Department of Energy & Climate Change

Smart Metering Implementation Programme

Government Response to the Consultation on the second version of the Smart Metering Equipment Technical Specifications

Part 2

1 July 2013

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

Telephone: 0300 068 4000

Website: www.gov.uk/decc

This Consultation Response can also be found on DECC's website

Published by the Department of Energy and Climate Change.

Table of Contents

1. Executive summary

1 In August 2012, the Government launched a consultation on the second version of the Smart Metering Equipment Technical Specifications (SMETS 2). The consultation sought views on a range of issues to be addressed through an updated version of the SMETS, as well as on governance and assurance of security and interoperability; on operational licence conditions; and on the next steps for SMETS 2.

2 The consultation comprised 50 questions on the above topics. Part 1 of the Government's Response was published in January 2013. This addressed 16 of these questions which needed to be resolved in order to notify the first iteration of SMETS 2 to the European Commission. No detailed opinions were issued, nor any significant concerns with the proposed approach raised during the standstill period by the European Commission or other Member States.

3 This document forms Part 2 of the Government's Response to the SMETS 2 Consultation, and addresses the remaining 34 questions on SMETS 2 development, on governance and assurance of security and interoperability, and on next steps for the Smart Metering Implementation Programme (SMIP).

Smart Metering Equipment Technical Specifications - Version 2 Development

HAN Strategy

4 Interoperability is at the heart of the Smart Metering Implementation Programme, both to support interconnection of equipment in the home, and the Change of Supplier (CoS) process. Interoperability requires that standards are specified for both the application and physical layers of the Home Area Network (HAN).

5 Part 1 of the Consultation Response set out our conclusion that the HAN physical layer in SMETS 2 will initially be based on a radio frequency of 2.4GHz, as this solution should be available within the required timescales and provide coverage for at least 70% of GB consumers. We also noted that the HAN strategy allows for the inclusion of an 868MHz-based solution as this becomes available, as this is expected to provide coverage of over 95% of consumers (the balance requiring an alternative HAN solution).

6 The consultation sought views, and received a mixed response on any additional measures that might be needed to encourage the development of an 868MHz-based solution. We have since worked further with energy suppliers to identify the potential variants of an 868MHz-based solution, and the options for its development.

7 Through these discussions, we have concluded that energy suppliers have a clear incentive to initiate the development of an 868MHz-based solution, as they will need to develop HAN solutions to meet their roll-out licence obligations to install smart meters in every property by the end of 2019[1], and

[1] Following the Government's announcement on 10 May 2013, this date has been changed to 2020.

the operational licence requirement that they provide certain smart services where they install these meters. This comes into effect in July 2013. We welcome the steps suppliers are taking, facilitated by the trade association Energy UK, to carry out a study to determine the feasibility of the different options for an 868MHz-based solution. To maintain visibility of this work, suppliers are required to report progress on their HAN strategies in their Annual Supplier Reports to DECC, which are requested under licence conditions.

8 Responses to the consultation question on the approach to determining the balance between single (2.4GHz) and dual-band (2.4GHz / 868MHz) communications hub deployment were also very mixed, with no clear views emerging. We have concluded that the first tranche of communications hubs will be single-band, 2.4GHz-based models.

9 When the additional HAN solutions have been developed, we expect that the Communications Hub Technical Specification (CHTS) will be amended to identify variants of the communications hubs that provide these HAN solutions. The DCC's CSP(s)[2] will be required to offer terms for the provision of each of these communications hub variants, which suppliers will be able to order based on their commercial and operational preferences. We will consult on charging arrangements for communications hubs during the drafting of the SEC. We expect to propose a model of differential costs for single and dual-band hubs, which should motivate suppliers to optimise their installation procedures.

10 A very small number of responses were received to the consultation question on the potential value to smart metering of spectrum next to the 868MHz licence exempt part, to be released by Ofcom. We consider that reserving spectrum at this frequency does not offer any significant advantages in support of an optimised smart metering HAN strategy, either in terms of timescales or costs.

