critical elements of national infrastructure.
Critical Service Request		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Customer Identification Number	CIN	means a number issued to Smart Meter for display on the User Interface.
Data		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Data Communications Company	DCC	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Data Protection Act		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Access Control Broker	DCC ACB	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Alert		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Key Infrastructure	DCCKI	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Major Incident		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Major Security Incident		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Scheduled		means a mode of operation in which a Service Request is to be generated and processed by the DCC on behalf of the User at regular intervals for future times as specified in the Service Request.
DCC Service Flag		means a flag used to indicate the status recorded by DCC of each MPAN or Supply Meter Point with respect to whether a Smart Metering System is Enrolled, Suspended or Withdrawn.
DCC Service Provider		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC Status File		means the file produced by DCC and transferred to each Network Party's Registration Data Provider detailing the DCC Service Flag of each MPAN or Supply Meter Point registered to that Network Party.
DCC Systems		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC User Interface		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DCC User Interface Services		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
DCC WAN Provider		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Decommissioned		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Decrypt		has the meaning given to that expression in the Great Britain Companion Specification.
Delivery Date		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Delivery Location		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Delivery Month		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Delivery Note		means, in relation to a Region, the documentation containing the information listed in Annex A of SEC Appendix H under 'Delivery Note' identified as being provided in relation to that Region.
Delivery Quantity		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device Alert		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device Certificates		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device Log		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device Model		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Device Security Credentials		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device Signing Request	DSR	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Device Type		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Digital Signature		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Digital Signed		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Disable		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Dispute		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
DLMS		means Device Language Message Specification..
DLMS User Association		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Domestic Premises		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Dual Band Communications Hub	DBCH	A communications Hub capable of forming and maintaining a Home Area Network on both 2.4GHz and Sub-GHz frequencies.
DUIS XML Schema		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Elective Communication Services		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Electricity Smart Metering Equipment	ESME	has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Eligible Subscriber		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Eligible User		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Emergency Credit		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Emergency Credit Balance		has the meaning given to that expression in the Communications Hub Technical Specifications.
Emergency Credit Limit		has the meaning given to that expression in the Communications Hub Technical Specifications.
Emergency Credit Threshold		has the meaning given to that expression in the Communications Hub Technical Specifications.
Enable		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Encrypt		has the meaning given to that expression in the Great Britain Companion Specification.
End to End Design Issues Group	EEDIS	a sub-group of the TBDG.
Energy Consumer		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Enrolment		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Enrolment Service		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Event Log		has the meaning given to that expression in the Great Britain Companion Specification.
Fast-Track Notification		means submission from a User to the DCC of an Anomaly Detection Thresholds File that is submitted with the intention of being applied in shorter timescales than standard processing timescales.
Firmware		has the meaning given to that expression in the Great Britain Companion Specification.
Firmware Image		means the code which compromises a specific version of firmware.
Firmware Version		means the active (so operational) version of Firmware on a Device.
Gaining Supplier		means the Supplier which is gaining the Energy Consumer in the event of a CoS.
Gas Proxy Function	GPF	has the meaning given to that expression in the Communications Hub Technical Specifications.
Gas Smart Metering Equipment	GSME	has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
GPF Identifier		has the meaning given to that expression in the Communications Hub Technical Specifications.
Great Britain Companion Specification	GBCS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Hand Held Terminal	HHT	A device on which Commands can be loaded
Hash		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Hand Connected Auxiliary Load Control Switch	HCALCS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Hot Shoe		a physical mount with a safe power supply connected to the mains as an input and a DC power as an output to provide power so that a Gas Smart Meter can be installed before an Electricity Smart Meter
Home Area Network	HAN	A low power radio network used for communication between devices in a premises.
Incident		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Incident Category		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Incident Management Log	IML	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Incident Parties		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Information Commissioner		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Infrastructure Key Infrastructure Certificate	IKI Certificate	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
In Home Display	IHD	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Installer		means a person acting on behalf of a Supplier to carry out installation and maintenance of a SMS (could be a Meter Asset Managers or Meter Operator acting in a user role of Registered Supplier Agent.
Interested Party		means a Party or Registration Data Provider that is or has the potential to be affected by a Problem or Incident.
InterPAN		has the meaning given to that expression in the Communications Hub Technical Specifications.
Key Activation Ceremony		means a meeting at which a Private Key or Symmetric Key is activated by the DCC and / or Key

Term	Acronym	Meaning
		Custodians, such that the Private Key or Symmetric Key may be used.
Key Agreement		has the meaning given to that expression in the Great Britain Companion Specification.
Key Custodians		means individuals nominated by Parties to activate Contingency and Recovery Private Keys
Known Error		means a fault in a component of the DCC Total System which is used for the provision of Live Services, identified by the successful diagnosis of an Incident or Problem and for which both Root Cause and a temporary workaround or a permanent solution have been identified.
Known Remote Party	KRP	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Lead Supplier		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Load Limit Period		means the length of time (in seconds) which the Active Power Import needs to continuously exceed the Load Limit Power Threshold before a load limiting event is deemed to have occurred.
Load Limit Power Threshold		means the Active Power threshold in kW above which the measurement of a Load Limit Period is commenced.
Load Limit Restoration Period		means the length of time in seconds after the Supply has been Armed following a Load Limiting Event before the Supply is Enabled by Electricity Smart Meter.
Load Switch		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Local Command Services		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Locked		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.

