Department of Energy & Climate Change

Smart Metering Implementation Programme

A Consultation on New Smart Energy Code Content (Stage 3)

16 December 2013

This document is also available from our website at www.gov.uk/decc.

General information

Purpose of this consultation:

This consultation will help inform the content of the third stage of the Smart Energy Code, which governs the end-to-end management of Smart Metering in Great Britain.

Issued: 16 December 2013

Respond by: 14 February 2014

Enquiries to:
Smart Metering Implementation Programme - Regulation
Department of Energy & Climate Change
Orchard 3, Lower Ground Floor

1 Victoria Street

London, SW1H 0ET

Telephone: 0300 068 5953
Email: smartmetering@decc.gsi.gov.uk

Territorial extent:

This consultation applies to the gas and electricity markets in Great Britain. Responsibility for energy markets in Northern Ireland lies with the Northern Ireland Executive's Department of Enterprise, Trade and Investment.

How to respond:

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

Responses to this consultation should be sent to smartmetering@decc.gsi.gov.uk no later than 14 February 2014.

Additional copies:

You may make copies of this document without seeking permission. An electronic version can be found at https://www.gov.uk/government/consultations/new-smart-energy-code-content-stage-3.

Other versions of the document in Braille, large print or audio-cassette are available on request. This includes a Welsh version. Please contact us under the above details to request alternative versions.

Confidentiality and data protection:

DECC intends to summarise all responses and place this summary on our website at https://www.gov.uk/government/consultations/new-smart-energy-code-content-stage-3. This summary will include a list of names or organisations that responded but not people's names, addresses or other contact details. In addition DECC intends to publish the individual responses on its website and you should therefore let us know if you are not content for the response or any part of it to be published. We will not publish people's personal names, addresses or other contact details. If you indicate that you do not want your response published we will not publish it automatically but it could still be subject to information requests as detailed below.

Further, information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004).

If you do not want your individual response to be published on the website, or to otherwise be treated as confidential please say so clearly in writing when you send your response to the consultation. For the purposes of considering access to information requests it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

Quality assurance:

This consultation has been carried out in accordance with the Government's Consultation Principles, which can be found here:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60937/Consultation-Principles.pdf

If you have any complaints about the consultation process (as opposed to comments about the issues which are the subject of the consultation) please address them to:

DECC Consultation Co-ordinator
3 Whitehall Place
London SW1A 2AW
Email: consultation.coordinator@decc.gsi.gov.uk

Table of Contents

1 Executive summary

1.1 A New Industry Code

1 Smart Meters are the next generation of gas and electricity meters. They will offer a range of intelligent functions and provide consumers with more accurate information, bringing an end to estimated billing. Consumers will have near-real time information on their energy consumption to help them control and manage their energy use, save money and reduce emissions.

2 On 23 September 2013, a new licensed entity, the Data and Communications Company (DCC), was established. Together with its sub-contractors, the Data Service Provider (DSP) and Communications Service Providers (CSPs), the DCC will provide a Smart Meter communications service. The DCC will offer a means by which Suppliers, Network Operators and others can communicate remotely with Smart Meters in Great Britain.

3 The Smart Energy Code (SEC) is a new industry code which has been created through, and came into force under, the DCC Licence. The SEC is a multiparty contract which sets out the terms for the provision of the DCC's Smart Meter communications service, and specifies other provisions to govern the end-to-end management of Smart Metering.

4 The DCC, Suppliers and Network Operators are required by licence to become a party to the SEC and comply with its provisions. Other bodies who wish to use the DCC's services, such as energy efficiency and energy service companies, must accede to the SEC to do so.

5 Consistent with other industry codes, the SEC is self-governed, enabling participants to raise change proposals, debate issues, and resolve disputes without the need for day-to-day regulatory intervention. It is managed by a Panel of experts drawn from SEC Parties, and is regulated by Ofgem.

1.2 The Next Stage of the Code

6 SEC content is being introduced in stages, so that it is available when the DCC and DCC Users need it. Stage 1 of the SEC (SEC1) was introduced to deal with matters that were required to support the initial operations of the DCC.

7 Stage 2 of the SEC (SEC2) addresses a number of important areas required to aid design, build and test of systems in the run up to Systems Integration Testing (SIT). The consultation on SEC2 legal drafting closed on 29 November 2013, and responses are now being analysed.

8 Stage 3 of the SEC (SEC3) addresses specific issues relating to security, and in particular, the Smart Metering Key Infrastructure (SMKI). The SMKI will provide a secure and effective means of ensuring that messages to and from Smart Metering Equipment are properly authenticated, provide integrity and, where applicable, provide non-repudiation[1] through the use of public key cryptography and certificates.

[1] a reliable audit trail to guarantee that the sender of a message cannot later deny having sent it

9 In this consultation, we set out an introduction to SMKI, and follow this with the proposed legal text to cover:

- the establishment of a Policy Management Authority under the SEC to provide overall governance of the SMKI;
- the provision of an SMKI Service by the DCC which will issue and manage Certificates for both Organisations (e.g. the DCC and DCC Users) and Smart Metering Devices;
- the approach to SMKI assurance;
- the Certificate Policies which govern the Certificates for use in relation to both Organisations and Devices;
- requirements to be placed on the DCC to provide and manage an SMKI Repository for Certificates and SMKI Documents;
- SMKI Recovery Processes;
- provisions for testing the SMKI Service and the SMKI Repository; and
- other security requirements, covering the location of system controls, and obligations on both the DCC and DCC Users relating to the secure storage of cryptographic material.

10 The SMKI arrangements proposed for SEC3 will need to be supplemented by additional provisions in a later SEC consultation, including further obligations to govern the relationship between the DCC in its role as a SMKI Service Provider and those persons holding or using Certificates, including the DCC and its sub-contractors. To assist us in developing those obligations, we are seeking views in this consultation in relation to liabilities, warranties and indemnities associated with SMKI.

11 The SEC provides for Meter Operators in the electricity sector (MOPs) and Meter Asset Managers in the gas sector (MAMs), acting as Supplier Nominated Agents, to engage directly with the DCC to obtain a limited set of services.

12 In the SEC2 consultation we indicated that we would be reviewing the arrangements applying to Supplier Nominated Agents, particularly in light of the SMKI arrangements. Views are invited in this consultation on possible options for supporting the operation of MOPs and MAMs.

13 We recently published our response to the August 2013 consultation on a detailed testing regime that will allow the DCC to demonstrate that all the DCC developed systems work prior to its operational service 'going live' (Initial Live Operations). This testing regime also includes requirements on SEC Parties to complete User Entry Process Tests, prior to taking services from the DCC.

14 This consultation sets out the proposed legal text to support this detailed testing regime. It also includes provisions for the enduring test facilities that our recent response document concluded should be provided by the DCC.

15 Finally, this consultation sets out the proposed legal text that obliges Suppliers to demonstrate the interoperability of enrolled Smart Metering Equipment with DCC systems, and provides a resolution mechanism for SMETS and CHTS compliance disputes.

2 Introduction

2.1 The Regulatory Framework for Smart Meters

16 Under the terms of their licence, Suppliers are required to provide Smart Meters to their domestic and smaller non-domestic customers across Great Britain by 2020[2]. In order to support this, we are utilising powers in the Energy Act (2008) to modify the rules set out in legislation, licence conditions and industry codes that determine how the gas and electricity markets operate.

17 In September 2013, we introduced two important components of the regulatory framework for Smart Metering:

- the award and commencement of the DCC Licence; and
- the designation of Stage 1 of the Smart Energy Code (SEC).

18 The DCC Licence was awarded to Smart DCC Ltd, a wholly owned subsidiary of Capita PLC, and introduced a new licensed entity into the energy market. In addition, CGI IT UK Limited, Arqiva Smart Metering Limited and Telefónica UK Limited have signed contracts with Smart DCC to operate a data and communications infrastructure that will link Smart Meters in homes and businesses with the business systems of Suppliers, Network Operators and energy service companies.

19 Further information on the Licence, and on the DCC commercial model, was provided in the SEC2 consultation document[3].

The Smart Energy Code

20 Simultaneously with the award of the DCC Licence in September 2013, the Government designated the first stage of the Smart Energy Code (SEC) and, as part of it, the DCC's charging methodology, both of which came into effect immediately. The SEC is the first 'dual fuel' code to be designated and apply from the outset to gas and electricity market participants.

21 At the same time the members of the first SEC Panel were confirmed, the Smart Energy Code Administrator and Secretariat (SECAS) was appointed and over 75 parties (Suppliers, Network Operators and others) acceded to the SEC.

22 Following its initial designation, the Smart Energy Code is being introduced in stages by the Secretary of State using powers under Section 88 of the Energy Act (2008). The content of each stage is prioritised according to the needs of the Smart Metering Implementation Programme (SMIP) and stakeholders.

23 Stage 1 of the Smart Energy Code (SEC1) contains the provisions necessary to support the operation of the DCC from the point at which its Licence came into force. These deal primarily with code governance, how parties to the code can propose and implement changes to it, and how the DCC calculates charges over time.

[2] Currently 2019 but as announced in May 2013, a Supplier Licence Amendment is being progressed to change to this date to 2020.
[3] https://www.gov.uk/government/consultations/new-smart-energy-code-content-stage-2

24 SEC1 provides a starting point for future content by setting out a general approach to contractual matters such as the limitations of liability, and treatment of disputes. Whilst fit for purpose at the time of designation, it is recognised that these provisions may have to be revisited to reflect the development and existence of new content.

25 In October 2013, we published a consultation on Stage 2 of the SEC[4] (SEC2). This consultation addressed a number of important areas relating to the DCC's operational service provision that are required to aid design, build and test of systems in the run up to Systems Integration Testing (SIT). Some of this content will also inform the DCC, Registration Data Provider (RDP) and DCC User Design, Build and Test phases.

26 The SEC2 consultation closed on 29 November 2013, and responses are currently being analysed.

27 This SEC Stage 3 (SEC3) consultation addresses specific issues in relation to security (in particular, the Smart Metering Key Infrastructure), the operations of Supplier Nominated Agents, Smart Meter Equipment testing, the legal obligations required to support the transitional testing of the DCC Systems, and the provision of enduring test facilities for DCC Users and others to use.

28 Taken together, the SEC2 and SEC3 consultations set out to provide key content ahead of SIT, and ensure that the bodies that need to be established through the SEC are in place when they need to be. They are expected to account for a large proportion of the outstanding content required in the SEC.

29 However further stages are planned in advance of User Integration Testing and ahead of commencement of Initial Live Operations. A full list of outstanding content anticipated to be delivered in future stages is set out in Annex 2.

SEC Subsidiary Documents

30 A number of subsidiary documents will be incorporated into the SEC over time. Some will be developed by the DCC; others will be developed by the SMIP, working together with stakeholders.

31 Where the DCC is responsible for producing a document, it must consult appropriately with users on the proposed content. Part G of Condition 22 of the DCC Licence provides for the incorporation of these documents into the SEC. Examples referenced in this SEC3 consultation include:

- the SMKI SEC Document Set (see Section 3.2);
- the SMKI Interface Specification and Code of Connection (see Section 3.3); and
- the Common Test Scenarios (see Section 5.1).

32 Certain documents produced by the SMIP will also be designated under Part G of Condition 22 of the DCC Licence (via Section X5 of the SEC). Before designating, the SMIP must consult on the date for designation, and the content of the document must have been subject to such consultation as the Secretary of State considers appropriate.

[4] https://www.gov.uk/government/consultations/new-smart-energy-code-content-stage-2

2.2 Content of this Consultation

Stage 3 of the SEC

33 This document sets out proposed legal text for SEC3.

34 As far as possible the consultation is structured to reflect the structure of the SEC itself. The key sections of new legal text in the SEC which are the subject of this consultation are set out in the table below, and described in Sections 3 to 6 of this document. As required, these sections also reference any minor or consequential changes to SEC1 or SEC2 drafting which have been identified in the course of SEC3 preparation.

SEC Section	Content
F: Smart Metering System Requirements	**F2**: Requirements relating to Certified Products List, CPA certification and the Deployed Products List **F3**: The disputes resolution process relating to SMETS and CHTS compliance **F4**: Equipment configuration and interoperability requirements **F5**: Requirements on the DCC relating to firmware updates on Communications Hubs
G: Security	**G1**: Proposed relevant obligations on Supplier Nominated Agents **G2**: Obligations on the DCC for the establishment of cryptographic modules and processing of cryptographic material. **G3** sets out equivalent arrangement for DCC Service Users **G3**: Provisions relating to the location of DCC User Systems which affect the electricity or gas supply to any premises **G5**: Requirements on the DCC and DCC Service Users for the management of private cryptographic material
H: DCC Services	**H1**: Updated requirements for completion of User Entry Process Tests by potential DCC Users **H2**: Provision for SNAs to be Parties to the SEC under the User Role of SNA, and changes to show responsibility of the Supplier for certain SNA activities. Minor consequential changes also to **H3**, **H8** and **M** **H14**: Requirements for enduring Testing to be provided by the DCC, on participants in testing, on liabilities during testing, and provision of an Issue Resolution Process
L: Smart Metering Key Infrastructure	**L1**: Provision of the SMKI Policy Management Authority **L2**: Provision of the SMKI Compliance Policy, and requirements for the SMKI PMA and all SMKI Participants to comply with it **L3**: Requirements for the DCC to provide the SMKI Service, for parties to become Authorised Subscribers, and which parties are entitled to become a Subscriber for SMKI certificates **L4**: Requirements on the DCC to develop and maintain the SMKI Service Interface Design Specification and Code of Connection **L5**: Requirements on the DCC to provide the SMKI Repository, the PMA's duties in relation to it, and Parties to access it **L6**: Development and maintenance of the SMKI Repository interface specification and code of connection **L7**: Requirements to complete the SMKI and Repository Entry Process in order to apply to become an Authorised Subscriber **L8**: SMKI Service performance standards and SMKI Service demand management **L9**: Obligations on the PMA and SMKI Participants in relation to SMKI Document Set, the development of the Registration Policies and Procedures document and the production and approval of the Certification Practice Statements

T: Testing During Transition	**T1**: Methodology for Device selection for testing during transition **T2**: Arrangements for Systems Integration Testing **T3**: Arrangements for Interface Testing, and provision for the switching on and concurrent provision (alongside Interface Testing) of the enduring Testing Services **T4**: Arrangements for SMKI Testing **T5**: Development of Common Test Scenarios and SMKI Test Scenarios

35 The sections of this consultation relating to each of the above topics are split into four parts:

- the first part ('Description of the Issue') sets out the policy approach which provides the basis for the proposed legal text. We reference previous consultations where appropriate;
- the second part ('Translation into Detailed Requirements') summarises how each policy approach has been translated into the proposed legal requirements to be included in SEC3 (and which themselves are the subject of this consultation);
- the third part ('Legal Text') cross-references policy positions to the appropriate legal clauses in SEC3 for ease of use; and
- the fourth part ('Consultation Questions') sets out the questions inviting a response. All sections include a general question inviting views on the proposed text for the SEC. In addition, some sections include additional questions seeking views on specific topics.

36 Annex 4 of this document sets out the legal text proposed in this consultation as it would look combined with the designated text of SEC1, and the proposed text for SEC2 (as published in the October consultation). Annex 4 also includes a copy of the proposed legal text in change-marked form to show all the insertions, deletions and movements of text for SEC3, as compared to the combined designation text of SEC1 and proposed text for SEC2.

37 The legal text in Annex 4, including all references to Smart Meters, Smart Metering Equipment, and Devices applies only to those that are SMETS2 or CHTS compliant, as relevant. Arrangements for SMETS1 meters will be the subject of a separate consultation exercise[5].

38 Every effort has been made to ensure that the explanatory text in the main body of this consultation document reflects the legal drafting included at Annex 4. However, we have sought to ensure that the explanatory text provides a clear and simplified overview of our proposals. The legal drafting should be treated as the definitive text.

39 During the course of this consultation we will engage with stakeholders to discuss the proposed text for the SEC as described in the explanatory text and set out in Annex 4.

[5] Consultation on the Regulatory Arrangements for Enrolment and Adoption of Foundation Meters - https://www.gov.uk/government/consultations/regulatory-arrangements-for-enrolment-and-adoption-of-foundation-meters

2.3 Next Steps

Aligning SEC3 and the DCC's Service Provider Contracts

40 Many of the detailed requirements for the DCC's operational service provision have been developed through the procurement exercises undertaken to appoint the DCC's Service Providers. These requirements are now reflected in their contracts with the DCC.

41 The DCC must act in accordance with the SEC as a condition of its Licence, and the DCC fulfils the delivery of many of its SEC obligations through the Service Provider contracts as appropriate. It is therefore important for the DCC that where relevant, the SEC, DCC Licence and Service Provider contracts align; any misalignment could cause the DCC to be in breach of the SEC or its Licence, and / or impose costs on DCC Users if changes to the contracts need to be made.

42 On closure of this consultation, we will analyse all responses, and may conclude that changes need to be made to proposed SEC legal text, which have consequential impacts for provisions that are already reflected in the Service Provider contracts. In this scenario, the DCC is responsible for ensuring that its Service Provider contracts remain in line with the SEC, and with its Licence obligations.

43 The DCC is required to procure additional Service Providers to support its provision of SMKI services, including the procurement of an SMKI Trusted Service Provider and the associated SMKI assurance function. The DCC is also required to provide an SMKI Repository. The SEC drafting places obligations for all these roles on the DCC as the Licensee.