11 An alternative HAN solution is needed for the estimated 5% of properties where wireless solutions will not achieve satisfactory propagation – including high rise flats. We completed a trial to measure a range of wired HAN parameters in a variety of multiple dwelling units, and are also seeking further information from industry on the likely performance of different technologies. These findings will be used to inform the further, on-going development of alternative HAN solutions. Further work will also be done on how to take this work forward, including who is best placed to do it and if any regulatory intervention will be required.

12 A mixed response was received to the consultation question on a proposal to place a 'fit for purpose' obligation on suppliers, to ensure that the solution they install at any property is capable of serving all the smart metering equipment that will be needed at that property (e.g. where customers have gas and electricity provided by different suppliers). Having assessed the responses, we have concluded that a fit for purpose requirement is not necessary at this

[2] The outcome of the CSP competition is on a regional basis and may result in one, two, or three CSPs; we therefore refer to CSP or CSPs, contracted to CSP(s).

stage. Instead, the communications hub charging methodology (see paragraph 9 above) will be structured to ensure it appropriately incentivises cost-effective outcomes when alternative HAN solutions are available for installation at any premises.

Communications Hub

13 The consultation also sought views on the proposed communications hub functionality, and on any potential additional requirements. Respondents were supportive of the proposed functionality for connections to the WAN and the HAN, message handling, and data storage and processing, and also suggested a number of additions.

14 Having assessed these, we have decided to extend the CHTS to include provisions for wireless firmware updates to Type 1 devices connected to the HAN, and for the buffering of firmware upgrades to gas meters. It will also mandate a requirement that the communications hub is able to send power outage alerts, and that the communications hub is powered by a DC power feed from the electricity meter.

15 Building on the evidence submitted in response to the consultation, and working in conjunction with industry, we have also decided that the CHTS will set out a requirement for communications hubs to be able to support up to 16 devices, including four electricity meters (conventional and micro-generation), a gas meter and a gas proxy device, five auxiliary load control switches, three CADs (including one IHD), and two prepayment interface devices (PPMIDs).

16 In the light of majority support for the proposal, we have decided that an intimate interface should be mandated between the electricity meter and the communications hub. All communications hubs must comply with the Intimate Communications Hub Interface Specification (ICHIS), which will be developed by the DCC and CSP(s), in conjunction with suppliers and industry. The SMETS will require all suppliers to provide an intimate electricity meter at each smart metering installation, or a hot shoe which allows the communications hub to be fitted in standalone mode, together with a 12v power supply to the hub.

17 The proposal that suppliers should not be required to install CHTS-compliant communication hubs for opted-out non-domestic consumers was strongly supported and will be implemented. Procedures will be developed to mitigate cost and complexity on change of supplier, including that the registered supplier (likely to be the gaining supplier) should bear the site visit costs of any requirement to remove a communications hub.

18 More widely, in all cases where communications hubs are removed from consumers' premises, we have taken steps to ensure that the CSP(s) are incentivised to recondition and reintroduce them into the supply chain if it is economic to do so.

19 Respondents were strongly supportive of the proposal that the CHTS is extended to include a requirement for power outage detection. We agree with the view that power outage reporting could sit either in the communications hub, or in the CSP network. We will require the CSP(s) to be

responsible for power outage reporting, and to decide where in their end-to-end infrastructure this best sits.

20 Power outage reporting will not be mandated for opted-out meters. Respondents noted that this is potentially complex, and that 100% coverage of outage reporting is not required for the realisation of full benefits from outage management.

CAD Pairing

21 The consultation set out two options for securely connecting ('pairing') Consumer Access Devices (CADs) to the consumer's HAN: local (where the consumer enters information locally on their meter) and remote (where the consumer pairs through a third party – e.g. via the internet or a call centre). In the case of remote pairing, the consultation sought views on the obligations which might be placed on energy suppliers to support this process. Finally, we asked whether any other options for pairing should be considered.

22 The majority of respondents favoured the option for remote pairing, principally on the grounds of security. However, a significant minority supported local pairing as this does not require third party input or a WAN connection, and may better support the anticipated increase in the volume of pairing over time. In the light of this spread of views, we have decided to pursue both options. No significant other options for pairing were identified.