Term	Acronym	Meaning
Losing Supplier		means the Supplier which is losing an Energy Consumer in the event of a CoS.
Low Credit Threshold		means the threshold in Currency Units below which a low credit Alert is signalled.
Manufacture Image		means a Firmware Image a Device can apply to upgrade its Firmware alongside any manufacturer specific Data needed.
Manufacturer		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Maximum Credit Threshold		means the maximum credit which can be applied by any Add Credit Command.
Maximum Meter Balance Threshold		means the Meter Balance threshold in Currency Units above which an Add Credit Command is rejected.
Message Authentication Code	MAC	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Message Identifier		has the meaning given to that expression in the Great Britain Companion Specification.
Meter		means either an Electricity Smart Meter or a Gas Smart Meter (as the context requires).
Meter Asset Manager	MAM	has the meaning given to that expression in the Communications Hub Technical Specifications.
Meter Balance		has the meaning given to that expression in the Communications Hub Technical Specifications.
Meter Operator	MOP	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Meter Point Administrator Number	MPAN	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Meter Point Reference Number	MPRN	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Metering Point		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Minimum Service Level	MSL	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Modification Proposal		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Monthly Service Metrics		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Monthly Service Threshold		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
National Cyber Security Centre	NCSC	means UK Government national technical authority for information assurance.
Network Enhancement Plan		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Network Time		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Network Operator		means a Party that is an Electricity Distributor and / or a Gas Transporter.
Non-Critical Service Request		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Non-Device Service Request		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Non-Disablement Calendar		means a Switching Table comprising a set of rules specifying periods during which the Supply will not be Disabled due to the combined credit of the Meter Balance and Emergency Credit Balance falling below the Disablement Threshold when Smart Meter is operating in Prepayment Mode.

Term	Acronym	Meaning
Non-Domestic Premises		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
OCA Certificate		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Organisation Certificate		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Organisation Certificate Revocation List		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Organisation Compromise Notification	OCN	has the meaning given to that expression in SEC Appendix L- Annex B
Organisation Information Form		has the meaning given to that expression in SEC Appendix D, Annex A.
Originator Counter		has the meaning given to that expression in the Great Britain Companion Specification.
OTA Header		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Panel		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Parse and Correlate Software		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Party		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Party Signifier		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Payment Based Debt Recovery		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.

Term	Acronym	Meaning
Payment Debt Register		has the meaning given to that expression in the Communications Hub Technical Specifications.
Pending Private Key		has the meaning given to that expression in the Great Britain Companion Specification.
Personal Data		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Post Commissioning Obligations		means the obligations relating to Post Commissioning Information laid out in Appendix AC (Inventory Enrolment and Withdrawal Procedures).
Pre-Command		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Prepayment Meter Interface Device	PPMID	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Prepayment Mode		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Prepayment Top Up Token	PTUT	has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Prepayment Token Decimal	PPTD	has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Price		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Privacy PIN		means a number comprising of four digits used by the Energy Consumer to enable temporary access to a specified set of display items and Commands via the User Interface of the Smart Meter.
Private Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Problem		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Public Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Public-Private Key Pair		has the meaning given to that expression in the Great Britain Companion Specification.
Quarantined Communications Action File	QCA File	means a CSV file submitted by a User for the purposes of notifying the DCC of the actions to be taken by DCC in respect of quarantined communications.
Randomised Offset Limit		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
RDP Systems		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Recovery Certificate		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Recovery Private Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Registered Supplier Agent		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Registration Data		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Registration Data File		means the file or files containing Registration Data for one or more Network Parties, produced by (or on behalf of) each Network Party and transferred to the DCC detailing the Registration Data for that Network Party pursuant to Section E2 of the Code.
Registration Data Interface		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Registration Data Provider	RDP	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Registration Data Refresh File		means the Registration Data File containing Registration Data for a subset or full set of MPANs or Supply Meter Points.