44 It will be important that the services procured by the DCC align with the SEC drafting that relate to them. We will keep under review the SEC arrangements in light of progress on all the DCC's procurement activities relating to the provision of SMKI, and may bring forward consequential proposals for changes to the SEC in subsequent releases if appropriate.

Incorporating SEC3 content into the regulatory framework

45 The SMIP is currently working with stakeholders to confirm an approach to the delivery of the proposed SEC2 and SEC3 legal drafting into the regulatory framework. We will set out further details in the New Year, when the approach is confirmed.

3 Smart Metering Key Infrastructure

3.1 Introduction

46 The proposed Smart Metering Key Infrastructure (SMKI) is based on existing industry and international Public Key Infrastructure (PKI) standards, mechanisms and principles. PKI is used widely across business sectors where secure transactions are needed, including for example, internet trading, banking transactions and billing systems. In supporting existing secure business operations with their consumers, most users of the DCC's services should be familiar with PKI.

47 We have modelled our SEC SMKI arrangements on the widely used standard PKI approach to establish trusted relationships between the equipment in premises (Devices), and the DCC and DCC Users (Organisations) that communicate with that equipment. The SMKI establishes trust by:

- providing authentication that messages originate from an authorised party that is entitled to send the message;
- ensuring the integrity of the message in transit, preventing undetected interference; and
- where appropriate, providing a reliable audit trail to guarantee that the sender of a message cannot later deny having sent it (non-repudiation).

Key obligations on the DCC and SEC Panel

48 Most of the content that follows in this consultation relates to:

- the rules that apply to the DCC in providing a SMKI Service to DCC Users;
- the establishment of a SMKI Policy Management Authority (PMA) as a Sub-Committee to the SEC Panel to govern SMKI and to gain assurance of the DCC operation of SMKI services; and
- the documentation with which the DCC (and SMKI Participants) will need to comply in providing the SMKI services.

49 As such, these sections of the consultation are likely to be of particular interest to the DCC and the SEC Panel.

Key obligations on DCC Users

50 The parts that apply specifically to users of the DCC's services, i.e. Suppliers, Network Operators and Other Users focus on:

- the right to ask for SMKI certificates from the DCC and how to go about doing so by using the DCC's Registration Authority Policies and Procedures (RAPP);
- what level of service to expect from the DCC and the turnaround time when requesting certificates; and
- the involvement of DCC Users in testing the SMKI Service and the SMKI Repository of public key certificates.

51 We are also consulting the liabilities, indemnities and warranties that may be involved in using SMKI and on proportionate arrangements for the storage and use of cryptographic keys in line with the individual risk assessments of DCC Users. Sections G3 and G5 of the SEC cover these provisions.

52 The table below summarises the areas of interest to the different parties:

Chapter	DCC and SEC Panel	DCC Users
Section 3.2: Policy Management Authority	Section 3.2. include the establishment of a SMKI Policy Management Authority (PMA) as a Sub-Committee to the SEC Panel to govern SMKI and to gain assurance of the DCC operation of SMKI services	
Section 3.3: The SMKI Service	Section 3.3 includes the rules that apply to the DCC in providing the SMKI Service to DCC Users. It includes requirements in relation to the SMKI Service Interface, providing a test SMKI Service and performance targets of the Service	Section 3.3 includes the rules regarding which parties are eligible to receive different types of certificate
Section 3.4: SMKI Assurance	Section 3.4 covers assurance of the SMKI Service – which includes requirements on DCC to procure an independent assurance scheme and the role of PMA and SEC Panel in dealing with material breaches	Section 3.4 also covers requirements on SMKI Participants to comply with the Compliance Policy, which may involve cooperating with *ad hoc* assurance assessments
Section 3.5: Certificate Policies	Section 3.5 introduces the Certificate Policies which the DCC will need to comply with when providing the SMKI Service. It also includes requirements on the DCC to produce Certificate Practice Statements and Registration Authority Policies and Procedures	The Certificate Policies will also be of interest to DCC Users as they set out the process the DCC has to follow when issuing certificates
Section 3.6: Using the SMKI Service	Section 3.6 covers a discussion on the proposed approach to liabilities, warranties and indemnities between the DCC and parties using the SMKI Service or relying on certificates. It is therefore of interest to all parties.	
Section 3.7: Providing the SMKI Repository	Section 3.7 includes the requirement on DCC to provide the SMKI Repository – including requirements related to the SMKI Repository Interface, providing a test repository and performance targets;	Section 3.7 also includes information on DCC User access to the SMKI Repository
Section 3.8: SMKI Recovery Processes	Section 3.8 includes information on the DCC producing and complying with a Recovery Process	Any DCC Users needing to recover private keys will also have to participate in the Recovery Process
Section 3.9: SMKI Service and SMKI Repository Testing	Section 3.9 includes requirements on DCC to test the SMKI Service and SMKI Repository	Section 3.9 also includes questions around when the SMKI Service and Repository needs to be tested and whether DCC Users need to be obliged to participate in testing
Section 3.10: Other Security Requirements	Section 3.10 sets out requirements in respect of processing cryptographic material	Section 3.10 sets out requirements in respect of processing of cryptographic material and restriction of certain components of DCC User Systems

53 Separate SMKI arrangements apply to:

- Devices, specifically Gas Smart Meters, Electricity Smart Meters, Communication Hubs (which comprise Communication Hub Functions and Gas Proxy Functions), Pre-Payment Metering Interface Devices (PPMID) and HAN Controlled Auxiliary Load Control Switches (HCALCS); and
- Organisations, such as the DCC, Suppliers, Network Operators and other users of the DCC's Smart Meter communications service.

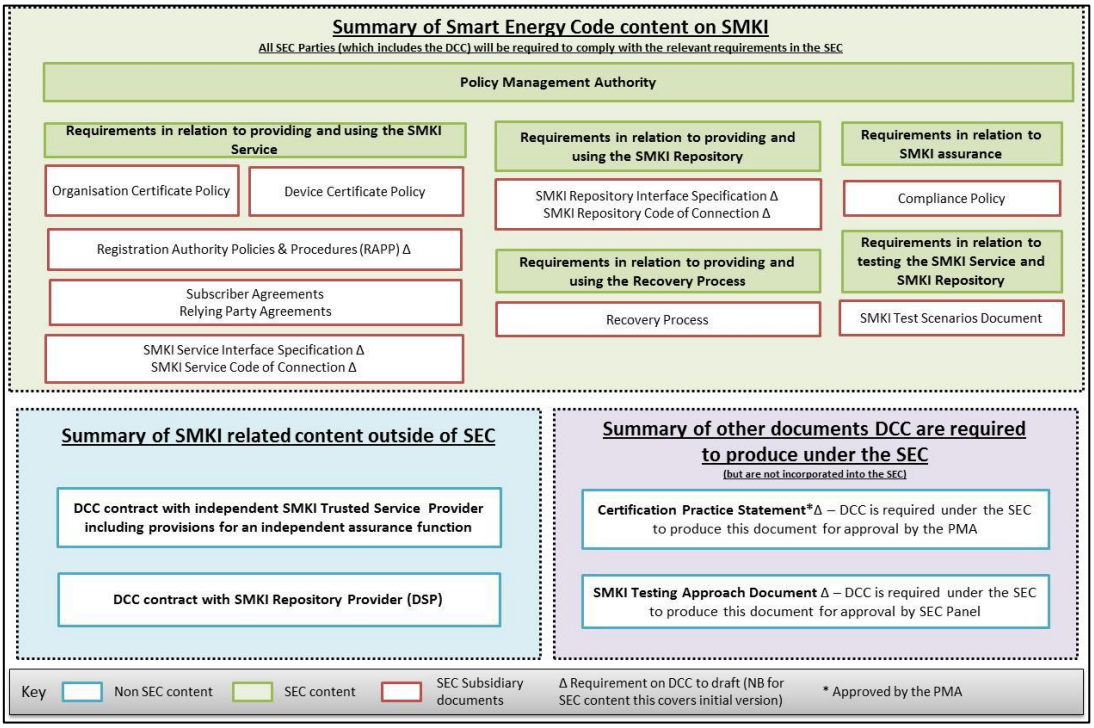
54 The SMKI effectively 'binds' the identity of Devices and Organisations to (public) cryptographic keys contained within SMKI Certificates, thereby allowing these to be trusted. The cryptographic algorithms in use across the SMKI will be detailed in the GB Companion Specification (which will form part of the SEC), and the Certificate Policies.

Translation into the Regulatory Framework

55 To ensure the delivery of a secure and effective SMKI, the following measures will be incorporated into the regulatory framework and are included in this consultation:

- strong governance arrangements through an SMKI Policy Management Authority (PMA) as a Sub-Committee to the SEC Panel (see Section 3.2), which will also oversee assurance of compliance with SMKI obligations in the SEC (see Section 3.4);
- requirements on the DCC to provide the SMKI Service – see Section 3.3;
- establishment of Certificate Policies – see Section 3.5;
- requirements in relation to those using the SMKI Service (including DCC Users) – see Section 3.6;
- requirements on the DCC to provide the SMKI Repository – see Section 3.7;
- requirements for SMKI Recovery Processes in the exceptional event that these may be needed – see Section 3.8; and
- requirements in relation to testing the SMKI Service and SMKI Repository – see Section 3.9.

56 The diagram below illustrates at a high level the proposed elements of SMKI:



57 Further consultation will be undertaken in 2014 to gather views on additional elements of SMKI including:

- the provisions relating to the Subscribers Agreement and Relying Party Agreement, which will contain provision for liabilities, warranties and indemnities (further information in Section 3.6);
- clarifying how the contractual arrangements will apply to the DCC operating in its various SMKI roles; and

- the arrangements relating to Opted Out Non-Domestic Suppliers, following on from the 'minded to' position set out in this consultation (see Section 3.6).

3.2 SMKI Policy Management Authority

Description of the Issue

58 In line with standard industry practice for Public Key Infrastructure (PKI) arrangements, an SMKI Policy Management Authority (PMA) will be established, in this case as a sub-committee of the SEC Panel, to govern the SMKI.

59 To ensure that the SMKI governance arrangements are in place as quickly as possible, we will work with the SEC Panel and SECAS to facilitate early appointment of the SMKI PMA, with the intention of having it in place when the relevant SMKI provisions in SEC3 take effect. In line with the approach taken for the SEC Panel, SMKI PMA members should act independently, not as a delegate of their organisation, and in a manner designed to meet the objectives of the SMKI PMA.

60 The specification and operation of the SMKI will be set out in the SMKI SEC Document Set. This is a portfolio of SEC Subsidiary Documents (prepared in line with procedures set out in paragraph 30 *et seq*), including the Organisation Certificate Policy, Device Certificate Policy, Registration Authority Policy and Procedures (RAPP), Subscriber Agreements, Relying Party Agreements, Compliance Policy and Recovery Process.

61 The SMKI PMA's duties will include:

- periodically reviewing the effectiveness of the SMKI SEC Document Set;
- proposing modifications to the SMKI SEC Document Set;
- providing support and advice on proposed modifications to the SMKI SEC Document Set, and other SMKI-related modifications;
- approving the Certification Practice Statements;
- ensuring compliance with the SMKI SEC Document Set and Certification Practice Statements, which includes the maintenance of a Compliance Policy, itself setting out the scope of independent assurance of the SMKI Service (see Section 3.4 for further detail on SMKI Assurance);
- supporting the SEC Panel in consideration of action following instances of material non-compliance with the SMKI SEC Document Set; and
- supporting the SEC Panel with respect to the SMKI arrangements as the Panel or other SEC sub-committees may request.

Translation into Detailed Requirements

Composition and Appointment

62 The SMKI PMA will be a Sub-Committee as defined in the SEC, and will comprise the following:

- voting Members, including the PMA Chair (casting vote only), Large Suppliers (2) and Small Suppliers (1), and a representative of each of the SEC Security, and Technical Sub-Committees; and

- non-voting Attendees, including a PKI specialist, and representatives of each of the DCC, Ofgem and DECC / the Government.

63 In addition, the SEC will allow the PMA Chair to invite additional attendees to a meeting if this is necessary to support the Committee's work. This may include, for example, a specialist Public Key Infrastructure (PKI) legal advisor, a representative of the assurance body (see Section 3.4) or a representative from Smart Meter manufacturers.

64 To seek to ensure that the PMA is in place when the SEC3 drafting relating to SMKI takes effect, we propose that the initial PMA members will be identified as follows:

- PMA Chair: in advance of the first PMA meeting the SEC Panel will invite applications for the post of PMA Chair and select a person to act for a period of three years;
- Large and Small Supplier Members: open nominations will be invited by DECC for the first appointment and by SECAS thereafter. In the event of more eligible candidates than places for any role, an election will be arranged amongst the relevant group[6]. The initial appointment period for successful candidates may be staggered to avoid the loss of expertise caused by the simultaneous retirement of a large proportion of members but the ongoing period thereafter will be for two years;
- Members of the Technical and Security Sub-Committees: for the first appointment, the SEC Panel will be asked to nominate an appropriate member from each of the Transitional SMIP Security and Technical Working Groups, in advance of the enduring Security and Technical Sub-Committees being established under the SEC. In the event that the member is not subsequently appointed to the relevant Sub-Committee, the Sub-Committee will select a new member from amongst their number and notify SECAS;
- PKI Specialist and Specialist PKI Legal Adviser: the SEC Panel (via a competition run by SECAS) will undertake the procurement of the PKI specialist and PKI legal adviser. The subsequent contracts (with SECCo) will be for a period they choose to set. The PKI Specialist will attend meetings as a non-voting member and the Specialist PKI Legal Adviser will be invited by the Chair as needed;
- DCC, Ofgem and DECC / Her Majesty's Government (HMG) Representatives: the other non-voting members will be nominated by their parent organisation; and
- additional attendees will be invited by the PMA Chair as needed.

65 The PKI Specialist Member will be deemed to be the Chair's Alternate. If the PKI Specialist is unavailable, the Chair may nominate another Alternate from among PMA Members.

66 The PMA will be subject to all SEC provisions relating to Sub-Committees[7] including, for example, procedures for establishing the frequency and conduct

[6] This is set out in Section 6.4.1 in the SEC1 consultation document - https://www.gov.uk/government/consultations/smart-energy-code

[7] As set out in Section C6 of the SEC

of meetings, and the right of Ofgem and / or DECC / HMG representatives to attend.

The PMA Role in SMKI SEC Document Set Modifications

67 In addition to the existing rights of SEC Parties to raise modifications, the PMA will have the right to propose modifications to the SMKI SEC Document Set where it considers such a change is necessary. Changes to any part of the SMKI SEC Document Set must be handled through the SEC Modifications Process.

68 The PMA will advise and support the Change Board, SEC Panel and other Sub-Committees to the SEC Panel on any SMKI SEC Document Set modification.

69 The PMA will keep under review the effectiveness of the SMKI SEC Document Set and evaluate whether it continues to contribute to meeting the SEC objectives.

Emergency Powers of the PMA

70 The PMA needs to be able to apply certain processes in the event of an emergency. When the PMA reasonably considers that an immediate threat or compromise to the security or integrity of the SMKI Service has occurred or is likely to occur, it can require the suspension of some or all of the DCC's SMKI Service, or instruct the DCC to suspend the rights of an SMKI Participant to use all or part of the DCC Services. It is important to note that this could include the suspension of any or all User Gateway services for a DCC User and that this power is subject to the normal appeal rights to Ofgem under the SEC but retrospectively.

71 The PMA can also require that the DCC place certificates on the Certificate Revocation List, following the process set out in the Organisation Certificate Policy.

Legal Text

Summary of new SEC Provisions	
Changes to Section L	L1.1 and L1.2 establish the SMKI PMA and subject it to the general provisions relating to Sub-Committees set out in Section C6 L1.3 to L1.9 cover PMA membership, including composition, role of the Chair and other Members, and the appointment process for each L1.10 to L1.14 set out the proceedings of the PMA, including requirements for a quorum and provisions for the attendance of invitees. L1.15 to L1.17 confirm the role of the PMA, including their role in modifications L.5.7 to L5.12 set out the PMA's duties in relation to the SMKI Repository L9.1 to L9.4 set out obligations on the PMA in relation to SMKI Document Set

Consultation Questions

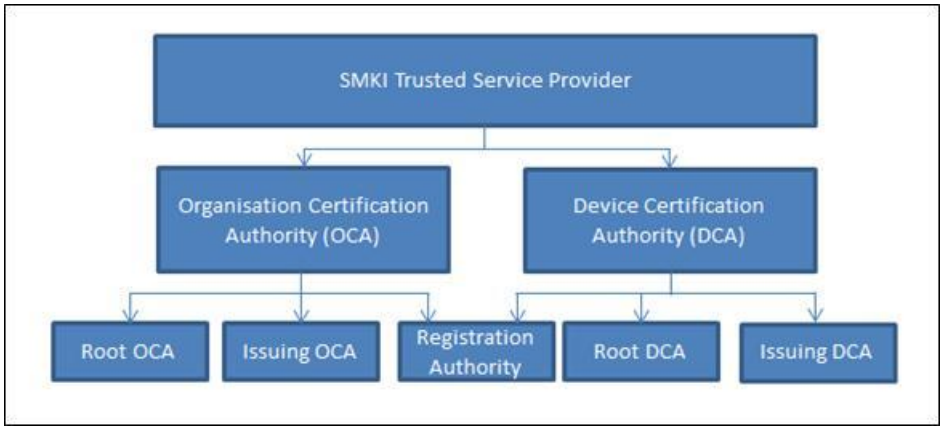
SMKI Policy Management Authority	
Q1	Do you agree with our proposed approach and text for the SEC with respect to the Policy Management Authority? Please provide a rationale for your views.
Q2	Do you agree with our proposed approach to securing the timely appointment of PMA members? Please provide a rationale for your views.