23 The SMETS 2 and the CHTS will be extended to include requirements to support both remote and local options for consumers to pair and de-pair CADs to their HANs.

24 In the case of the remote option, any DCC User will be allowed to use a DCC service to initiate CAD pairing and de-pairing. Users of this DCC service will be required to verify the identity of the energy consumer from whom they have obtained permission to initiate CAD pairing, in line with good industry practice.

25 In the case of the local option, security concerns will be addressed through measures to support that a consumer is entitled to, and does, pair the right device to the right meter.

26 We anticipate that DCC Users may need to offer additional services to support both remote and local pairing. Further work will be undertaken to determine what these services should be and who would be best placed to deliver them.

Other Interfaces

27 In the light of strong support for both proposals, the SMETS will be extended to support a prepayment interface device (PPMID) and an interface for hand held terminals (HHT).

28 Suppliers will optionally be able to provide consumers who are on a prepayment tariff with a PPMID, which will provide a more accessible interface than that available through the meter itself. The PPMID interface will allow the consumer to activate emergency credit for both gas and electricity, re-enable the electricity supply following disconnection (provided it is armed), and display a range of pre-payment data, for example the meter balance.

The case for gas enablement via the PPMID has not been made and will not be included in the current version of the SMETS.

29 An HHT could be used by a supplier to support meter installation processes, or to configure meters where there is no WAN connection. An HHT interface to the HAN will be specified to facilitate their use. The interface will allow all supplier commands to be 'passed through' from an HHT to the HAN, provided that they meet the same security requirements for signing to show they are authorised by the supplier, applicable to those delivered via the WAN.

Governance and Assurance of Security

30 The consultation sought views on the appropriate governance regimes for security requirements for the period following commencement of DCC services.

31 Respondents were broadly supportive of the proposal that the maintenance of smart metering security requirements will best be performed by a technical sub-committee of the SEC Panel.

32 A Security Sub-Committee will be created under the SEC Panel to keep security arrangements under review and consider whether they continue to be appropriately balanced against the SEC objectives and the wider threat and risk landscape. This approach will allow the security arrangements to reflect changing circumstances and provide effective coverage of evolving risks.

33 The consultation proposed that independent assurance procedures be put in place to demonstrate that elements of the solution have achieved a known level of compliance with published security requirements. Respondents were broadly supportive of this proposal, but less supportive of performing re-testing at set intervals.

34 We have decided that the DCC, and DCC Users, will be subject to independent assurance processes, to demonstrate compliance with security controls and the application of security good practice in the management of emerging threats. For DCC Users, this will depend on their SEC Role Code; the DCC will be audited in accordance with the Service Organisation Control 2 (SOC2[3]) standard. Both the DCC and DCC Users will be subject to time-based testing.

35 In line with the majority of views, the UK Government's National Technical Authority for Information Assurance Commercial Product Assurance– Foundation Level security certification scheme for Type 1 SMETS 2 equipment[4] will be introduced to provide assurance that it complies with the smart metering security requirements. We consider that this scheme will provide a cost effective, flexible and proportionate certification regime to meet the security assurance requirements for smart metering deployment.

[3] The Service Organisation Control 2 (SOC2) standard, as defined by the AICPA until such time that the equivalent ISAE standard is in place.
[4] Any equipment which is relied upon to enforce specific security controls, and can issue commands to other devices on the HAN. Examples include the gas and electricity meters, and communications hub. Type 2 devices, which are essentially 'read only', will not be subject to certification under the CPA scheme.

36 Recertification will be required periodically in accordance with the requirements of the CPA scheme or in response to a significant change. The effort and cost of this will be proportionate to the nature and extent of the event. We are discussing further with industry whether the default of two yearly re-certification is appropriate for smart meters.

37 The majority of respondents were supportive of sanctions for non-compliance with security requirements, which will be provided within the SEC. These are likely to be hierarchical in structure, and take account both of remediation of security issues, and the impact on consumers, before they are imposed.