Term	Acronym	Meaning
Registration Data Update File		means the Registration Data File sent periodically that records changes to Registration Data.
Release Note		means instructions provided by Manufacturers on how to deploy Firmware.
Relevant Private Key		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Response		means a communication from the Device to the DCC in response to a Command.
Response File		means a file produced whilst processing a DCC Status File. For each record in the file being processed, the Response File contains either an acknowledgement that the record has been processed successfully or in the case of a failure in processing the record, the validation errors found.
Responsible Supplier		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Return Materials Authorisation	RMA	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Root		has the meaning given to that expression in the Great Britain Companion Specification.
Root Cause Analysis		means a class of problem solving methods aimed at identifying the Root Cause of a Problem or Incident
Secure Perimeter		has the meaning given to that expression in the Great Britain Companion Specification.
Security Credentials		has the meaning given to that expression in the Great Britain Companion Specification.
Security Log		has the meaning given to that expression in the Great Britain Companion Specification.
Security Sub-Committee	SSC	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Self Service Interface	SSI	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Senior Responsible Officer	SRO	means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP.
Service Alert		means an Alert notifying Interested Parties of a current issue which may impact the provision of Services.
Service Desk		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Service Management Service Request	SMSR	means the request raised by the User to facilitate management of a Service Desk call.
Service Management Standards		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Service Request		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Service Response		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Signed Pre-Command		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SM WAN Coverage Database		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Smart Energy Code	SEC	means the document of that name, as was designated by the Secretary of State under Condition 22 (The Smart Energy Code), that is maintained for the purposes of that condition, that is subject to modification pursuant to Condition 23 (Change control for Smart Energy Code), and that may be referred to in this Licence as “the SEC”.
Smart Energy Code Administration and Secretariat	SECAS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Smart Meter		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Smart Metering Equipment Technical Specifications	SMETS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Smart Metering Implementation Programme	SMIP	means the Government led programme to implement Smart Metering in Great Britain.
Smart Metering Inventory	SMI	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Smart Metering Key Infrastructure	SMKI	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Smart Metering Systems	SMS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMI Status		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI Interface		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI PMA		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI PMA Member		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI Portal		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI Recovery Procedure		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI Registration Authority Manager		means an individual who acts on behalf of the SMKI Registration Authority to perform tasks relating to the management of the SMKI Registration Authority, as set out in the SMKI RAPP.

Term	Acronym	Meaning
SMKI Repository		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SMKI Services		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Special Day		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Special Installation Mesh Communications Hub	SIMCH	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
SRO Nomination Form		has the meaning given to that expression in SEC Appendix D, Annex A.
Statement of Service Exemption		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Successfully Executed		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Supplier		means a Party that is an Import Supplier and / or a Gas Supplier.
Supply Depletion State		means a setting to control the state of the Supply in the case of loss of power to Gas Smart Meter, being Locked or unchanged.
Supply Meter Point		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Supply State		means the state of the Supply being Enabled, Disabled or Armed.
Supply Tamper State		means a setting to control the state of the Supply in the case of Unauthorised Physical Access being detected, being Locked or unchanged.
System		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
T3 Aerial Type		means the high gain aerial type in the Central Region and the South Region further described in the Communications Hub Supporting Information and which may not be ordered by Parties but is supplied and fitted directly by DCC.
Target Initial Response Time		means the time period within which an Incident within each Category should be recorded on the Incident Management Log and assigned to a resolver
Target Response Time		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Target Service Level	TSL	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Tariff		has the meaning given to that expression in the Great Britain Companion Specification.
Tariff Block Counter Matrix		has the meaning given to that expression in the Communications Hub Technical Specifications.
Tariff Block Counter Register		has the meaning given to that expression in the Communications Hub Technical Specifications.
Tariff Switching Table		has the meaning given to that expression in the Communications Hub Technical Specifications.
Tariff Threshold Matrix		has the meaning given to that expression in the Communications Hub Technical Specifications.
Tariff TOU Price Matrix		has the meaning given to that expression in the Communications Hub Technical Specifications.
Tariff TOU Register Matrix		has the meaning given to that expression in the Communications Hub Technical Specifications.
Technical and Business Architecture Sub-Committee	TABASC	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Technical and Business Design Group	TBDG	a transitional governance group established by the SMIP.

Term	Acronym	Meaning
Technical Code Specification		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Tenant		means the occupant of property
Threshold Anomaly Detection	TAD	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Time Debt Register		has the meaning given to that expression in the Communications Hub Technical Specifications.
Time-Based Debt Recovery		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
Time Of Use	TOU	has the meaning given to that expression in the Great Britain Companion Specification.
Transform		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Transitional Change of Supplier	TCoS	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Trust Anchor Cell		has the meaning given to that expression in the Great Britain Companion Specification.
Type 1 Device		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Type 2 Device		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Unauthorised Physical Access		has the meaning given to that expression in the Great Britain Companion Specification.
Uniform Network Code	UNC	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).

Term	Acronym	Meaning
Unique Property Reference Number	UPRN	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Unique Transaction Reference Number	UTRN	has the meaning given to that expression in the Great Britain Companion Specification.
User		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
User Interface		has the meaning given to that expression in the Smart Metering Equipment Technical Specifications.
User Role		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
UTRN Check Digit		has the meaning given to that expression in the Great Britain Companion Specification.
Wide Area Network	WAN	has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
WAN Provider		means the DCC in the role of the Communications Provider.
Warning Threshold		means a number of communications within a period of time which, if exceeded, will result in the DCC notifying the User. Where both that number and the period of time are set by the User.
Working Day		has the meaning given to that expression in SEC Section A (Definitions and Interpretation).
Zigbee SE	ZSE	has the meaning given to that expression in the Great Britain Companion Specification.