3.3 The SMKI Service

Description of the Issue

72 A central SMKI Service is needed to ensure the consistent, secure and effective operation of SMKI across all the participants. Under the SEC, the DCC will be required to provide an SMKI Service for both Organisations and Devices. Schedule 5 of the DCC Licence already includes a high level obligation for the DCC to provide the SMKI Service, and we have engaged with the DCC to provide information to help initiate the procurement of a third party SMKI Trusted Service Provider.

73 The requirements for the SMKI Service have been aligned with industry best practice for operating a Public Key Infrastructure. The diagram below describes the expected constituent elements of the DCC operating as the SMKI Trusted Service Provider:



74 The Organisation SMKI will be required to have an Organisation Certification Authority (OCA) which will consist of:

- an Organisation Root Authority - the ultimate source of 'trust' within the Organisation SMKI. The Organisation Root Authority holds its own private key and associated systems offline (to minimise the risks of compromise) and signs its own Certificate. It also issues the Certificates of Issuing OCAs;
- an Issuing OCA - the body responsible for issuing Certificates to Organisations who request them; and

- a Registration Authority – the body responsible for verifying the authenticity of those requesting Certificates and for carrying out activities on behalf of Issuing OCAs. The Registration Authority processes will also be applied to the Root and Issuing Authorities themselves, as well as to the DCC and DCC Users when they are seeking Organisation Certificates.

75 A parallel arrangement to the OCA will also be in place for the Device SMKI but, although they may share the same Registration Authority, other aspects of the Device Certification Authority (DCA) will always be kept entirely separate to the Organisation SMKI. The DCA should consist of:

- a Device Root Authority - the ultimate source of 'trust'. The Device Root Authority holds its own private key and signs its own Certificate. It also issues the Certificates of Issuing DCAs;
- an Issuing DCA - the body responsible for issuing Certificates in accordance with the Device Certificate Policy; and
- a Registration Authority – the body responsible for verifying the authenticity of those requesting Certificates and for carrying out activities on behalf of Issuing DCAs.

76 In time for the start of SIT, the DCC is required to provide a SMKI Test Service for issuing 'test' certificates and a SMKI Test Repository for storing these test certificates (see Section 3.7).

77 In addition, the DCC will make Certificates and relevant SMKI documents available to SEC Parties through an SMKI Repository also provided by the DCC under the SEC. This will be operated in parallel with, but be separate from, the SMKI Service. Further information is provided in Section 3.7.

78 The DCC's SMKI Service will be subject to assurance, as described in Section 3.4, and also have obligations in relation to testing, as described in Section 3.9.

Translation into Detailed Requirements

79 As part of its SEC obligations, the DCC will provide an SMKI Service, in line with the SMKI SEC Document Set.

80 The legal text describes parties eligible to apply for an Organisation Certificate or a Device Certificate, as summarised in the table below:

	Organisation Certificates	OCA Certificates	Device Certificates	DCA Certificates
Subscriber	SEC Parties only i.e. DCC or DCC Users (excluding SECCo)	DCC	For Devices with any status: • Gas Supplier: Gas Smart Meter and Type 1 Devices • Electricity Supplier: Electricity Smart Meter and Type 1 Devices • DCC: Communications Hub Function or Gas Proxy Function For Smart Meters only, any SEC Party so long as the Smart Meter is not either 'commissioned' or 'installed not commissioned'	DCC

81 Provisions governing the relationship between the DCC as provider of the SMKI service, parties receiving Certificates (SMKI Subscribers), and those relying upon Certificates (SMKI Relying Parties) will be incorporated as part of SEC4.

82 The DCC will propose a draft of a SEC subsidiary document which provides a technical specification for the SMKI Service Interface, and a Code of Connection which will be different and separate to the DCC User Gateway Interface. This document will be incorporated into the SEC in line with the provisions set out at paragraph 30 *et seq*.

83 The SMKI Interface specification will be made available to DCC Users, and will be the means by which SEC Parties will be able to communicate over the SMKI Service Interface. It will include a description of how the mutual authentication and protection of communications will operate.

84 The DCC will be required to provide an SMKI Test Service for issuing test Device Certificates and Organisation Certificates for use in test environments only ('test certificates'). The SMKI Test Service should never be able to issue or use live certificates and live certificates should not be used for test purposes.

85 The DCC will need to provide this test service on an enduring basis, in parallel to the live SMKI Service and SMKI Repository, to support the enduring testing activities set out in H14 of the SEC, and also to support parties to undertake equipment testing in their own test environments.

86 To ensure that they are never used for live operations, the SMKI Test Service must only issue 'test' certificates which must:

- indicate that they are for testing purposes only; and
- emulate live certificates but must not be capable of being used for live operations.

87 Section L of the SEC explains the availability and performance targets for the SMKI Service where these differ from those already described at Section H. Requests for single Organisation or Device Certificates must be processed within thirty seconds, whilst Batched Device Certificate requests (which are requests for more than one but less than 50,000 Device Certificate Requests in one communication) must be dealt with by 07:00 the following morning, when made between the hours of 07:00 and 19:00.

88 Where a Batched Certificate Signing Request is not made during these hours, it must be dealt with within 24 hours.

89 When fully operational, the SMKI will be supporting over 100 million Device Certificates but only a few hundred Organisation Certificates. To enable the DCC to manage the demand for Device Certificates, the SEC requires potential subscribers for SMKI Device certificates to provide, in December, March, June and September, a forecast of the number of Device certificate requests that the subscriber expects to send in each of the six months following the end of the month in which such forecast is provided. The intention here is to allow the DCC sufficient time to ensure it has the appropriate capacity to handle demand for certificates, whilst minimising the impact on DCC Users by mimicking the demand forecast process for User Gateway Services.

90 However, when the certificate is being requested by a non-licensee, this proposed obligation will only take effect from the point at which they become a

SEC Party, which may only be a short time in advance of ordering Device certificates.

Legal Text

Summary of new SEC Provisions	
Changes to Section A	The definition of Services is extended to SMKI Services. A number of other new definitions are included
Changes to Section H	H4 is amended to ensure that Service Requests must not be processed where the private key corresponds to a test certificate H14.12 set out requirements to provide a SMKI Test Service for issuing test certificates H14.23 to H14.31 set out entry process tests for Parties seeking to become Authorised Subscribers and / or access the SMKI Repository
Changes to Section L	L3.1 to L3.5 require the DCC to provide the SMKI Service and for parties to become Authorised Subscribers L3.6 to L3.10 set out which parties are entitled to become a Subscriber for SMKI certificates L3.11 requires the DCC to establish and lodge in the Repository Organisation Certificates required to facilitate installation of Devices that are capable of being commissioned L4.1 to L4.7 require the DCC to develop and maintain the SMKI Service Interface Design Specification and Code of Connection L7.1 to L7.10 set out requirements to complete the SMKI and Repository Entry Process in order to apply to become an Authorised Subscriber L8.1 to L8.3 and L8.6 set out SMKI Service performance standards L8.7 to L8.11 cover SMKI Service demand management, including requirements to submit forecasts
Changes to Section M	M8 is amended in relation to expulsion, to add subscribing for a Certificate or accessing the Repository within the first six months of becoming a SEC party

Consultation Questions

The SMKI Service	
Q3	Do you agree with our proposed approach and text for the SEC with respect to provision of the SMKI Service? Please provide a rationale for your views.

3.4 SMKI Assurance

Description of the Issue

91 The overarching SMKI policy that defines how the DCC and DCC Users must operate the SMKI is described in the Device Certificate Policy (for equipment in the home) and in the Organisation Certificate Policy (for the DCC and DCC User organisations who are Subscribers). The Certification Practice Statement (CPS) is the statement by the DCC to the PMA to confirm how the DCC will apply the two Certificate Policies in practice, and how the DCC will meet its obligations under the two Certificate Policies. These documents are described further in Section 3.5.

92 Given the importance of the SMKI as a security control, the SEC Panel, on behalf of SEC Parties, needs assurance that the SMKI Service is being operated in accordance within the SMKI SEC Document Set and also in line with the Certification Practice Statement (CPS). The DCC, acting in its roles as the SMKI Service Provider and SMKI Repository Provider, will be required to comply with the SMKI Compliance Policy, which may also include some *ad hoc* requirements for Subscribers.

93 The purpose of the SMKI Compliance Policy is to set out:

- the assurance scheme and its operation;
- what the DCC (acting in its role as SMKI Service Provider and SMKI Repository Provider) must do to comply;
- any compliance rules for Subscribers; and
- how the PMA will monitor and enforce that compliance.

94 Following dialogue with stakeholders, including the Security Technical Expert Group (STEG)[8], we understand that individual SEC Parties recognise they are dependent on the compliance of the DCC and other SEC Parties with the SMKI SEC Document Set and, with respect to the DCC specifically, the CPS (see Section 3.5) to maintain their own security.

95 This requirement for confirmation of compliance has led to the requirement to procure an independent assurance scheme against which the DCC's SMKI Service (and elements of the SMKI Repository Service) can be assessed, and the need for such an assessment prior to the SMKI Service issuing certificates for use in the live environment. Therefore these key elements will be written into the first version of the Compliance Policy, which will form part of the SEC.

96 Once appointed, the PMA will review and consider the need for any SEC modifications to the first version of the Compliance Policy, to satisfy itself that it is complete, and meets its requirements for compliance with the SMKI policy requirements. The scope of revisions that we consider the PMA might deem appropriate is set out in Annex 3.

97 The PMA will also play a role in considering whether there has been a material breach of the SEC with respect to the SMKI SEC Document Set and CPS, whether as a result of an assurance assessment or otherwise. It will advise the

[8] The Security Technical Expert Group (STEG) is an industry body of security experts that has advised DECC on security matters from 2010 to 2013

SEC Panel accordingly, and review any remedial action plan that the SEC Panel has required a SEC Party to produce, to confirm that it will meet the SEC requirements.

98 The systems used by the DCC in carrying out its SMKI roles are included within the scope of systems covered by Section G (i.e. those to which security obligations apply). Additional, and sometimes overlapping, security obligations also apply in relation to the SMKI systems defined by the Certificate Policies which are also subject to SMKI governance by the PMA. We expect the parties to work together, where these may be satisfied by a single demonstration of compliance.

Translation into Detailed Requirements

99 As part of their SEC obligations, the DCC and DCC Users as Subscribers must comply with the relevant sections of the Compliance Policy.

100 The DCC and Subscribers will be required to co-operate in all assurance assessments, including the provision of data / information reasonably requested and allowing reasonable access to premises and staff.

101 The proposed legal drafting for the Compliance Policy can be found at Appendix C to Schedule L2 of the SEC (see Annex 4).

102 As a subsidiary document under the SEC, any changes to the Compliance Policy will be subject to the SEC modification process, with input from the PMA (see Section 3.2).

First Version of the Compliance Policy

103 The first version of the Compliance Policy sets out the need for the DCC to procure an independent assurance scheme, the characteristics of that independent assurance scheme (and its associated Assessors), and the requirement for a pre-operational assessment.

104 The body that provides the SMKI assurance scheme and also the UKAS–accredited Assessor must all be independent of the DCC, and any of its Service Providers who provide Relevant Service capabilities to the DCC that would be the subject of such assurance (but this does not include, for example, corporate independent assurance functions). The assurance scheme provider must:

- be recognised and used by the UK Government to provide assurance of electronic trust services;
- be recognised as an accreditation scheme consistent with Article 3(2) of the European Directive 1999/93/EC;
- require all scheme assessors to be UKAS certified; and
- be based on ISO27001.

105 The first assurance assessment of DCC compliance with the Certificate Policies will be carried out in advance of the SMKI Service issuing certificates for use in live environments (see Section 5.1), and continued as appropriate on an on-going basis in accordance with the requirements of the Compliance Policy. The Assessor will be required to produce a report identifying any potential non-compliance, which must be made available to the PMA.

First full Compliance Policy

106 The first full Compliance Policy will be developed by the PMA to consider the inclusion of:

- further detail on the independent assessment of the DCC's SMKI service including e.g. the frequency and scope of assessments;
- requirements with respect to the DCC's internal audits of its SMKI Service;
- the approach to the PMA's *ad hoc* assessment of other SMKI Participants;
- the extent to which the SMKI Repository Service will be subject to Assurance; and
- the PMA's approach to non-compliance.

107 An expected scope of the first full Compliance Policy is set out in Annex 3.

108 The PMA will play an important role in dealing with non-compliance and potential non-compliance with the SMKI SEC Document Set and CPS. The PMA will consider whether an event of non-compliance (whether by the DCC or Subscribers) with respect to the SMKI SEC Document Set and CPS has occurred. The PMA will inform the SEC Panel if it considers a material event of non-compliance has occurred.

109 Following the receipt of such a report, the SEC Panel will consider what sanctions are appropriate. Where the SEC Panel has required that an SMKI Participant produces a remediation plan, the PMA will advise the SEC Panel as to whether that plan meets the SMKI requirements (insofar as it applies to SMKI compliance).

Legal Text

Summary of new SEC Provisions	
Changes to Section L	L2.1 and L2.2 require the SMKI PMA, and all SMKI Participants, to comply with the SMKI Compliance Policy L2.3 and L2.4 place a duty on SMKI Participants to co-operate in assessments by the PMA (or any person acting on its behalf) L2.5 to L2.13 set out procedures in the event of an SMKI Participant's material breach of the Compliance Policy, including investigation by the PMA, and a need to develop a remediation plan L2.14 to L2.16 provide for emergency suspension of Services relying on SMKI by the PMA, where it believes there is a reasonable threat to the DCC or DCC User Systems
Appendix C	sets out the first version of the SMKI Compliance Policy

Consultation Questions

SMKI Assurance	
Q4	Do you agree with our proposed approach and text for the SEC with respect to SMKI Assurance? Please provide a rationale for your views.

3.5 Certificate Policies

Description of the Issue

110 As described in Sections 3.1 and 3.3, the SMKI Service will have two key elements:

- a Device SMKI to support the issuing of Device Certificates; and
- an Organisation SMKI to support the issuing of Certificates to organisations including the DCC, Suppliers, Network Operators and other SEC Parties.

111 Two Certificate Policies will set out further details of each part of SMKI:

- a Device Certificate Policy; and
- an Organisation Certificate Policy.

112 The DCC will be required to provide an SMKI Service which issues Certificates in accordance with the Device Certificate Policy and the Organisation Certificate Policy. The Certificate Policies will form part of the SMKI SEC Document Set and so will be subject to oversight by the SMKI PMA (see Section 3.2), and will be stored on the SMKI Repository (see Section 3.7).

113 In line with standard PKI best practice, the DCC will be required to produce:

- a Certification Practice Statement, outlining how the SMKI Service will meet the requirements set out in the relevant Certificate Policies;
- Registration Authority Policies and Procedures (RAPP), providing more detail on the specific processes and procedures for SMKI participants to follow, for example, on how to prove their authenticity and to request Certificates.

Translation into Detailed Requirements

Device Certificate Policy

114 Annex 4 provides a draft Device Certificate Policy (DCP). The DCP defines how the DCC must operate in its role of Device Certification Authority (DCA). It defines specific obligations on the DCC in relation to issuing the different hierarchies of Device Certificates and DCA Certificates.

115 The DCA must only issue Device Certificates for the purposes of creating, sending, receiving and processing communications to and from Devices in accordance with the SEC. The Certificates must follow the Certificate Profiles set out in the legal drafting of the Device Certificate Policy (DCP).

116 The DCP includes, for example, requirements on the DCA to carry out the following steps:

- complete a Subscriber Authorisation process;
- ensure the SMKI Subscriber proves possession of the Private Key associated with the Public Key to be contained within a Certificate;
- authenticate and enrol individuals who will be submitting Certificate requests on behalf of Subscribers;
- process, and issue or reject certificate signing requests;
- define the process for the SMKI Subscriber to accept the Certificate; and
- lodge the Certificates for publication with the SMKI Repository (see Section 3.7).

117 Further information on each step will be provided in the RAPP. Section 5 of the Certificate Policies contains a range of requirements in relation to facility management and operational controls. Section 6 covers Technical Security Controls.

118 The key elements where the Device Certificate Policy differs from the Organisation Certificate Policy include:

- the DCC User who is a Subscriber applying for a Device Certificate will be responsible for warranting information in their request (i.e. that the request is for a valid Device). However, the DCA will not have to verify that all the information in the Device Certificate Request is correct;
- Device Certificates are issued for the life of the Device. Revocation of the Device Certificate is therefore not permitted, and it is not necessary to replace the Device Certificate unless the Subscriber chooses to do so for their own reasons and at their own expense;
- because Device Certificates cannot be revoked, the DCA does not provide a list of Revoked Device Certificates;
- to minimise risks of the Device Issuing Authority having its private keys lost, stolen, corrupted or otherwise becoming unreliable, the Device Issuing Authority is required to destroy the existing private key, and issue a new private key once they reach one of the following limitations:
    - three months after the time at which any component of the Issuing DCA first comes online / is operational (the Maximum Operational Time Period); or
    - it has issued 100,000 Device Certificates (the Maximum Issue Volume).

119 Prior to, or on reaching one of these limits, the Issuing DCA's private keying material must be verifiably destroyed. A new private key will then be established, by a re-created Device Issuing Authority.

120 The activities involved in the destruction of a private key that reaches the limits described above and the establishment of a new private key is wholly confined to the DCC, and the Device Issuing Authority. It requires no action by Subscribers, and has no impact on Subscribers or meters.