38 In line with the majority of respondents' views, we will place specific security obligations on non-domestic suppliers operating SMETS equipment outside the DCC, through a licence condition. This will be based on high level principles, requiring them to implement appropriate security obligations, and carry out a number of recognised industry good practice disciplines for identifying and managing security risks to their systems. It will provide assurance that a consistent level of security is achieved across SMETS installations.

39 For non-domestic suppliers who enrol smart metering systems into the DCC will have detailed security obligations in the SEC, supplemented by a general licence obligation to maintain the security of their systems.

40 We will consult on the legal drafting for embedding the arrangements for the Security Sub-Committee, assurance, and the sanctions framework into the SEC. We will also consult further on the content of the enduring licence conditions for opted-out non-domestic suppliers.

Assurance of Smart Metering Equipment Interoperability

41 Many participants will play a role in the procurement and deployment of smart metering equipment. It is in the interests of all parties that equipment from multiple manufacturers interoperates seamlessly within consumers' premises, so that equipment does not have to be replaced, adding cost and creating disturbance for customers.

42 The consultation sought views on the regimes that will be required to provide appropriate levels of assurance for interoperability, including the inter-changeability of certified equipment between suppliers. The great majority of respondents agreed that these regimes are in the interests of all parties, and should be subject to assurance.

43 The GB Companion Specification will set out those elements of the base ZigBee SEP and DLMS communication protocol specifications applicable to the GB market and successful testing against these specifications will enable equipment to receive protocol certification. The equipment will also be security certified under the CPA – Foundation Level regime. On achievement of both certificates, the equipment will be placed on a 'certified products list' to be introduced and maintained by the SEC Panel. SMETS 2 equipment that is not on the certified product list will not be eligible for automatic enrolment into the DCC.

44 We will make a consolidated proposition for testing and certification available for further comment by industry in July 2013. This will include proposals for:

- the DCC and its Service Providers testing their systems to ensure that they deliver the services defined in their licences, the SEC and their contracts as part of the end-to-end system, and using SMETS and CHTS compliant equipment when they undertake this testing;
- equipment to be enrolled in the DCC being interoperable with the DCC's systems – and suppliers and the DCC undertaking testing to ensure that they meet the inter-operability requirement; and
- large energy suppliers being ready to participate in testing at the user integration stage of SMIP delivery.

45 The DCC will be required to provide a test environment that can be used to test the interoperability of in-home equipment with the DCC's systems. It will also be required to maintain, for information purposes, a deployed products list of the combinations of equipment enrolled in DCC, including details of each device's configuration and version number.

Next Steps

Finalising SMETS 2 and the CHTS

46 Following the notification of the first iteration of SMETS 2 in January 2013, a number of activities now need to be completed in the period through to the start of smart metering roll-out in 2015. The consultation sought views on a number of issues which will inform the development of more detailed plans for this period.

47 In Part 1 of the Consultation Response, we set out our decision that we would adopt a CSP-led model for communications hubs responsibilities. The great majority of respondents agreed that this model should be reflected in the regulatory framework.

48 We intend that the requirements to provide the communications hub will be placed in the DCC licence, and that the DCC would procure communications hubs via the CSP. In addition, the roll-out licence condition will be amended to require that suppliers install a DCC communications hub in domestic consumer premises.

49 The consultation also sought views on the likely timescales for equipment availability. Taking account of evidence submitted, alongside wider analysis of the timescales needed to design, build and test the smart metering system, we announced in May 2013 a revised timetable for the overall smart metering programme. We now expect suppliers to be ready to start mass roll-out by autumn 2015, and to complete this by the end of 2020. An updated high level view of the Smart Meters delivery plan will be published later in 2013.

50 We plan to introduce SMETS 2 into the regulatory framework at the earliest possible date. However, it seems reasonable that SMETS 1 metering equipment installed after this date should also count towards suppliers' roll-out targets for a limited period. We will give notice of the date after which new SMETS 1 installations will no longer count towards suppliers' roll-out targets.