Organisation Certificate Policy

121 Annex 4 provides a draft Organisation Certificate Policy (OCP). The OCP defines how the DCC must operate in its role as the Organisation Certification Authority (OCA). It defines specific obligations on the DCC in relation to issuing the different hierarchies of Organisation Certificates and OCA Certificates.

122 The OCA is only able to issue Certificates for the purposes of creating, sending, receiving and processing communications to and from Organisations in accordance with the SEC. The Certificates must follow the Certificate Profiles set out in the Organisation Certificate Policy.

123 The OCA is required to carry out the same steps highlighted for Device Certificate Policy above (paragraph 116).

124 The key elements where the Organisation Certificate Policy differs from the Device Certificate Policy include:

- revocation of the Organisation Certificate is permitted. The OCA must revoke certificates where for various operational reasons:
    - the Subscriber's Private Key material has been lost, stolen, corrupted or has otherwise become unreliable;
    - the security of the cryptographic module holding the Private Key associated with a Certificate can no longer be relied upon; or
    - where requested by the relevant Subscriber or by the PMA.
- the OCA must produce a Certificate Revocation List (CRL) identifying revoked Organisation Certificates which should be lodged with the SMKI Repository every 12 hours or immediately following a certificate being revoked;
- the OCA must produce an Authority Revocation List (ARL) identifying revoked OCA Certificates which should be lodged with the SMKI Repository (see Section 3.7) for publication at least once every 12 months or within an hour of a certificate being revoked; and
- the OCA will be required to verify all information in relation to an organisation certificate request i.e. there will be processes to follow to determine that the organisation is who it says it is.

Certification Practice Statement and Registration Authority Policies and Procedures

127 In line with standard PKI best practice, the DCC will be required to produce:

- a Certification Practice Statement (CPS), outlining how the SMKI Service provided by the DCC will meet the requirements set out in the relevant Certificate Policies. This document will be approved by the PMA and will be a key focus for the SMKI Assurance process (see Section 3.4). Note the CPS is confidential to the DCC as SMKI Service Provider, and to the PMA because it contains details of internal SMKI Trusted Service Provider operations that are not for public disclosure. It is not published to SEC parties and is not part of the SEC; and
- Registration Authority Policies and Procedures (RAPP), providing more detail on the specific processes and procedures for SMKI participants to follow, for example, on how to prove their authenticity and to request Certificates. A draft of the RAPP will be produced by the DCC as SMKI Service Provider, in line with the procedure for SEC Subsidiary Documents set out in paragraph 30 *et seq.* Once incorporated into the SEC, it will be part of the SMKI SEC Document Set.

Legal Text

Summary of new SEC Provisions	
Changes to Section L	L9.1 to L9.2 and L9.19 set out obligations on the PMA and SMKI Participants in relation to SMKI Document Set, which is defined in L9.3 to 9.4, along with the SMKI SEC Documents L9.7 to L9.8 set out obligations in relation to the development of the Registration Policies and Procedures document L9.7 to L9.18 set out obligations on the DCC to produce, and the

	SMKI PMA to approve, the Certification Practice Statements
Appendix A	SMKI Device Certificate Policy
Appendix B	SMKI Organisation Certificate Policy

Consultation Questions

Certificate Policies	
Q5	Do you agree with our proposed approach and text for the SEC with respect to the Device Certificate Policy? Please provide a rationale for your views.
Q6	Do you agree with our proposed approach and text for the SEC with respect to the Organisation Certificate Policy? Please provide a rationale for your views.

3.6 Using the SMKI Service

Description of the Issue

125 SMETS 2 and the GB Companion Specification will contain details of the public and private key cryptography standards and specifications that will apply to Devices and to Commands sent across the end to end Smart Metering system. The SEC will contain details of the SMKI-related obligations placed on the DCC (which in turn will relate to activities carried out by the following sub-contractors to the DCC: the SMKI Service Provider; DSP and CSPs) and on DCC Users who will send and receive Service Requests.

126 The SEC will require relevant SEC parties to use the SMKI service and to abide by the relevant sections of the SMKI SEC Document Set that will include:

- provisions applying to subscribers in a Subscriber Agreement, i.e. contractual terms and conditions between the DCC (as SMKI Service Provider under the SEC) and Subscribers to SMKI Certificates; and
- provisions applying to Relying Parties in a Relying Party Agreement, i.e. the arrangements that apply to any party that relies on a SMKI Certificate.

127 Equally the DCC will need to require its Service Providers to comply with equivalent provisions, as relevant, in its contracts with them. These arrangements will be developed further as part of a future SEC consultation, but initial thinking on these matters is set out further below.

128 In particular, we are consulting now on the liabilities, warranties and indemnities that will be associated with the use of the SMKI. This will enable respondents' views to be taken into account when formulating the provisions applying to Subscribers and Relying Parties in a future SEC consultation.

129 For the purposes of this discussion, it has been assumed that all Subscribers and all Relying Parties will be SEC Parties. In the case of the DSP and CSPs, it is currently envisaged that they will be the subject of Certificates for which the DCC is the Subscriber as a SEC Party. Further detail on these arrangements,

including how such matters apply to DCC and its Service Providers will be set out in future versions of the SEC.

Opted Out Non-Domestic Suppliers

130 The proposals set out above do not address how the arrangements will apply to Opted Out Non-Domestic Suppliers. We have considered the scenario where a consumer changes from an Opted Out Non-Domestic Supplier to an Opted In Supplier and vice versa. In the first of these scenarios, the Opted In Supplier would be unable to confirm the status of the cryptographic keys on the meter unless they were SMKI Device certificates. To ensure trust, authenticity and integrity, the Opted In Supplier would need to replace the metering equipment. To minimise any disruption that this would cause for consumers and to avoid unnecessary cost, we are minded to require all SMETS 2 equipment to have SMKI Device Certificates.

131 To achieve this, it will be necessary for subscribers for these certificates to enter into arrangements with the DCC (as the DCA) to receive the Certificates.

132 In this respect, there are proposals to allow installers to become SEC Parties solely for the purposes of requesting Device Certificates or to access Organisation certificates held in the Repository. When acting in this capacity, only very limited parts of the SEC apply to them. This is discussed further in Section 4.

133 It may be appropriate to extend these arrangements to apply to those seeking Device Certificates for opted out Devices. However, it will also be necessary to establish the provisions that apply to those relying on Device Certificates for the purposes of non-SEC related Smart Metering communications, and to permit access to Device Certificates and other information held in the SMKI Repository.

134 We have held initial discussions with stakeholders who may choose to become Opted Out Non-Domestic Suppliers, to ensure that SMKI and wider security obligations are not disproportionate. These discussions are continuing, and the arrangements that will apply to this section of the energy market will be considered further in SEC drafting next year. Our aim is to avoid disruption for consumers on change of supplier between opted in and opted out suppliers, and we welcome views in this consultation on whether the ‘minded to’ position is reasonable and proportionate, or whether it should be left to the market to determine.

Liabilities, Warranties and Indemnities

135 We will consult on detailed proposals for the liability regime in a further SEC consultation next year. However, we welcome comments in this consultation on our ‘minded to’ position to help to shape the SEC drafting.

136 In general, it is intended that the existing liability regime applying under the SEC will apply between SEC Parties when participating in SMKI. In essence, parties waive their rights to claim against one another in negligence or claim for consequential losses, but face limited liabilities for physical damage (and the costs of site visits) if this arises as a consequence of their breach of the SEC. They also face potentially unlimited liabilities for breaches of confidentiality and IPR.

137 We propose that this liability framework be extended into SMKI with a limited number of amendments as follows:

- where a SEC breach leads to the need to replace Organisation Certificates on Devices, the costs of replacement of such certificates on Devices should also be included in the amounts that parties are permitted to claim. The existing SEC liability cap of £1m per incident or series of related incidents in Section M2 would apply; and
- where it is necessary to rely on the Recovery Process to replace certificates, the costs of doing so would also be included;.

138 We do not foresee the need for any special arrangements to be pursued to try to limit tortious claims (i.e. in negligence) by third parties (including consumers), although to the extent that these are made against the DCC and are successful, then the DCC may be able to claim from its Service Provider (to the extent that the DCC had a successful claim against them), or the costs would be subject to the existing revenue restriction arrangements (i.e. pass through subject to the approval of Ofgem).

139 Where a SEC breach leads to the compromise of a Device Certificate (or a DCA Certificate), then this would not result in the need to replace the Device Certificate and hence any such costs would not be included in any potential claim. If the affected party wishes to replace the Device Certificate in such circumstances, they could do so, but this would be at their own cost.

140 The information contained within a Certificate may originate either from the Subscriber or from the relevant Certification Authority. A Subscriber will be required to warrant that the information it has provided for inclusion in a Certificate is correct. As SMKI Service Provider, the DCC will provide warranties to Relying Parties that certain relevant content of the Certificate is correct.

141 Where, despite these warranties and the Certification Authority checks, the information contained within a Certificate proves to be incorrect, then a potential liability will arise in favour of the Relying Party. Subscribers would also be potentially liable if an error had arisen because of inaccurate Subscriber information. Again these liabilities will be limited in accordance with Section M2 (amended to include any costs of replacing Certificates on Devices).

142 The Certification Authority might also be liable to the Subscriber for such costs in the event that it has introduced any errors in the Certificate.

143 In a future SEC consultation, we will explain in greater detail how this will work. However, it is envisaged that a number of further limitations will apply as follows:

- liabilities will only arise in specified circumstances, i.e. where the Certificates are being used for the purposes of carrying out an activity under the SEC or for the purposes of interpreting information received from Devices in Service Responses; and
- liabilities for breaches will be capped and limited to physical damage, the costs of site visits and the costs of replacement of Organisation Certificates (including the costs of their replacement on Devices if this proves necessary).

144 Where a SEC Party acts as a Subscriber and as a Relying Party in relation to a particular Certificate (or is required to ensure a particular Certificate is held on a particular Device), they will not be eligible to claim in their capacity as a Relying Party (or otherwise) if the error had been caused by them acting in the capacity of Subscriber.

145 Whether or not these liabilities are passed on by the DCC to its third party Service Provider is a matter for the contractual arrangements between them. In general however, it is expected that SEC Parties will waive their rights to claim against the DCC Service Providers in exchange for a waiver of the Service Provider's right to claim against Users in the DCC contract, and a contractual right for the Service Provider to claim against the DCC in the circumstances described above.

146 It is also expected that the SMKI Service Provider to the DCC will face limited liabilities to DCC, where a breach of its obligations under its Service Provider contract has resulted in a SEC breach by the DCC, and which causes the DCC to be liable to one or more SEC Parties.

147 The above arrangements will need to be kept under review in light of the contractual arrangements put in place by the DCC.

148 Another issue that arises is that of confidentiality and intellectual property rights. The contractual provisions applying to Subscribers will require the Subscriber to ensure that all of the information that it submits to the Certification Authority which is to be included in the Certificate is permitted to be made available to other persons in the Certificate. It may be appropriate to require Subscribers to indemnify the DCC against any costs arising as a consequence of the Subscriber's breach of this requirement.

149 It will also be necessary in a later version of the SEC to clarify how the contractual arrangements apply to the DCC operating in its various guises. For example it is expected that the DCC will be a Subscriber for the Certificates for which the DSP and CSPs are the subject.

150 In addition it is envisaged that the DCC will act contractually as the Root and Issuing Authority for both Device and Organisation Certificates under the SEC, with these roles being actually carried out by its SMKI Service Provider. How obligations are placed on the DCC to take account of its multiple internal roles, whilst preserving the broad approach on limitation of liability described above will need to be addressed in a future iteration of the SEC.

151 It will also be necessary to understand how the above arrangements will be extended to apply to Device Certificates issued in relation to opted out Devices. Initially, we consider that the liability arrangements outlined above should be extended into the framework applying to opted out Devices. However appropriate drafting of Subscriber and Relying Party agreements will be needed to achieve this.

Translation into Detailed Requirements

152 This consultation seeks views on the principles set out above. The legal drafting on liabilities, warranties and indemnities will be the subject of a future consultation, and thus is not included in the current drafting shown in Annex 4.

Consultation Questions

Using the SMKI Service	
Q7	Do you agree with our proposed approach to parties using the SMKI service, including by Opted Out Non-Domestic Suppliers? Please give a rationale for your views.
Q8	Do you agree with our proposed approach for the SEC with respect to Liabilities, Warranties and Indemnities? Please provide a rationale for your views.

3.7 Providing the SMKI Repository

Description of the Issue

153 During the day to day operation of the SMKI, Subscribers will need to access the Certificates and a number of related SMKI documents such as the Certificate Policies, the Registration Authority Policies and Procedures and the Compliance Policy.

154 The DCC (as DSP) will therefore be required to provide a SMKI Repository – which is essentially a directory and library function for SMKI Certificates, Certificate Revocation Lists (CRLs) and key related SMKI documents. The DSP contract already includes requirements to provide this service.

155 As described in Section 3.3, the DCC will also need to provide a SMKI Test Service for issuing 'test' certificates, and a SMKI Test Repository for storing these test certificates for the start of SIT.

156 Section 3.9 provides more information on testing of the SMKI Repository.

Translation into Detailed Requirements

157 The SEC will require the DCC to provide an SMKI Repository. It will also place obligations on the DCC (in its role as the SMKI Trusted Service Provider) and the SMKI PMA (via SECAS) to lodge certain information in the SMKI Repository. No other parties will be allowed to write information directly into the SMKI Repository.

158 The DCC (in its role as the SMKI Repository Provider) will then have obligations / permissions to publish relevant information, and ensure it is capable of being accessed by any SEC Party who needs to access the information for the purposes of activities under the SEC.

159 The following table sets out:

- the information to be published;
- the party responsible for lodging the information in the SMKI Repository;
- when the information should be published; and
- where the obligations to publish this information sit within the SEC.

Section of SMKI	Information to be published	Responsibility for lodging in the Repository	Timing of publication	Location of obligations
Device SMKI	All Device Certificates	DCC (in its role as SMKI Service Provider)	Promptly upon acceptance from Subscriber	Device Certificate Policy
	All DCA Certificates (Root and Issuing)	DCC (in its role as SMKI Service Provider)	Promptly upon issuing the certificate	Device Certificate Policy
	Device Certificate Policy	PMA	Promptly following SMKI Repository becoming available (or if a later date, promptly following document incorporation into the SEC). Updates should be lodged following any subsequent SEC modification	SEC
Organisation SMKI	All Organisation Certificates	DCC (in its role as SMKI Service Provider)	Promptly upon acceptance from Subscriber	Organisation Certificate Policy
	All OCA Certificates (Root and Issuing)	DCC (in its role as SMKI Service Provider)	Promptly upon issuing the certificate	Organisation Certificate Policy
	Certificate Revocation List (CRL)	DCC (in its role as SMKI Service Provider)	Every 12 hours (even if there is no change in information). Following Revocation of a certificate, the CRL should be updated within one hour.	Organisation Certificate Policy
	Authoritative Revocation List (ARL)	DCC (in its role as SMKI Service Provider)	Every 12 months or whenever an Organisation CA Certificate is Revoked	Organisation Certificate Policy
	Organisation Certificate Policy	PMA	Promptly following SMKI Repository becoming available (or if a later date, promptly following document incorporation into the SEC). Updates should be lodged following any subsequent SEC modification	SEC
Both Device and Organisation	Compliance Policy	PMA		SEC
	Registration Authority Policy and Procedures	DCC (in its role as SMKI Service Provider)		Certificate Policies
	Subscriber Agreements	PMA		SEC
	Relying Party Agreements	PMA		SEC
	Recovery Process	DCC (in its role as SMKI Trusted Service Provider)		Certificate Policies

158. The DCC will produce a technical specification for the SMKI Repository Interface and a Code of Connection. The interface specification will form part of the SEC and will be the means by which parties will be able to communicate over the SMKI Repository Interface, including a description of how the mutual authentication and protection of communications will operate.

159. The DCC will be required to provide an SMKI Test Repository for storing Test Device Certificates and Test Organisation Certificates. The DCC will need to provide this test service on an enduring basis, in parallel with the live SMKI Service and SMKI Repository, to support testing undertaken under the enduring arrangements, for example, testing with late starters, new entrants or Suppliers undertaking Device testing.

160 The SEC drafting explains the availability and performance targets for the SMKI Repository; all documents must be sent within 30 seconds of receiving a request for that document over the SMKI Repository interface.

Legal Text

Summary of new SEC Provisions	
Changes to Section A	The definition of DCC Live Systems is extended to include the SMKI Repository
Changes to Section H	H14.12 sets out requirements to provide a SMKI Repository Service for making available test certificates
Changes to Section L	L5.1 to L5.6 require the DCC to provide the SMKI Repository, and include requirements in relation to lodging documents and accessing information on the Repository L.5.7 to L5.12 set out the PMA's duties in relation to the SMKI Repository L5.13 summarises requirements on Parties accessing the SMKI Repository L6.1 to L6.7 relate to the development and maintenance of the SMKI Repository interface specification and code of connection L7.1 to L7.10 set out requirements to complete the SMKI and Repository Entry Process in order to apply to access the SMKI Repository L8.4 to L8.6 set out SMKI Repository target response times
Changes to Section M	M8 is amended in relation to expulsion to add accessing the Repository within first six months of becoming a SEC party

Consultation Questions

Providing the SMKI Repository	
Q9	Do you agree with our proposed approach and text for the SEC with respect to the SMKI Repository? Please provide a rationale for your views.

3.8 SMKI Recovery Processes

Description of the Issue

161 Under Section G5.1 of the SEC, all DCC Users are required to conduct a risk assessment (in line with the standard set out in ISO 27005). These risk assessments should enable DCC Users to calibrate and mitigate the security risks to their private cryptographic keys based on their individual circumstances.

162 In addition, we are seeking views in this consultation on the proposed obligations for the storage and operation of SMKI private cryptographic keys (Section 4). The mitigations from the risk assessments, and the security controls proposed for private cryptographic keys, should enable SMKI participants to deal with any individual, small scale SMKI security-related incidents that may occur.

163 However, in the exceptional event that large numbers of private keys become lost, stolen, corrupt or otherwise become unreliable, then a SMKI Recovery Process will provide a means of returning the SMKI operations to a secure state.

Translation into Detailed Requirements

164 The DCC is required to develop a Recovery Process as part of its SMKI Service design and to make it available for testing from the start of Systems Integration Test (SIT). Once approved by the PMA, the DCC will keep the Recovery Process under periodic review.

165 The Recovery Process is expected to include:

- the technical solution that the DCC will employ to support the provision of this service;
- the responsibilities of the DCC, SEC Parties and the PMA; and
- the procedures for regenerating any Recovery Key Pair after its use in a recovery situation.

166 Following the appointment of a SMKI Trusted Service Provider, the DCC will consult with SEC Parties on the proposed Recovery Process and present it to the SEC Panel (who may seek advice from the SMIP Working Group – the Transitional SMKI PMA Group (TPMAG) as appropriate) for approval. Once the proposed arrangements have been added to the SEC as a Subsidiary Document, the PMA will have the right to raise any necessary modifications to them. Any SEC Parties will be expected to comply with these arrangements insofar as they relate to them.

167 Some specific details about the Recovery Process will need to be confidential to the DCC and to the PMA to ensure that the security of the SMKI operations is maintained. However, the general operation of the Recovery Process, including the actions to be taken by any SMKI party that is compromised will be published on the SMKI Repository.

Legal Text

Summary of new SEC Provisions	
Changes to Section L	The Recovery Procedure is part of the SMKI Document Set and is subject to overall review by the PMA, including modifications at L1.17, and to all the assurance provisions at L2 Furthermore, the PMA is required to: • review the Recovery Procedure following its incorporation into the SEC at L1.15(d); and

	• nominate Parties to support the Recovery Procedure at L1.15(e). L9.2 requires all SMKI Participants to comply with the Recovery Procedure

Consultation Questions

SMKI Recovery Processes	
Q10	Do you agree with our proposed approach and text for the SEC with respect to SMKI Recovery Processes? Please provide a rationale for your views.

3.9 SMKI Service and SMKI Repository Testing

Description of the Issue

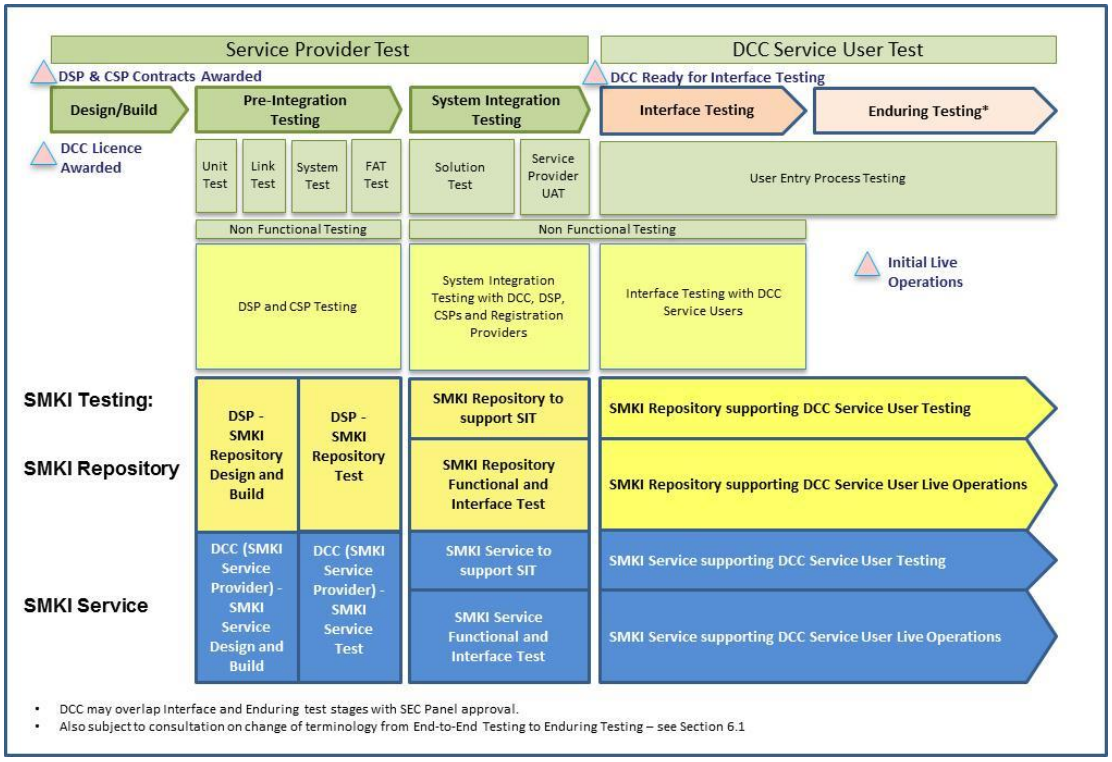
168 The SMKI Service and the SMKI Repository both need to be tested by the DCC and by DCC Users before live certificates can start to be issued at 'SMKI Service Go Live', and for these to be made available in the SMKI Repository at 'SMKI Repository Go Live'.

169 There is a lead time (which will vary between manufacturers) from the point at which Suppliers will order live Device and Organisation certificates to support an order for metering equipment, to when that metering equipment will be delivered. Following this, there will be a period (which will vary between Suppliers) when we understand that Suppliers will wish to pilot or trial that equipment using a limited quantity of Devices, and undertake their own tests to gain confidence in the security and functionality of the Device before starting a larger scale rollout.

170 In this consultation, we are seeking views from prospective DCC Users on the point at which they would wish to obtain live Device and Organisation certificates to be installed on metering equipment during the manufacturing process. This will require a fully tested SMKI Service and SMKI Repository to be available to issue and store live certificates. We are also seeking views on the extent to which DCC Users should be obliged to participate in testing the SMKI Service and SMKI Repository.

171 We are proposing to mirror, as closely as possible, the same testing approach for SMKI as for the wider testing arrangements in Section T (Systems Integration Testing (SIT) and Interface Testing - see Section 5.15.1).

172 The diagram below shows the proposed alignment of SIT, Interface Testing and Enduring Testing for the SMKI Service and SMKI Repository with the wider Smart Meters testing approach.



Timing for availability of live Certificates

173 DCC Users will wish to consider when they will first require live Device and Organisation certificates. This will require the SMKI Service and SMKI Repository to have fully completed Interface Testing involving the DCC and DCC Users, and for the DCC to have met its exit criteria and thus to be live and operational.

174 The default option is that SMKI participants will test the SMKI Service and Repository alongside the wider tests in Interface Testing (see Section 6.1).

175 However, if Suppliers wish to order equipment earlier than this, we need to consider whether it is feasible for DCC Users to test the SMKI Service and SMKI Repository, with the associated interfaces, towards the end of System Integration Testing. This will depend on the availability of a live SMKI Service and SMKI Repository at that point, in view of the short timescales for SMKI Service and SMKI Repository design, build and test.

176 The SEC drafting in Annex 3 currently has obligations that need to happen by the start of Interface Testing or such other date determined by the Secretary of State e.g. requirements in relation to approving the Certificate Practice Statements, and for the DCC to have lodged certain certificates in the Repository to enable User to request live Device and Organisation certificates. This drafting is placed in square brackets pending the views expressed by respondents.

Participation in testing the SMKI Service and SMKI Repository

177 We also welcome comments from stakeholders on the extent to which potential DCC Users should be obliged under the SEC to participate in SMKI Service and SMKI Repository testing. DCC Users will need to test their own processes to apply for, and receive, certificates before using the SMKI live service.

178 On the wider testing arrangements, we previously concluded[9] that Large Supplier Parties should be mandated through an obligation in the SEC to be ready to participate in Interface Testing. Using the same approach for SMKI, a similar obligation could be placed on Large Supplier Parties to be ready to participate in SMKI and Repository testing. We are also minded to make it a condition that at least one large Supplier must have tested the functionality of the SMKI Service and SMKI Repository, as a condition for the SMKI Service and SMKI Repository to be considered to have completed testing.

SMKI Entry Processes

179 Prior to accessing the live SMKI Service or the SMKI Repository, parties will need to go through SMKI Entry Processes to demonstrate that they can undertake the procedures necessary to access those services safely and successfully.

180 We are obliging the DCC to produce a first draft of an SMKI and Repository Scenarios document, which sets out the details of the tests that need to be performed, including entry criteria, which we will then incorporate into the SEC as set out in paragraph 30 *et sec*.

181 We are modelling the approach taken to entry processes in this area to the approach for User Entry Process Testing in relation to the DCC User Gateway and Self Service Interface.

Translation into Detailed Requirements

182 The SMKI Service and SMKI Repository testing will be defined by an SMKI and Repository Testing Objective in the SEC. The proposed objective of SMKI and Repository testing is to demonstrate that the DCC is able to comply with the relevant provisions regarding SMKI and the Repository in the SEC and to enable those SEC parties seeking to do so to complete SMKI and Repository entry process tests.

183 In order to demonstrate that the SMKI and Repository testing objective can be met, the DCC will develop a SMKI and Repository Testing Approach Document, in consultation with SEC Parties. This document will describe how the DCC will undertake testing, and the exit and entry criteria which need to be satisfied with regard to SMKI and Repository testing. This document will be submitted to the SEC Panel for approval, with various rights of appeal provided to SEC Parties throughout the process.

184 It is proposed that the DCC will additionally be required to develop an SMKI and Repository Test Scenarios document, in consultation with SEC Parties, which sets out the scenarios for testing user entry processes for applying for and accepting certificates, specific for each SMKI User role, and for accessing the Repository. This will need to be submitted to DECC and will then be introduced into the SEC, as set out in paragraph 30 *et seq*.

185 We propose that the DCC will be required to comply with the approved SMKI and Repository Testing Approach Document, and apply to the SEC Panel when it has met the relevant exit criteria for SMKI and Repository testing. The SEC

[9] https://www.gov.uk/government/consultations/smart-metering-system-and-equipment-testing

Panel will therefore determine when SMKI testing has been complete, and so when they consider that the SMKI Service and SMKI Repository are capable of starting live operations.

Legal Text

Summary of new SEC Provisions	
Changes to Section T	T4.1 to T4.8 describe the SMKI and Repository Testing Objective, the process for developing, and the required content of, the SMKI and Repository Test Approach Document, and the process by which the document is approved T4.9 to T4.19 describe how the SMKI and Repository Testing will commence, the obligation that must be followed during SMKI and Repository testing, and how it will be determined that SMKI and Repository testing has been completed T5 describes the purpose of the SMKI and Repository Test Scenarios document and the process by which will be developed and introduced into the SEC

Consultation Questions

SMKI Testing	
Q11	Do you agree with our proposed approach and text for the SEC with respect to SMKI and Repository Testing? Please provide a rationale for your views.
Q12	Where appropriate, when do you consider your organisation will first need to obtain live Device and Organisation certificates to be placed on Devices ordered from manufacturers? This will help to determine when the SMKI Service and SMKI Repository should Go Live. Please provide a rationale for your views.
Q13	Do you agree that Large Supplier Parties should be obliged under the SEC to be ready to participate in SMKI and Repository Testing? Please provide a rationale for your views.
Q14	Do you agree that it is sufficient for only one large Supplier to complete SMKI and repository testing for the SMKI Service and repository to have been proved? Please provide a rationale for your views.
Q15	Do you agree that the SMKI entry processes should be aligned with the User Entry Process Testing in relation to the DCC User Gateway and Self Service Interface? Please provide a rationale for your views.

3.10 Other Security Requirements

Description of the Issue

Location of DCC User Systems

186 We have worked with Suppliers, our security expert groups and security advisers to consider the need for any additional security requirements relating to restrictions on location. As part of this process, we considered the obligations already placed on the DCC, the proportionality of the requirements to each party's rights and capabilities, the protection of national infrastructure and compliance with EU legislation.

187 The obligations already placed on the DCC require that the operations that control the supply of energy to the premise are located in the UK. We propose to extend this obligation to those parts of DCC Users' systems that control the supply of energy. This should not affect the corporate billing systems (often referred to as 'back-end systems') or the customer support and call centre systems, but should be limited to the discrete functions that send a supply-affecting Service Request to Smart Metering Equipment at the end of a business process.

188 These discrete functions that need to be located, operated, configured, tested and maintained in the United Kingdom by User Personnel who are located in the United Kingdom (see Section G 3.19) include:

- cryptographic modules which contain private keys to sign supply affecting commands; and
- anomaly detection checks carried out to detect whether any message to the Smart Metering Equipment might have an unintended effect.

Storage of Cryptographic Material

189 We have also considered the security arrangements that need to be applied to the storage and operation of SMKI private cryptographic keys. We are mindful that the security controls need to be proportionate to the risk which will differ across SEC parties. We have therefore proposed a solution that is intended to be proportionate and not represent a barrier for new entrants to the energy market.

190 We expect that the risk assessments of larger Suppliers will lead to the need for a FIPS 140-2 Level 3 cryptographic module, such as that we propose the DCC is obliged to use. The risk assessments of small Suppliers (depending on the multiple factors relating to the volume of meters, the security of the premises from which they operate, the existing secure storage arrangements etc.) may be met by a different form of secure storage that will be less expensive, and present a proportionate cost whilst also satisfying the risk assessment.

Translation into Detailed Requirements

191 The SEC will place obligations on those DCC Users who are able to request Services that may affect the supply of electricity or gas to premises[10], to locate and operate those discrete components of their overall systems that control the

[10] Currently only Suppliers have this capability. However this capability may be extended to Network Operators in the future

supply of energy, in the UK. These components will also need to be operated by personnel located in the UK. The SEC drafting explains the precise nature of the components to which this obligation applies.

192 The DCC and DCC User information security obligations set out in the SEC drafting will extend to the implementation of policies governing the management of cryptographic material, including the use of cryptographic modules. The DCC will be specifically obliged to meet a defined international standard, but the obligation on DCC Users is to make arrangements in line with their risk assessment.

Legal Text

Summary of new SEC Provisions	
Changes to Section G	G2.30 to G2.31 set out DCC obligations in respect of establishment of cryptographic modules and processing of cryptographic material. G3.18 sets out equivalent arrangement for DCC Service Users G3.19 to G3.21 set out provisions relating to: • restrictions of certain components of User Systems and of User Personnel operating these system components; • a secure environment in which User Personnel should operate these system components; and • the processing of Service Requests that may affect the quantity of gas or electricity supplied to a premises. G5.13 and G5.21 require the DCC and DCC Service Users to develop procedures support the management of private cryptographic material

Consultation Questions

Other Security Requirements	
Q16	Do you agree with our proposed approach and text for the SEC with respect to the Location of System Controls? Please provide a rationale for your views.
Q17	Do you agree with our proposed approach and text for the SEC with respect to the Obligations for Cryptographic Material? Please provide a rationale for your views.

4 Supplier Nominated Agents

Description of the Issue

193 SEC1 provided for Supplier Nominated Agents (SNAs) to engage directly with the DCC to obtain some limited services, in particular to access information relating to individual meter points for which a Supplier has nominated them.

194 Under SEC1, SNAs were not expected to become SEC Parties, and Suppliers would be solely responsible for the actions of their agents with respect to SEC matters. This approach was consistent with the 'Supplier Hub' principle, and the range of enforcement options available to Ofgem under the Supplier's licence, covering all aspects of Supplier services (including action against a Supplier, even where those services have been contracted out to third parties).

195 The security model (including the SMKI proposals) and the DCC User Gateway proposals for Smart Metering developed under SEC2 and SEC3, require that this position is revisited.

196 In addition, the original approach envisaged that MOPs / MAMs would only be accessing information on behalf of a specific Supplier for a particular meter point. However, the SMIP has now identified a number of activities that MOPs and MAMs may need to undertake which are not easily attributable to an individual Supplier.

197 In combination, then, it is envisaged that MOPs and MAMs will require access to the following services from the DCC:

- diagnostic service requests: where a MOP / MAM reads information pertaining to a particular meter point on behalf of the registered Supplier;
- installer service requests: where a MOP / MAM needs to access DCC services at a time when their actions cannot be attributed to an individual Supplier, for example in planning an installation programme to support a number of Suppliers; and
- equipment procurement: where a MOP / MAM procures meters from a manufacturer (and at the time of procurement does not know which of its Supplier clients will become the registered Supplier for the meter), and needs to access SMKI services in order to establish the initial credentials for that Device at the point of manufacture, consistent with the supply chain assurance arrangements.

198 Any user of DCC Services must be an SMKI User in their own right, and Suppliers are not permitted to share their SMKI private credentials with any other entity, including their nominated agents. Where a Supplier wishes to subscribe for an Organisation Certificate, the subject of which is the MOP / MAM (as would be the case were the SEC1 model for SNA participation to continue), then a single Supplier might find itself subscribing for a Certificate that is used by a MOP / MAM for the purpose of providing services to a number of Suppliers (for example reading the Smart Metering Inventory or looking up the WAN matrix).