Governance of Technical Specifications

51 The consultation considered when the Technical Specifications (the SMETS, CHTS, GBCS and CPA Security Characteristics) should become part of the SEC, and how subsequent modifications should be handled.

52 In line with the majority view, it is anticipated that the Technical Specifications will be managed via the SEC governance procedures when SMETS 2 is introduced into the regulatory framework.

53 To a large extent, we will rely on the standard SEC modification procedure for any changes to the Technical Specifications. However, we will introduce a number of additions to reflect their highly specialist nature. This will include a requirement for the SEC Panel to set up a Standing Technical Specifications Sub-Committee which, amongst other matters, will consider the impact of proposed modifications on the end-to-end smart metering architecture. The DCC will be required to assess the impact of any proposed modifications on its systems, and advise the SEC Panel accordingly, via the sub-committee.

Other Matters

54 We have addressed a number of outstanding issues from Part 1 of the Consultation Response. These include:

- a decision to remove the provisional requirement for a keypad to be provided on all meters;
- confirmation that the licence conditions for the operational requirements have been amended as set out in the Consultation Response, and will come into effect on 14 July 2013; and
- further information on the definition of communications hubs type faults, and the allocation of costs to the CSP or supplier depending on cause under the 'costs lie where they fall' principle.

55 Finally, we set out our proposals to meet the requirements of the EU Energy Efficiency Directive, and our response to the December 2012 consultation on this subject. SMETS 2 will be extended to include a requirement for the electricity meter to store 24 months of daily consumption data. The CHTS will require that the communications hub stores the equivalent for gas. We intend to update suppliers' licence conditions to require that domestic consumers with any SMETS meter are provided with consumption data over the meter interface or the internet on request, and to ensure it is provided free of charge.

2. Introduction

Overview of Consultation

56 The Government published the first version of the Smart Metering Equipment Technical Specifications (SMETS 1) in April 2012. SMETS 1 provided a standardised and consistent definition of the functional requirements for smart metering equipment, allowing suppliers to install and operate smart meters which would count towards their roll-out targets during the Foundation Stage of the programme. Such installations provide early learning and benefits.

57 In parallel to the publication of SMETS 1, the Government identified several issues which would require further consideration before their inclusion in a future version of the SMETS. In August 2012, a consultation was launched to seek industry views on these outstanding issues, and on related technical and security issues, presenting a proposed way forward on each.

58 The consultation set out proposals to address the following issues:

- Extensions to SMETS, including the proposed standards of the Home Area Network (HAN); functionality of, and responsibility for the Communications Hub; and additional capabilities to be included in the SMETS;
- Governance of security requirements, and the provision of appropriate levels of assurance for both security and interoperability of the end-to-end smart metering solution;
- Operational licence conditions to be placed on energy suppliers to ensure the availability of smart metering data to consumers, network operators and third parties; and
- Next steps, for the publication of SMETS 2, for its governance in the Smart Energy Code (SEC), and for expected equipment availability.

The Consultation Process

Response to the Consultation

59 All consultees were invited to submit their comments to a consultation email address (smartmetering@decc.gsi.gov.uk). The Consultation was available on the Department of Energy and Climate Change (DECC) website and a paper version of the consultation document was made available on request.

60 The Consultation invited all interested parties to comment on the proposals by 8th October 2012. 56 written responses were received, broken down by sector as follows:

Sector	Number of responses
Communications and Technology	12
Consumer Group	3
Energy Network	6
Energy Supplier	11
Industry participants	5
Member of the Public	1
Meter Manufacturer	9

Sector	Number of responses
Other Government	1
Security Specialist	1
Other	7

61 Annex 1 provides a list of the organisations that provided a written response to the Consultation and Annex 2 provides an overview of responses to the 34 Consultation questions included in this Part 2. The majority of responses were sent electronically. The collation and summary of responses has been prepared by DECC. We will also publish any non-confidential consultation responses.

62 DECC has continued to meet with the Solution Design Advisory Group[5] (SDAG) and the Overall Design Authority Group (ODAG) from the launch of the Consultation through to the publication of this response document. These groups, which include experts from consumer bodies, manufacturers, energy suppliers, DNOs, Ofgem and other interested parties, have continued to advise on the development of the SMETS, the Communications Hub Technical Specification (CHTS) and related issues. We have also taken into account advice from bidders to the CSP and DSP procurements, and applicants for the DCC licence award, on relevant issues.

Publication of the Government's Response to the SMETS 2 Consultation

Publication of Part 1

63 The questions in the SMETS 2 consultation were grouped into the following categories:

- SMETS 2 development – 30 questions;
- Governance and assurance – 9 questions;
- Operational licence conditions – 5 questions; and
- Next steps – 6 questions.

64 Our response to the SMETS 2 Consultation has been published in two parts. Part 1 of the Consultation Response was published in January 2013[6], and set out our response to 11 questions relating to SMETS 2 development, and all five questions relating to operational licence conditions.

65 The publication of Part 1 of the Consultation Response was designed to support the notification of that part of SMETS 2 pertaining to gas and electricity meters, and the IHD, to the European Commission as per the requirements of the Technical Standards and Regulations Directive[7]. Henceforth, that notified document is referred to as the first iteration of SMETS 2.

66 Notification of the first iteration of SMETS 2 was designed to facilitate equipment availability for the next generation of GB smart metering equipment. SMETS 2 reflects the original 'A-H Requirements' set out in the

[5] Prior to December 2012, the SMETS Stakeholder Advisory Group (SSAG)
[6] https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version
[7] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services

March 2011 Prospectus Response, and provides a strong basis for the industry's development programmes in advance of mass roll-out.

67 After notification of any document under this Directive to the European Commission, a standstill period of a minimum of three months applies during which time the draft measures may not be adopted. This period may be extended if the European Commission or a Member State believes the specifications may create obstacles to the free movement of goods in the internal market.

68 The standstill period for the notification of the first iteration of SMETS 2 ended on 25 April 2013. No 'detailed opinions' were issued, nor any significant concerns with the proposed approach raised during the standstill period by the European Commission or by other Member States.

Publication of Part 2

69 Part 2 of the Consultation Response (this document) contains our response to the remaining 19 questions relating to SMETS 2 development (Section 3), all questions relating to governance and assurance (Sections 4 and 5), and next steps (Section 6). Annex 2 summarises the responses received for each question.

70 Section 7 includes an update on the issues outstanding from the publication of Part 1 of the Consultation Response, and / or the first iteration of SMETS 2; and information on communications hubs type faults further to inform the 'costs lie where they fall' principle for repair and replacement set out in Part 1 of the Consultation Response.

71 Section 8 sets out our response to the consultation on the Energy Efficiency Directive.

Next Steps

Overall Programme timescales

72 In December 2012, we committed to review the programme plan and timetable for smart metering, taking account of learning from energy suppliers from their early smart meter deployments, and from bidders who wish to provide the common data and communication infrastructure (the 'DCC services') necessary to support smart metering on a nationwide scale. We published the results of our review on 10 May 2013[8].

73 As part of the procurement process, we have tested with bidders for DCC communication and data service provider contracts, and with the energy industry, the time needed for the design, build and test phases of their programmes. The consistent message was that more time was needed if the mass roll-out was to get off to the best possible start and ensure a quality experience for consumers. As announced, we therefore now expect suppliers to be ready to start their full scale roll-out by autumn 2015, supported by the DCC services.

[8] https://www.gov.uk/government/speeches/written-ministerial-statement-by-edward-davey-smart-metering

74 Completing the national roll-out will be an enormous logistical and technical challenge for the industry, involving visits to around 30 million homes and small businesses and installing over 50 million meters. To this end, and reflecting the extended period to build and test the systems required by industry we have announced a move in completion date for the mass roll-out from end 2019 to end 2020 - although we expect the vast majority of smart meters to be in place against the original 2019 deadline.

Further development of the SMETS

75 The second iteration of SMETS 2 is now under development with a detailed assurance process, including industry representations. The second iteration will include the GB Companion Specification (GBCS), which will set out how the application protocols will be used to deliver the SMETS functionality, and requirements of the Commercial Product Assurance (CPA) regime, covering the security characteristics of devices.