199 A MOP / MAM would need a connection to the DCC User Gateway in order to send Service Requests. Under the SEC1 model, as a non-SEC party, it would need to arrange this connection through its Supplier. However where a MOP /

MAM provides services on behalf of multiple Suppliers, then it would need multiple connections unless it could make arrangements with one Supplier that enabled the MOP / MAM to use the connection provided by that Supplier when acting for other Suppliers.

200 In view of these developments, we are now consulting again with stakeholders on the most appropriate approach to MOP/ MAM access to DCC Services. Taking into account the overall security and technical architecture, three options have been identified:

- Option 1: provision for MOP / MAM access to DCC Services through the SEC could be removed, meaning that MOPs / MAMs would have to rely on commercial arrangements with Suppliers to access information;
- Option 2: a distinction could be created in the SEC between activities which are undertaken on behalf of an individual Supplier (the diagnostic Service Requests) and activities a MOP/ MAM undertakes on its own behalf (installer Service Requests and equipment procurement). The former would be covered by the SNA arrangements included in SEC1, whilst the latter would require a MOP / MAM to accede to the SEC and participate as a user in its own User category; or
- Option 3: for all the services it is allowed to access, a MOP / MAM must accede to the SEC and participate in its own User category. With this model, in order to preserve the Supplier Hub principle where possible, the Supplier would be responsible for ensuring that when a SNA accesses 'diagnostic Services' (i.e. those that relate to an enrolled metering system for which the Supplier is responsible), the SNA only accesses them for the purpose of providing services to that Supplier.

201 Each option is likely to have different implications and issues, including:

- effects on the way that MOPs / MAMs are able to operate and support the roll-out of Smart Meters;
- operational complexities including obtaining and managing security keys and DCC access; and
- regulatory and governance issues around the operation of the Supplier hub principle and participation of different Parties in the SEC governance arrangements.

202 We intend to work with relevant stakeholders, through the consultation period, to understand the relative weight and importance of these, or other, issues in the light of the newly available security and technical architecture. This will help inform the final policy position and legal drafting.

Translation into Detailed Requirements

203 Option 1 does not require any new legal drafting, and Option 2 is already partly covered within the SEC.

204 For completeness, legal drafting is now included at Annex 4 for Option 3, allowing MOPs / MAMs to become SEC Parties in the Other User Party Category, and thus to access all the services they are permitted from the DCC.

205 The services that will need to made available to a MOP / MAM acceding to the SEC in its own right include:

- Read Device Configuration (Service Request 6.2);
- Read Event or Security Log (Service Request 6.13);
- Read Supply Status (Service Request 7.4);
- Read Inventory (Service Request 8.2);
- Read Firmware Version (Service Request 11.2);
- WAN Matrix Look-up (Service Request 12.1); and
- Device Pre-notification (Service Request 12.2).

206 In cases where a MOP / MAM procures Devices from a manufacturer (independently of a specific Supplier), the initial credentials installed on the Device will be those of the DCC, and not any specific to that MOP / MAM. When the Device is subsequently commissioned, the DCC will then replace its own credentials with those of the relevant Supplier.

207 If a MOP or MAM participates in its own category of User, it would be liable for associated Explicit Charges as a DCC User as set out in Sections J and K.

Legal Text

Summary of new SEC Provisions (for Option 3 above)	
Changes to Section G	G1.4 sets out the proposed relevant obligations on SNAs, namely G5.1, G5.2 and G5.14
Changes to Section H	H2 is updated to make SNAs Parties to the SEC under the User Role of SNA. Changes have been made to show responsibility of Supplier for certain SNA activities. The concept of Eligible Supplier Agent is removed, together with the definition of Eligible Supplier Agent from Section A H3.14, H16 and H8.15 are updated in relation to proposed services SNAs can access
Changes to Section M	References to SNAs have been removed from M2 as SNAs will now be Parties to the SEC

Consultation Questions

Supplier Nominated Agents	
Q18	Do you think that it is important that MOPs / MAMs are able to access DCC services directly? Please provide a rationale for your views.
Q19	Do you have any views on the possible options identified for MOPs / MAMs to access DCC services? Please provide a rationale for your views.
Q20	Are there other options which should be considered for MOPs/MAMs to access DCC services?

5 DCC Testing

5.1 Testing Phases

Description of the Issue

208 Testing will be undertaken prior to the DCC's Initial Live Operations, to demonstrate that it and Registration Data Providers can provide the arrangements set out in the SEC. Additionally the DCC will be required to provide test facilities for use by prospective DCC Users and others, both during the period prior to Initial Live Operations, and on an enduring basis.

209 In August 2013, we published a consultation[11] setting out our proposals for a detailed phased testing regime that would allow these objectives to be met. This consultation also sought views on SMETS2-compliant equipment testing[12], which is explored further in Section 6. However, it did not cover SMKI testing, which we are now consulting on in Section 3.9.

210 We published our consultation response on 2 December 2013[13], which confirmed our proposals for a phased testing regime.

Translation into Detailed Requirements

211 The consultation response confirmed that no further requirements are needed for Pre-Integration Testing (PIT) beyond those already in place in SEC1[14].

212 However, a new Section T of the SEC will reflect the requirements and obligations on all parties for System Integration Testing (SIT), and Interface Testing, which were set out in the consultation response, together with the procedure by which the DCC is to develop User Entry Process Common Test Scenarios[15].

213 Section H of the SEC will be amended, principally through the inclusion of a new part H14 'Testing Services'. This will set out the testing services to be made available by the DCC, the requirement for prospective DCC Users to execute User Entry Process Tests, and a process to support resolution of issues that arise during testing.

Device Selection

214 The SEC will require that during SIT, the DCC uses as many Devices (Smart Metering Equipment) as it considers appropriate in order to meet the objectives of SIT. As a minimum, the SEC will require that the selection of Smart Metering Equipment must include at least the first two sets of Smart Meters that are presented to the DCC for each fuel type, that meet the specified selection criteria.

[11] https://www.gov.uk/government/consultations/smart-metering-system-and-equipment-testing
[12] Testing of SMETS1-compliant equipment will be considered as part of the individual Foundation enrolment projects.
[13] https://www.gov.uk/government/consultations/smart-metering-system-and-equipment-testing
[14] These are the obligations on the DCC and SEC Parties to meet the transitional objectives.
[15] SEC Parties must complete User Entry Process Testing that is relevant to their DCC 'role' (e.g. Supplier, Network Operator, Other User) before they can take services from the DCC. This is done by testing against a set of Common Test Scenarios (CTS) that are applicable to each DCC User role, and which set out scenarios for testing the use of both the relevant DCC User Gateway Commands, and the Self-Service Interface.

215 The DCC must publish a methodology for the selection of Smart Metering Equipment, and this process must be open to all Device manufacturers

216 If it has successfully used Smart Metering Equipment in SIT, the DCC must use the same equipment in the same configuration during Interface Testing. The DCC will be able to amend the equipment selected, with the approval of the SEC Panel.

System Integration Testing

217 The objective of System Integration Testing (SIT) is to demonstrate that the DCC systems operate with one another and with the RDP systems, and thus that:

- the DCC is capable of complying with its SEC obligations under Sections E (Registration Data), F (Smart Metering System Requirements), G (Security), H (DCC Services), and L (SMKI); and
- Network Parties, are capable of complying with obligations under Section E (Registration Data) of the SEC, passing these onto the RDPs as appropriate.

218 The SEC will require that SIT is undertaken on a region-by-region, and an RDP-by-RDP basis, to demonstrate that each of the SIT objectives can be met for each region and each RDP system separately.

219 The DCC will be required to prepare a SIT Approach document in consultation with RDPs, and to seek SEC Panel approval of the final document. The approved document must be published on the DCC website not less than three months in advance of SIT commencement.

220 All parties must comply with their obligations set out in the SIT Approach in their conduct of SIT. The DCC may amend the SIT Approach, but only after consultation with the RDPs, and with the approval of the SEC Panel.

221 The SEC will also require the DCC to procure an independent, competent auditor to confirm its completion of SIT exit criteria, together with a supporting explanation. The DCC must publish the auditor's report on its website, as soon as reasonably practicable, on completion of SIT.

222 The DCC can only exit SIT where it and the independent auditor consider that the SIT exit criteria have been met, and must publish its SIT exit report on its website.

Interface Testing

223 Interface Testing allows the DCC (together with the DSP, CSPs and the RDPs) to prove it can interoperate with the prospective DCC Users in a test environment. It also provides the first opportunity for User Entry Process Testing (see below), allowing prospective DCC Users to test, amongst other things, that they can send and receive the messages and commands that are relevant to their chosen User Role(s).

224 The SEC requires that at least two Large Suppliers must successfully complete Interface Testing as a minimum, in each of the 'Electricity Import Supplier' and 'Gas Supplier' User Roles, before the DCC can exit Interface Testing.

225 The SEC will allow Interface Testing to commence before all elements of SIT are completed. Interface Testing for one region may therefore run concurrently with SIT for another region, to the extent it is reasonably practicable to do so. However, the DCC will not be allowed to exit Interface Testing until SIT has been completed for all three CSP regions.

226 The DCC will be required to develop an Interface Testing Test Approach document, which sets out the practical arrangements for conducting Interface Testing, and how the Interface Testing objectives will be achieved. The Approach will include the entry and exit criteria and arrangements for DCC progress reporting. It will be approved by the SEC Panel and published on the DCC website not less than six months in advance of the commencement of Interface Testing.

227 Whilst Interface Testing will be open to all prospective users, the SEC will include an obligation on Large Supplier Parties to take all reasonable steps to meet the entry criteria for the Supplier User Role in time for the planned start of Interface Testing.

228 At the time of writing, and as stated in the testing consultation response, we do not consider that there is a sufficient case for other parties to be mandated to participate from the start of Interface Testing, although we hope that they may choose to do so. Given the residual risk, we will keep this case under review, most notably in relation to Network Operators, who we expect to be ready to commence live operations from Autumn 2015.

229 To mitigate the residual risk, we propose that it be prudent to include a new provision in the SEC for a similar obligation on Network Operators to be ready to participate from the start of Interface Testing, in relation to the Network Operator User Role, but for this provision initially to be switched off, and kept under review.

230 The DCC must assess whether Large Supplier Parties (and Network Operators, if applicable) meet the Interface Testing entry criteria for the relevant User Role. All such parties must make the relevant information reasonably available to the DCC to support its assessment. Parties will have a right of appeal to Ofgem (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) if the DCC determines they have not met the entry criteria.

231 The SEC will require that the DCC (together with the DSP, CSPs and RDPs) and all prospective DCC Users who wish to undertake Interface Testing comply with their obligations set out in the Interface Testing Test Approach.

232 In order to exit Interface Testing, the DCC must be able to demonstrate achievement of the Interface Testing Objective to the SEC Panel, by reporting that all exit criteria have been met, including successful completion of the relevant tests by two Large Suppliers who are not affiliated with one another. The SEC Panel will confirm completion of Interface Testing, and advise Ofgem and all parties accordingly, giving reasons for its decision.

233 SEC Parties (including the DCC) and RDPs will have rights to appeal Panel decisions to Ofgem (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs)

relating to approval of the Interface Test Approach, and its determination that the Interface Testing Objective has been achieved.

234 The DCC cannot treat Interface Testing as complete until the SEC Panel has agreed that it is, or where Ofgem (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) has agreed in the event of a referral.

User Entry Process Testing

235 The DCC will be required to prepare a Common Test Scenarios Document. For each User Role, this document will set out the scenarios which must be completed to demonstrate that the prospective DCC User can process the Service Requests for each Service set out in the DCC User Gateway Services Schedule relevant to that User Role, and will include tests for the DCC Self-Service Interface. It will also set out the entry and exit criteria applicable to the Entry Process Tests for each User Role, forming the basis for User Entry Process Testing.

236 Each Testing Participant seeking to undertake the User Entry Process Tests must develop its own test scripts, and demonstrate how these meet the requirements of the relevant scenarios set out in the Common Test Scenarios Document.

237 As a SEC Subsidiary Document, the Common Test Scenarios Document will be prepared and incorporated into the SEC, as set out in paragraph 30 *et seq*. The DCC must submit the document to the Secretary of State at least six months before the start of Interface Testing (and therefore in line with publication of the Interface Testing Test Approach).

238 The SEC will place an obligation on the DCC to provide prospective and current DCC Users with Testing Services, in accordance with Good Industry Practice. As far as reasonably practicable, the DCC must allow parties to undertake those tests concurrently, but should it prove necessary to schedule users, it must do so in a non-discriminatory manner, scheduling Suppliers ahead of other test participants.

239 Prospective DCC Users may undertake their User Entry Process Testing either in Interface Testing, and / or in the Enduring Testing Phase, which continues after the completion of Interface Testing. SEC Parties will be required to provide the DCC with as much notice as possible of their intent to undertake User Entry Process Testing, to allow the DCC to plan the best use of its test facilities.

240 All prospective DCC Users must successfully complete the Common Test Scenarios in order to satisfy the requirements of the User Entry Process.

Enduring Testing

241 In the Consultation Response on Testing (2 December 2013), we stated that:

"We have also carefully considered the purpose of End to End Testing, which the August Consultation proposed would be a time based test stage that enables test participants to bring forward their own variants of metering equipment. We have concluded that, as the DCC is required to provide a test environment on an enduring basis, there is no material difference between End

to End Testing and Enduring Testing and that the term Enduring Testing should be used to encompass both test stages."

242 We would now like to consult on this proposed change of terminology to use the single term of 'Enduring Testing' (as is reflected in the proposed legal drafting) to encompass the previous terms of 'End-to-End Testing' and 'Enduring Testing'. In particular, we ask stakeholders to consider any possible implications of the consequential removal of the term 'End-to-End Testing'.

243 In so doing, we note that if the term 'User Integration Testing' is to continue to have currency, it will need to be redefined (as it was previously defined as being Interface Testing plus End-to-End Testing). For example, UIT could be defined in the SEC as being 'the period of Interface Testing followed by an additional sequential period of time of up to (e.g.) 12 months, as proposed by the DCC in its Interface Test Approach and agreed by the SEC Panel'.

244 We also note that the proposed change of terminology does not alter the nature or detail of the testing that testing participants must or can perform, their obligations with respect to that testing, or the testing environments which the DCC must provide.

245 The DCC will be required to provide an Enduring Testing environment to enable SEC Parties further to test the interoperability of their systems and processes with the DCC Systems across the User Gateway, beyond that required for User Entry Process testing. This facility will be open to both current and prospective DCC Users. Meter manufacturers and Suppliers will also be able to bring their Devices for the purposes of testing their interoperability with the DCC Total System.

246 As a minimum, the DCC must make available this facility from the point at which Interface Testing has been declared complete. However, and having consulted with SEC Parties, the DCC can propose to the SEC Panel that the facility be provided earlier (from or after the start of Interface Testing). It is likely that the SEC Panel will only approve the DCC's proposal to make its Enduring Testing facility available earlier, if it determines that the DCC has demonstrated that the proposal does not delay or put at risk the completion of Interface Testing.

247 If it wishes to propose the earlier provision of such a test facility, the DCC must do this prior to the anticipated start date for Interface Testing.

248 SEC Parties will be required to provide the DCC with as much notice as possible of their intended use of the Enduring Testing environment, to allow the DCC to plan for their best use.

Testing of Projected Operational Service Levels

249 For both SIT and Interface Testing, the DCC will be required to demonstrate that the objectives for both have been demonstrated to a level that is commensurate with the DCC's Projected Operational Service Levels. These operational service levels, delivered for the DCC by the DSP and CSPs, are set out in the Service Provider Contracts, as detailed spreadsheets covering a range of transaction volumes at different profiles.

250 We see merit in including these within the SEC, as a way to ensure that they are captured in the regulatory framework to the benefit of DCC Users. They will

therefore be subject to the scrutiny and rigour of a formal modification process, should in future it be proposed that they are changed for the purposes of testing.

251 As an alternative, we could include a simple requirement in the SEC for the DCC to test to the levels that have been procured in its Service Provider contracts, noting that the DCC and its Service Providers may change these without reference to DCC Users if they are not included in the SEC.

252 On balance, we are minded to include the Projected Operational Service Levels within the SEC, given the value of the certainty that this would provide, but subject to any constraints around commercial sensitivity. We would therefore welcome views from respondents on our proposed approach before reaching a conclusion.

Legal Text

Summary of new SEC Provisions	
Changes to Section H	H1 sets out updated provisions to require Users to complete the User Entry Process Tests for each User Role that they wish to perform H3 includes minor amendments to make specific reference to the newly introduced term of User Entry Process Tests H14 is a new section detailing: • the enduring Testing Services that the DCC shall provide; • how and when it shall make those Testing Services and associated facilities available; • requirements on participants in testing; • liabilities during testing; and • provision of an issue resolution process with associated rights of appeal to apply during testing
Changes to Section T	This is a new section, detailing the testing arrangements during transition T1 sets out the methodology for selecting Devices to be used by the DCC to support testing during transition T2 details the arrangements that are to apply in Systems Integration Testing in order to test the capability of the component parts of the DCC Total System to interoperate with each other, and with the systems of the RDPs T3 details the arrangements that are to apply during Interface Testing in order to test that the DCC Total System interoperates with the systems of Users. It also includes provision for the switching on and concurrent provision (alongside Interface Testing) of the enduring Testing Services, as if the relevant enduring provisions in Section H14 (Testing Services) had effect from that time T4 provides for SMKI Testing (as set out in Section 3.9 of this

	document) T5 sets out the requirements for, and process by which the DCC shall develop and document Common Test Scenarios (and SMKI Test Scenarios) for incorporation in the SEC, and against which User Entry Process Testing will be performed

Consultation Questions

Testing Phases	
Q21	Do you agree with our proposed text for the SEC with respect to Test Phasing, consistent with our decisions on testing arrangements detailed in our recent consultation response? Please provide a rationale for your views.
Q22	Do you agree that the term 'Enduring Testing' should be used to encompass both the End-to-End and Enduring Test stages in order to assist comprehension and simplicity? Would the consequential removal of the terms 'End-to-End Testing' and 'User Integration Testing' cause confusion or be undesirable, such that we should reinstate this terminology? Please provide a rationale for your views.
Q23	Do you agree with the proposed approach to include the Projected Operational Service Levels within the SEC? Please provide a rationale for your views.