76 The second iteration of SMETS 2 will also include provisions for:

- a Pre-Payment Interface Device (PPMID), including the functionality to allow a PPMID to interface with the HAN;
- Auxiliary Load Control switches;
- CAD pairing, including the functionality to allow a device to pair with the Communications Hub locally; and
- the use of Unique Transactional Reference Numbers (UTRNs), for use in prepayment should the WAN be unavailable.

77 We are continuing to work on these documents and will publish them in due course. If you would like to see early drafts, please contact us at smartmetering@decc.gsi.gov.uk.

78 The GBCS is intended to be notified to the European Commission as part of the second iteration of SMETS 2. Notification is expected to occur in Q2 2014, although the final timing is dependent on the development of further releases of the application protocols (including the GB security extensions needed to support SMETS functionality) by the protocol owners.

3. SMETS 2 Development

79 The consultation sought views on a range of topics related to the development of the next generation of smart metering equipment. Part 1 of the Consultation Response addressed questions which impacted on the notification of the first iteration of SMETS 2 to the European Commission, including those relating to the HAN application and the initial physical layers for 2.4GHz-based solutions, responsibility for the communications hub, and some additional functionality that will facilitate smart grids. The first iteration of SMETS 2 was notified to the European Commission, as set out in paragraph 65 *et seq* above.

80 This section addresses the remaining issues from the consultation, which were not part of the first iteration of SMETS 2. These include the further development and deployment of 868MHz and alternative (e.g. wired) HAN solutions, functional requirements of the communications hub (including provision for an intimate interface), CAD pairing and provisions for the development and use of PPMIDs and HHTs[9].

81 Having analysed the responses to Question 12 of the Consultation, we set out in Part 1 of the Consultation Response how we were minded to adopt a CSP-led model for communications hub responsibility, subject to further confirmation through the Invitation to Submit Final Tenders (ISFT) for CSP services.

82 CSP bidders have confirmed their willingness to adopt this model, and will now be required to supply communications hubs as part of their service contract. The remainder of this section is presented on this basis.

HAN Physical Layer – 868MHz-based Solution Development

Summary of issue under consideration

Part 1 of the Consultation Response set out the Government's conclusion that SMETS 2 will initially require solutions based on 2.4GHz, and will be extended to accommodate a solution based on 868MHz as this becomes available.

The consultation sought views on any additional measures that might be needed to encourage the development of an 868MHz-based solution (Question 7), the role of the market in determining both the roll-out balance between the 2.4GHz and 868MHz solutions (Question 8), and the approach to single / dual-band communications hub deployment (Question 9).

Ofcom is overseeing the release of spectrum next to the 868MHz licence-exempt part for HAN deployments. As part of the overall HAN strategy for smart metering, the consultation considered the compatibility, and potential value of this spectrum (870 – 876MHz) (Question 6).

[9] Although not the subject of the SMETS 2 consultation, our conclusions on meter keypads are set out in Section 7.

Government consideration of issue

Development of an 868MHz-based solution

83 A mixed response was received to the question on the need for additional measures to encourage the development of an 868MHz-based solution. A number of respondents argued that the market may not bring forward a solution without an external stimulus or will take a long time to develop such a solution. Others cited problems that may arise if an 868MHz-based solution is not available. However there were few practical suggestions as to the measures that might be adopted to mitigate this risk, although one respondent proposed that the CSP(s) should be required to deliver an 868MHz-based communications hub.

84 Some responses were caveated by the observation that a wired solution should be developed in parallel, as set out in the SMETS 2 consultation. This issue is covered below in paragraph 119 *et seq*.

85 A significant minority did not support the need for additional measures, arguing principally that market forces will drive the timely delivery of an 868MHz-based solution.

86 Responses to the proposal that the market should determine the balance between 2.4GHz and 868MHz-based solutions were mixed, with no clear preferences emerging.