5.2 Issue Resolution during Testing

Description of the Issue

253 Issues are likely to arise during testing that require resolution.

254 In this section, a Testing Participant is any Party other than the DCC participating in testing arrangements under the SEC, or a Registration Data Provider (acting on behalf of a Network Operator).

255 A Testing Issue is any situation where a party considers that the outcome of a test is not in line with expectations, but may also arise where a Party is prevented from performing the test as expected (e.g. due to a lack of connection or unavailability of environment).

256 The DCC Service Providers have been contracted to provide an issue resolution process, including the provision of a test management tool to all test participants for use in all phases of testing including Systems Integration Testing, User Integration Testing and Enduring Testing.

Translation into Detailed Requirements

257 The SEC will set out a process for the management of all issues arising during testing (the Issue Resolution Process).

258 Where a Testing Participant wishes to raise a Testing Issue it will be required to do so as soon as reasonably practicable. Prior to raising the issue, the Testing

Participant must carry out a reasonable level of due diligence to determine that the issue is not the result of something within their control.

259 The DCC must then ensure that its Service Providers provide '1st Line' support to:

- determine the severity level and priority status for the issue; and
- provide a decision on the resolution of the issue in a timescale consistent with its severity level and priority status.

260 The DCC must ensure that information on testing issues is made available to all users via publication on its website. The level of information provided for each issue should be commensurate with the priority / severity level of the issue, and its potential impacts on other Testing Participants.

261 It is possible that a Testing Participant may disagree with the findings of the Service Provider and could choose to appeal the decision. We consider that the following categories of appeal could arise:

- Category 1 appeal: where the Testing Participant wishes to appeal the priority or severity classification that has been assigned to the Testing Issue by the DCC Service Provider;
- Category 2 appeal: where the Testing Participant wishes to refer to the DCC a DCC Service Provider's performance in the resolution of a Testing Issue; or
- Category 3 appeal: where the Testing Participant wishes to appeal the decision on the appropriate resolution of the Testing Issue.

262 Where an appeal is raised with the DCC, it must consult with relevant stakeholders, determine the manner in which the issue should be resolved, provide its decision to the Testing Participant and publish this on the DCC website.

263 For Category 1 or 2 appeals, there is no further escalation route. However, the Testing Participant may escalate the DCC's decision on a Category 3 appeal, by notifying this to the DCC and the SEC Panel (in practice, SECAS) as soon as reasonably practical.

264 The SEC Panel (via SECAS) will indicate whether the SEC drafting (e.g. technical subsidiary document) that is the subject of / related to the disagreement is already in the SEC, or is draft text that has yet to be incorporated into the SEC (and will therefore be subject to transitional governance outside the SEC – see paragraph 267).

265 Where the appeal relates to text already in the SEC, the SEC Panel will provide its opinion on the appropriate resolution. In reaching its opinion, the SEC Panel may consult further with stakeholders and ensure that its decision is communicated to the Testing Participant, DCC and published on the SECAS website.

266 For the avoidance of doubt, the testing issue resolution process does not remove a Party's rights to:

- raise a SEC modification request in relation to a Testing Issue;
- raise a concern with Ofgem regarding (the DCC's) non-compliance with the SEC; or

- raise an appeal to the SEC Panel (and if unhappy with the SEC Panel's decision to Ofgem) regarding the compliance with User Entry Process Criteria, as set out in Section H 1.14 and 1.15 of the SEC.

267 Where the disagreement relates to draft text that has been published by DECC but is not yet in the SEC, SECAS will refer the matter to DECC for it to make a final determination on the Testing Issue, and whether or not any changes to the draft SEC text are required.

268 The testing issue resolution process and appeal mechanisms outlined above will be used when a Testing Participant engages in testing activities with the DCC during:

- System Integration Testing;
- Interface Testing;
- use of any of the Test Facilities set out in H14 (including User Entry Process Testing);
- SMKI Testing; and
- testing that is required to support the implementation of a SEC modification.

269 Where a Testing Participant is involved in testing DCC internal system changes, the testing issue resolution process outlined above will be used. However, where the Panel or (if the issue is appealed) Ofgem, considers that implementation of the tested systems would result in the DCC System or the User System not working in accordance with the SEC, then the Panel or Ofgem may require that the DCC does not implement the internal change until such time as this discrepancy is addressed.

Legal Text

Summary of new SEC Provisions	
Changes to Section H	A new Section H14 'Testing Services' sets out the Issue Resolution Process, which is to be used during both transitional and enduring Testing
Changes to Section T	T2 places requirements on the DCC to publish relevant information on testing issues in SIT. It also recognises that RDPs are Testing Participants and can utilise the Issue Resolution Process set out in Section H14 T3 requires the DCC to publish relevant information on testing issues in Interface Testing. It also recognises that all Parties engaged in Interface Testing are Testing Participants and can utilise the issue resolution process set out in Section H14 T4 requires the DCC to publish relevant information on testing issues in SMKI Testing. It also recognises that all Parties engaged in SMKI Testing are Testing Participants and can utilise the Issue Resolution Process set out in Section H14

Consultation Questions

Issue Resolution during Testing	
Q24	Do you agree with the need for an issue resolution process in testing? Does the proposed process meet that need? Please provide a rationale for your views.
Q25	Do you agree with our proposed text for the SEC with respect to Issue Resolution? Please provide a rationale for your views.

5.3 Liabilities in regard to Testing

270 Under SEC1, any Party non-compliant with its obligations under the SEC is liable for the specified costs of any resultant physical damage to another Party up to a cap of £1M per event.

271 These provisions will apply in the event that physical damage occurs as a result of non-compliance with, for example, a test approach document or User Entry Testing processes.

272 Physical damage may also occur in the absence of any breach or non-compliance (for example where a test goes wrong). In these circumstances, a Party will be liable for physical damage only if it can be shown that they have not undertaken their role in the testing arrangements in accordance with good industry practice.

273 Liability provisions for breach of IPR and confidentiality obligations will apply in relation to any activities involved in testing.

6 Smart Metering System Requirements

Description of the Issue

274 Many participants will play a role in the procurement and deployment of Smart Metering Equipment and Communications Hubs. It is in the interests of all parties that equipment from multiple manufacturers interoperates within consumers' premises and with the DCC's systems. This will ensure that equipment does not have to be replaced, thus avoiding additional cost and disturbance for customers.

275 Two consultations have now taken place gathering views on how to ensure that in-home equipment meets the technical requirements defined in the SMETS, CHTS and associated documents[16].

276 In our response to the SMETS 2 Consultation document (July 2013)[17], we confirmed that:

- the Suppliers' roll out licence obligations and the DCC Licence will require that Smart Metering Equipment and Communications Hubs comply with the SMETS and CHTS respectively;
- Smart Metering Equipment and Communications Hubs should be protocol (ZigBee and DLMS) and CPA certified;
- the SEC Panel should maintain a Certified Products List (CPL), with the DCC only able to enrol equipment that is on the CPL;
- the DCC should produce a Deployed Products List of all operational permutations of Devices comprising Smart Metering Systems;
- Suppliers and the DCC (for Communications Hubs) are best placed to undertake functional testing of equipment; and
- interoperability could only be fully assured when the Suppliers' Metering Equipment and the DCC's Communications Hubs are shown to operate with the DCC.

277 We also confirmed in the SMETS 2 response document that we would require time-based recertification of Devices under the CPA, noting that the time period for recertification was being discussed with industry. We have concluded that. time-based recertification should be undertaken every six years, but the controls relating to firmware upgrades that take place in the interim should be strengthened (see paragraph 293 *et seq*).

278 Six years is significantly longer than the standard two year period under the CPA, but reflects that Smart Metering Equipment is designed for greater longevity than the IT products for which CPA has been used to date. It is still expected that Smart Metering Equipment will be recertified two to three times during its lifetime. The longer recertification period will provide asset providers

[16] Different arrangements apply for SMETS 1 meters – these are defined in SMETS 1 documentation - http://www.decc.gov.uk/assets/decc/11/consultation/smart-metering-imp-prog/4965-gov-resp-cons-tech-spec-smart-meters.pdf. and covered further in the Consultation on the Regulatory Arrangements for Enrolment and Adoption of Foundation Meters - https://www.gov.uk/government/consultations/regulatory-arrangements-for-enrolment-and-adoption-of-foundation-meters

[17] https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version

and Suppliers with greater confidence in their investment, and provide more stability in the market, thus reducing the threat of meter removal.

279 The Smart Metering System and Equipment Testing consultation (August 2013)[18] included proposals to consolidate the approach to equipment certification and testing, focusing on the testing needed to ensure that equipment is interoperable with the DCC. We confirmed in our response to the testing consultation[19] that we would:

- introduce an obligation to make Suppliers and the DCC, in the case of the Communications Hub, responsible for testing the compliance of the equipment that they choose to install against SMETS2 and CHTS, and that they should retain evidence of this testing;
- make Suppliers responsible for testing the interoperability of the Smart Metering Equipment that they choose to enrol with the DCC and that they should retain evidence of this testing to be made available to the SEC Panel or Ofgem on request; and
- make the DCC responsible for testing the interoperability of the Communications Hubs they provide to Suppliers with DCC systems, and that they should retain evidence of this testing to be made available to the SEC Panel or Ofgem on request.

280 We also confirmed in Part 1 of the Government Response to the SMETS2 Consultation[20] that the SEC would include an obligation to require Suppliers to configure Smart Metering Systems to allow the DCC to provide services to other SEC parties. These requirements are included in Section F.

Translation into Detailed Requirements

In-Home Equipment Requirements

281 In addition to the existing licence requirements that Smart Metering Equipment and Communications Hubs should be compliant with the SMETS and CHTS respectively, the SEC will include the following provisions:

- A Supplier operating Smart Metering Equipment will be required to make evidence of SMETS compliance testing available to the SEC Panel and Ofgem on request;
- the DCC will be required to make evidence of CHTS compliance testing for the Communications Hubs they provide available to the SEC Panel and Ofgem on request; and
- the disputes process that may be used for SMETS and CHTS compliance disputes.

282 The SEC will require all Suppliers to ensure that any SMETS 2 equipment to be enrolled in the DCC is interoperable with DCC systems (i.e. that it will respond to GBCS-compliant commands received from the DCC). Suppliers must also ensure that enrolled equipment has been tested for interoperability, that they retain evidence of this, and that they make this evidence available to the SEC Panel and Ofgem on request. The requirement on the DCC that

[18] https://www.gov.uk/government/consultations/smart-metering-system-and-equipment-testing
[19] https://www.gov.uk/government/consultations/smart-metering-system-and-equipment-testing
[20] https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version

Communications Hubs are interoperable with DCC systems will be included in the CHTS.

283 To allow the DCC to provide the services described in the DCC User Gateway Interface Specification (DUGIS), Section F of the SEC also places two additional obligations on the Supplier responsible for an enrolled Smart Metering System, to:

- configure the meter such that the minimum functionality described in SMETS can be delivered; and
- provide the DCC with access to the Smart Metering System such that the DCC can deliver the services described in the DUGIS.

Provision of Testing Environments

284 The SEC will require the DCC to provide a test environment (including a lab that can be accessed physically and remotely) that allows Suppliers and other parties to determine the interoperability of their equipment with DCC systems (see paragraph 241 *et seq*). The test environment will not itself attract an explicit charge (including the provision of DCC support to ensure the environment is operational, and advice on its direct use).

285 All users will be responsible for defining and undertaking the tests themselves, and for meeting their own costs. However, the DCC will be required to offer additional support if requested on test definition and execution, and on resolving any issues arising over interoperability. Such support may be subject to any applicable charges set out in Section K.

286 Testing Participants will have the right to raise testing issues relating to equipment under the process described in section 5.2 above.

Certified Products List

287 The SEC will set out the assurance certificates[21] which are required for each Device Type[22] in order for it to be added to the Certified Products List (CPL). Suppliers will be required to notify the SEC Panel of changes to the certification status of any Device type on the CPL.

288 Any party may add Devices with valid certificates to the CPL. The party proposing a Device for inclusion on the CPL must also ensure that the manufacturer of the Device provides a hash of the firmware image and firmware ID generated using the SHA-256 algorithm. Hashing is an established approach to cryptographic protection, which allows the recipient independently to verify the integrity of a copy of the original data (i.e. the firmware image and ID), without having access to the original data itself.

289 The SEC Panel will be required to maintain the CPL, and to make it available both to SEC Parties and on the SEC website. The SEC Panel will also be required to notify all SEC Parties when any changes are made to the CPL.

290 The SEC will also require that the DCC creates, maintains and makes available on the SEC website a Deployed Products List of all operational permutations of

[21] ZigBee and DLMS / Cosem, and the CESG Commercial Products Assurance certificates as required in the SMETS and CHTS. Note these are unrelated to the SMKI Certificates referred to in Section 3.
[22] The Electricity Smart Meter, Gas Smart Meter, Communications Hub, PPMID, HCALCS, IHD and other Type 1 Devices.

Devices comprising Smart Metering Systems included on the Smart Metering Inventory.

291 Suppliers will be required to recertify all equipment (not simply equipment enrolled in the DCC) under the CPA scheme every six years. Equipment will be removed from the CPL on expiry of its certification.

292 The DCC will only be allowed to enrol and communicate with equipment which is on the CPL. Where the certification for any equipment expires, the DCC will cease communication with the relevant Device, and set its status to 'suspended' in the Smart Metering Inventory. Any associated Devices (including, in the case of the Communications Hub Function, Smart Meters) will also be suspended. The DCC will then be required to inform the relevant Supplier and Network Operator that it has done this, and withdraw (and notify the relevant DCC User) any future dated Service Requests and schedules.

293 Only Suppliers (for Smart Metering Equipment) and the DCC (for Communications Hubs) may add firmware and hardware versions to the CPL for Device Models which are already listed under an existing CPA certificate, where such changes satisfy the terms under which the existing CPA certificate was issued. Suppliers will be responsible for ensuring that all firmware and hardware (except Communications Hubs) is CPA compliant.

294 The Supplier will be required to provide the SEC Panel with details of the firmware or hardware versions to be added, together with details of the original certification. The Supplier will also be required to retain evidence as to why recertification was not required, and to make this available to the SEC Panel and Ofgem on request.

295 In providing details of firmware versions to be added to the CPL, the Supplier must also ensure that the manufacturer of the Device provides a hash of the firmware image and firmware ID generated using the SHA-256 algorithm.

296 Before submitting the 'Update Firmware' Service Request (or in the case of the DCC, before sending a Command to update the firmware on the Communications Hub), the Supplier (or the DCC) will be required to ensure that the firmware has been issued by the intended manufacturer (using digital signatures), and has not been modified since the manufacturer issued it (by comparing hashes).

297 When a Supplier submits an 'Update Firmware' Service Request, the DCC will be required to calculate a SHA-256 hash of the firmware image and firmware ID provided by the Supplier, and compare this with the hash listed for that firmware version ID on the CPL. The DCC will only construct the pre-command to allow the firmware update to be issued to the Device if the two hashes match.

Legal Text

Summary of new SEC Provisions	
Changes to Section F	F2.1 to F2.4, F2.6 to F2.7 and F2.11 to F2.24 describe requirements relating to the establishment and maintenance of a Certified Products List

	F2.5 and F2.8 to F2.11 describe requirements specific to CPA certification F2.15 requires that the DCC maintains a DPL F3 sets out the disputes resolution process relating to SMETS and CHTS compliance F4.1 and F4.5 describe how suppliers should configure equipment F4.2 to F4.4 describe interoperability requirements F5 describes the requirements on DCC relating to firmware updates on Communications Hubs

Consultation Questions

Smart Metering System Requirements	
Q26	Do you agree with our proposed text for the SEC with respect to Equipment Testing, and configuration of enrolled Smart Metering Systems? Please provide a rationale for your views.

7 Glossary

This section provides a glossary of the principal terms used in this document.

A complete set of definitions and interpretations of terms used in the SEC can be found in Section A of that document.

The definitions in this glossary are not intended to be legally precise, but instead to assist in understanding the consultation document.

Alert

A message from a Device or from DCC and sent to a DCC User across the User Gateway.

Authorised Subscriber

A SEC Party that has successfully followed the processes in the Registration Authority Policies and Procedures in order to be permitted to apply for Device Certificates and/or Organisation Certificates.

Certificates

A Device Certificate, DCA Certificate, Organisation Certificate or OCA Certificate issued by the SMKI Service as defined in the Device Certificate Policy or Organisation Certificate Policy.

Command

A message sent by DCC to a Device over the SMWAN (or to a DCC User over the User Gateway to be executed locally) in order to instruct the Device to carry out an action.

Commissioned

A Device status recorded in the Smart Metering Inventory. The steps a Device must go through to be Commissioned vary by Device type, but essentially this status is achieved when: the Device has been added to the Smart Metering Inventory; it has been demonstrated that DCC can communicate with it (and vice versa) over the SMWAN; and its relationship with either the Communications Hub Function or a Smart Meter has been established.

Communications Hub

A Device which complies with the requirements of CHTS and which contains two, logically separate Devices; the Communications Hub Function and the Gas Proxy Function.

Communications Hub Function

A Device forming part of each Smart Metering System which sends and receives communications to and from the DCC over the SMWAN, and to and from Devices over the HAN.

Communications Hub Technical Specifications (CHTS)

A document (which is to form part of the SEC) which sets out the minimum physical, functional, interface and data requirements that will apply to a Communications Hub.

Communications Service Provider (CSP)

Bodies awarded a contract to be a service provider of communications services to DCC as part of DCC's Relevant Services Capability. Arqiva Limited and Telefónica UK Limited have been appointed to provide these services.

Core Communication Services

The services associated with processing a specific set of Service Requests set out in the DCC User Gateway Services Schedule in a manner that involves communication via the SMWAN, but excluding the Enrolment Services.

Data and Communications Company (DCC)

The holder of the Smart Meter communication licence, Smart DCC Ltd.

Data Service Provider (DSP)

The company awarded a contract to be a service provider of data services to DCC as part of DCC's Relevant Services Capability. CGI IT UK Limited has been appointed to provide these services.

DCC Licence

The licence awarded under section 7AB of the Gas Act 1986, and the licence awarded under section 5 of the Electricity Act, each allowing Smart DCC Ltd to undertake the activity of providing a Smart Meter communication service.

DCC Service Providers

Companies or persons from whom DCC procures Relevant Services Capability; principally the DSP and the CSPs.

DCC User

A SEC Party who has completed the User Entry Processes and is therefore able to use DCC Services in a particular User Role.

DCC Systems

The systems used by the DCC and its DCC Service Providers in relation to the Services and / or the SEC, including the SMWAN but excluding the Communications Hub Functions.

DCC Total System

All DCC Systems and Communications Hub Functions.

DCC User Gateway

The communications interface designed to allow appropriate Smart Metering communications to be sent between DCC Users and the DCC.

Device

One of the following: (a) an Electricity Smart Meter; (b) a Gas Smart Meter; (c) a Communications Hub Function; (d) a Gas Proxy Function; (e) a Pre-Payment Interface; (f) an Auxiliary Load Control; or (g) any Type 2 Device (e.g. IHD).

Distribution Network Operators (DNOs)

Holders of electricity Distribution Licences.

Elective Communications Services

The services associated with processing of Service Requests that are (or are to be) defined in a Bilateral Agreement (rather than the DCC User Gateway Services Schedule) in a manner that involves communication via the SMWAN (provided that such Service Requests must relate solely to the Supply of Energy or its use).

Electricity Smart Meter

A Device meeting the requirements placed on Electricity Smart Metering Equipment in the SMETS.

Eligible Subscriber

An Authorised Subscriber who is permitted to receive a Certificate of a particular Type

Eligible User

A DCC User who, acting in a particular User Role, is eligible to receive particular DCC services, including in relation to a particular Device.

End-to-End Smart Metering System

Any DCC System, Smart Metering System, User System or RDP System.

Enrolled

The status of a Smart Metering System when the Devices which form part of it have all been Commissioned.

Enrolment Services

Services associated with the processing of Service Requests that are involved in the commissioning of Devices in the Smart Metering Inventory, and establishing their inter-relationships, and which ultimately result in the Enrolment of Smart Metering Systems ready for communication via DCC over the SMWAN.

Foundation stage

The period prior to the start of Initial Live Operations.

Gas Proxy Device

A Device which stores and communicates gas-related metering information, required in order to reduce the necessary battery life of Gas Meters, and which forms part of the Communications Hub. The Gas Proxy Device is treated as a separate logical Device for the purposes of Smart Meter communications.

Gas Smart Meter

A Device meeting the requirements placed on Gas Smart Metering Equipment in the SMETS.

GB Companion Specification

A document setting out amongst other things, the detailed arrangements for communications between the DCC and Devices and the behaviour required of Devices in processing such communications.

Hand Held Terminal (HHT)

A HAN-connected Device used by authorised personnel for meter installation and maintenance purposes.

Home Area Network (HAN)

The means by which communication between Devices forming part of Smart Metering System takes place within a premises and which is created by the Communications Hub Function.

In-Home Display (IHD)

An electronic Device, linked to a Smart Meter, which provides information on a consumer's energy consumption and ambient feedback.

Initial Live Operations

The expectation that the DCC will have built and tested its systems for SMETS2 equipment and be operationally ready; all of the Large Suppliers will be ready to use the DCC Services, start installing SMETS2 meters and offer basic services to both credit and pre-payment customers; the DNOs will be ready to support Smart Meter installation; and the Electricity DNOs ready to use the DCC Service to improve network management. Currently, this is planned to be September 2015.

MPAN

The Meter Point Administration Number, being a unique reference number for each metering point on the electricity distribution network and allocated under the Master Registration Agreement.

MPRN

The Meter Point Reference Number, being a unique reference number for each metering point on the gas distribution network and allocated under the Uniform Network Codes.

MPxN

A collective reference to the MPAN and MPRN.

Network Operators

A collective term for holders of electricity distribution licences and gas transportation licences.

Pre-Command

A message generated as part of the processes of converting of Service Requests into Commands, i.e. after Transformation by DCC. For Critical Service Requests Pre-Commands are returned to the DCC User for correlation and signing after DCC has transformed the Service Request.

RDP System

The systems used by, or on behalf of a Network Operator for the collection storage, back-up, processing, or communication of Registration Data prior to being sent to DCC.

Registration Data Provider

A person nominated by a Network Operator to provide Registration Data to DCC under the SEC.

Relevant Services Capability

The internal and external resources which the DCC relies upon in order to provide services to DCC Users.

SECAS

The company appointed and contracted to SECCo to carry out the functions of the Code Administrator and the Code Secretariat - Gemserv.

SECCo

A company established under the SEC, owned by SEC Parties and which acts as a contracting body for the SEC Panel.

SEC Subsidiary Documents

Documents that are referenced by and form part of the SEC, and thus subject to the SEC Modifications Process

Service Request

A communication to the DCC over the User Gateway (and in a form set out in the User Gateway Interface Specification) that requests one of the Services identified in the User Gateway Services Schedule (or, in future an Elective Communications Service).

Service Response

A message sent from DCC to a DCC User over the User Gateway (and in a form set out in the User Gateway Interfaced Specification) in response to a Service Request.

Smart Energy Code (SEC)

The Code designated by the Secretary of State pursuant to Condition 22 of the DCC licence and setting out, amongst other things, the contractual arrangements by which DCC provides services to users as part of its Authorised Business.

Smart Meter

A collective term for an Electricity Smart Meter, and a Gas Smart Meter.

Smart Metering Equipment Technical Specifications (SMETS)

A specification (which is to form part of the SEC) of the minimum technical requirements of Smart Metering Equipment. (Communications Hubs are separately dealt with in CHTS).

Smart Metering Equipment

A collective term for all SMETS equipment (Electricity Smart Meter, Gas Smart Meter, In-Home Device, Pre-Payment Metering Interface Devices, and HAN Controlled Auxiliary Load Control Switches, but not including the Communications Hub)

Smart Metering Inventory

An inventory of Devices which comprise Smart Metering Systems which are (or are to be) Enrolled with DCC. The Smart Metering Inventory also holds information about Devices and their inter-relationships.

Smart Metering System (SMS)

A particular collection of Commissioned Devices installed in a premises.

A Gas SMS comprises a Communications Hub Function, a Gas Smart Meter, a Gas Proxy Device and any additional Type 1 Devices.

An Electricity SMS comprises a Communications Hub Function, an Electricity Smart Meter and any additional Type 1 Devices.

Smart Metering Wide Area Network (SMWAN)

The network that is used for two way communication between Communications Hub Functions and the DCC.

SMKI Participant

The DCC as the provider of the SMKI Service and any SEC party using the SMKI Service

SMKI Subscriber

A SEC Party that has applied for and been issued with an SMKI Certificate

Supplier

The holder of a gas supply licence or an electricity supply licence.

Transformation

The conversion, by DCC, of a Service Request into the format required in order for the command to be executed by a Device.

User Role

One of a number of different capacities in which a DCC Party may (if appropriately authorised and having gone through the necessary User Entry Processes) act, including: Import Supplier; Export Supplier; Gas Supplier, Electricity Distributor, Gas Transporter or Other User.

User System

The systems used by a User for the collection storage, back-up, processing, or communication of data prior, to of for the purposes of, its sending or receipt to or from DCC.

Annex 1: Consultation Questions

3.2: SMKI Policy Management Authority	
Q1	Do you agree with our proposed approach and text for the SEC with respect to the Policy Management Authority? Please provide a rationale for your views.
Q2	Do you agree with our proposed approach to securing the timely appointment of PMA members? Please provide a rationale for your views.
3.3: The SMKI Service	
Q3	Do you agree with our proposed approach and text for the SEC with respect to provision of the SMKI Service? Please provide a rationale for your views.
3.4: SMKI Assurance	
Q4	Do you agree with our proposed approach and text for the SEC with respect to SMKI Assurance? Please provide a rationale for your views.
3.5: Certificate Policies	
Q5	Do you agree with our proposed approach and text for the SEC with respect to the Device Certificate Policy? Please provide a rationale for your views.
Q6	Do you agree with our proposed approach and text for the SEC with respect to the Organisation Certificate Policy? Please provide a rationale for your views.
3.6: Using the SMKI Service	
Q7	Do you agree with our proposed approach to parties using the SMKI service, including by Opted Out Non-Domestic Suppliers? Please give a rationale for your views.
Q8	Do you agree with our proposed approach for the SEC with respect to Liabilities, Warranties and Indemnities? Please provide a rationale for your views.
3.7: Providing the SMKI Repository	
Q9	Do you agree with our proposed approach and text for the SEC with respect to the SMKI Repository? Please provide a rationale for your views.
3.8: SMKI Recovery Processes	
Q10	Do you agree with our proposed approach and text for the SEC with respect to SMKI Recovery Processes? Please provide a rationale for your views.

3.9: SMKI Testing	
Q11	Do you agree with our proposed approach and text for the SEC with respect to SMKI and Repository Testing? Please provide a rationale for your views.
Q12	Where appropriate, when do you consider your organisation will first need to obtain live Device and Organisation certificates to be placed on Devices ordered from manufacturers? This will help to determine when the SMKI Service and SMKI Repository should Go Live. Please provide a rationale for your views.
Q13	Do you agree that Large Supplier Parties should be obliged under the SEC to be ready to participate in SMKI and Repository Testing? Please provide a rationale for your views.
Q14	Do you agree that it is sufficient for only one large Supplier to complete SMKI and repository testing for the SMKI Service and repository to have been proved? Please provide a rationale for your views.
Q15	Do you agree that the SMKI entry processes should be aligned with the User Entry Process Testing in relation to the DCC User Gateway and Self Service Interface? Please provide a rationale for your views.
3.10: Other Security Requirements	
Q16	Do you agree with our proposed approach and text for the SEC with respect to the Location of System Controls? Please provide a rationale for your views.
Q17	Do you agree with our proposed approach and text for the SEC with respect to the Obligations for Cryptographic Material? Please provide a rationale for your views.
4: Supplier Nominated Agents	
Q18	Do you think that it is important that MOPs / MAMs are able to access DCC services directly? Please provide a rationale for your views.
Q19	Do you have any views on the possible options identified for MOPs / MAMs to access DCC services? Please provide a rationale for your views.
Q20	Are there other options which should be considered for MOPs/MAMs to access DCC services?
5.1: Testing Phases	
Q21	Do you agree with our proposed text for the SEC with respect to Test Phasing, consistent with our decisions on testing arrangements detailed in our recent consultation response? Please provide a rationale for your views.

Q22	Do you agree that the term 'Enduring Testing' should be used to encompass both the End-to-End and Enduring Test stages in order to assist comprehension and simplicity? Would the consequential removal of the terms 'End-to-End Testing' and 'User Integration Testing' cause confusion or be undesirable, such that we should reinstate this terminology? Please provide a rationale for your views.
Q23	Do you agree with the proposed approach to include the Projected Operational Service Levels within the SEC? Please provide a rationale for your views.
5.2: Issue Resolution during Testing	
Q24	Do you agree with the need for an issue resolution process in testing? Does the proposed process meet that need? Please provide a rationale for your views.
Q25	Do you agree with our proposed text for the SEC with respect to Issue Resolution? Please provide a rationale for your views.
6.1: Smart Metering System Requirements	
Q26	Do you agree with our proposed text for the SEC with respect to Equipment Testing, and configuration of enrolled Smart Metering Systems? Please provide a rationale for your views.

Annex 2: Planned Further Changes to the SEC

298 The table below sets out the anticipated content that will be the subject of future stages of the SEC, which has been identified at the time of publication. This excludes subsidiary documents.

SEC Section	Content
D: Modification Process	• Role of the Security Sub Committee in modifications process
G: Security	• Provisions setting out the objectives, duties, composition and procedures of the Security Sub-Committee • Provisions setting out the assurance arrangements required to demonstrate compliance with the security requirements for DCC and for DCC Service Users (both at user entry and subsequently)
H: DCC Services	• Provision of Communications Hubs (including forecasting, ordering, delivery, installation and returns) • Business Continuity and Disaster Recovery • Provisions relating to Consumer Access Devices • Performance Assurance (DCC and Users)
I: Data Privacy and Access to Data	• Privacy Audits
K: Charging Methodology	• Charging for costs of security bodies • Communications Hub Charging • Allocation of Liquidated damages for WAN coverage at the end of rollout • Charging arrangements relating to adoption of SMETS 1 foundation meters and adopted communications contracts • Charging for data link costs
X: Transition	• Commencement of Communications Hub Ordering process • Provision of first installation support materials/installer training for Communications Hubs • Any steps to be taken prior to designation of Completion of Implementation • Any steps to be taken to support operational go-live
Y: Foundation meters	• Definition of DCC services in respect of enrolled Foundation meters and related provisions

Annex 3: Draft Compliance Policies

First Version of the Compliance Policy

299 The proposed legal drafting for the first version of the Compliance Policy is shown at Appendix C to Section L in Annex 4.

Full Compliance Policy

300 The proposed scope of the first full Compliance Policy is set out below. The actual text will come into being as a SEC modification raised by the PMA.

Compliance Policy content

301 The purpose of the Compliance Policy is to provide an overview of:

- the PMA's expectations of all SMKI Participants with respect to compliance with the Compliance Policy Materials; and
- how the PMA will monitor and enforce that compliance.

302 The PMA should ensure that the Compliance Policy at a minimum includes provisions relating to:

- the role of the Independent Assurance Scheme with respect to the DCC;
- the annual internal audit;
- the assessment of SMKI Users;
- assurance of the Repository Service; and
- non-compliance.

The role of the Independent Assurance Scheme with respect to the DCC

303 This will detail how the PMA approved Independent Assurance Scheme will enable an assessment of the SMKI Service Provider's compliance with the Compliance Policy Document Set.

304 The Compliance Policy should also set down:

- the frequency of assurance assessments of the DCC's SMKI Service and the role of the PMA in relation to those assessments;
- the scope of the assessments of the DCC's SMKI Service, which should be based on ensuring the DCC (acting as SMKI Service Provider) complies with its obligations in relation to complying with the relevant sections of the Compliance Policy Materials;
- a requirement for the DCC to undergo any further independent *ad hoc* external assurance assessment of its SMKI Service at any time, when requested by PMA;
- the scope of reports, following assessment, to the PMA, identifying any non-compliance with the Compliance Policy Materials; and
- the approach that the PMA will take with respect to reviewing the ongoing suitability of the independent assurance scheme.

Annual internal audit

305 This will place:

- obligations on the DCC (as SMKI Service Provider) to undertake an annual internal audit of the compliance of its SMKI service with the SMKI document set; and
- obligations on the DCC (as SMKI Service Provider) to certify annually to the PMA that they have at all times during the period in question complied with the requirements of the Compliance Policy Document Set as it relates to its SMKI Service. Where the DCC is unable to certify, it must state why it was unable to do so.

Assessment of SMKI Users

306 This will set out the PMA's approach:

- to commissioning *ad hoc* assessments and audits on a sample basis from time to time to provide assurance that all SMKI Users are complying with the Compliance Policy Materials; and / or
- to undertake assessments and audits where there have been instances of non-compliance by SMKI Users; and / or
- to confirm that a Remediation Plan has been completed satisfactorily.

Assurance of the Repository Service

307 This will set out the PMA's approach to assurance with respect to the Repository Service.

Non-compliance

308 This will set out the PMA's approach to dealing with non-compliance.

309 The DCC will be required to provide to the PMA a report containing details of any periods of non-compliance in its role as SMKI Service Provider, and explain the reasons for them.

Annex 4: SEC Drafting

The legal text proposed in this consultation has been combined together with the designated text of SEC1 and the text of SEC2 as consulted, and is published as a separate document alongside this publication.

A change marked version of the same document is also published, highlighting the proposed SEC3 drafting.

In addition, the legal text for each of the Compliance Policy, the Organisation Certificate Policy, and the Device Certificate Policy is also published as draft SEC Subsidiary Documents.

These documents are available from:

https://www.gov.uk/government/consultations/new-smart-energy-code-content-stage-3

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

www.gov.uk/decc

URN 13D/303