87 However, some respondents expressed concern that the earlier availability of 2.4GHz-based solutions could drive market dominance, and that 868MHz-based solutions might be used only as 'in-fill'. Potentially, the more limited demand may then undermine support for 868MHz-based solution development, and increase costs. To address this, it was suggested that the CSP(s) should be mandated either to supply dual-band communications hubs as these become available, or at least to offer a minimum volume of them.

88 Considering the options for communications hub deployment, respondents provided limited evidence on the costs and benefits of the different approaches (2.4GHz as the default; dual-band; or market led). The largest group of respondents favoured a market-led approach, citing the benefits of cost avoidance where a dual-band communications hub was not required, and the flexibility to allow the market to evolve. However, almost as many respondents supported a dual-band approach, citing the benefits of simplified logistics and flexibility in favour of this option.

89 We set out our preferred strategy for the HAN physical layer in Part 1 of the Consultation Response. We concluded that initially SMETS would require that a 2.4GHz-based solution was utilised. However, in time an 868MHz-based solution would likely be required and so would be included in SMETS as an option as soon as it becomes available. Accordingly SMETS 2, as notified to the EC in January 2013, specified that equipment must utilise the 2.4GHz-based solution.

90 Since publishing Part 1 of the Consultation Response, we have carried out further analysis of:

- the availability of 868MHz-based solutions, recognising the variants that are potentially available;
- the options for bringing an 868MHz-based solution to market; and
- the procurement approach for communications hubs.

91 Working with industry stakeholders and the ZigBee Alliance, we have identified several potential variants to the 868MHz-based solution. Some of these would support 'gas only' operations (i.e. to address situations where a 2.4GHz solution is unable to propagate to the gas meter) while others are 'full' solutions (i.e. would offer a fully-functional alternative to 2.4GHz). While the 'full' 868MHz-based solution offers greater flexibility as it can handle links to all devices, further work is required to identify all development challenges.

92 It should also be noted that the 'gas only' variant would, of necessity, require a dual-band communications hub as 2.4GHz would be used for the electricity meter and in-home display, with 868MHz used for the link to the gas meter. By contrast, the 'full' variant could operate with a single-band 868MHz communications hub, or a dual-band hub supporting both 2.4GHz and 868MHz.

93 With regard to the need for any additional measures to encourage the development of an 868MHz-based solution, we have reviewed the incentives that exist currently and considered whether additional regulatory or other actions are required.

94 The roll-out condition in the energy supply licences requires suppliers to install SMETS-compliant smart meters in every domestic and smaller non-domestic property by 2019[10]. In addition, the operational licence conditions, which are currently lying in Parliament in draft, will require that suppliers make certain smart services available to the consumer. Given that 2.4GHz solutions are not expected to facilitate the provision of some smart services in up to 30% of GB properties, we consider that energy suppliers will have to develop and deploy alternative HAN solutions (most likely including an 868MHz-based solution). Development of the alternative solution will be needed if consumers and suppliers are to realise the benefits of smart metering in these properties.

95 Furthermore there is a commercial incentive for suppliers to promote the early availability of an 868MHz-based solution, in order to optimise the efficiency of their roll-out programmes. Without an 868MHz-based solution, there is a risk that suppliers may find it increasingly difficult to screen properties for 2.4GHz suitability, and thus face a rise in the numbers of aborted visits.

96 We therefore welcome the fact that suppliers have recognised the need for an 868MHz-based solution and have agreed, through Energy UK (EUK), to undertake the detailed technical feasibility work referred to in paragraph 91 above. We understand that EUK will promote the adoption of an 868MHz-based solution into the ZigBee standard, and that meter manufacturers are also engaged in this process.

97 To ensure that Government has visibility of the 868MHz development work, suppliers are required to report progress on their HAN strategies in their

[10] Following the Government's announcement on 10 May 2013, this date will be changed to 2020.

Annual Supplier Reports to DECC, which are requested under licence conditions[11]. However, we have concluded, for the time being, that no further regulatory intervention is required in relation to the 868MHz-based solution. This position will be kept under review, and if suppliers fail to make progress as expected, we will consider introducing additional regulatory requirements.

98 We expect that the 868MHz-based solution will only be finalised after the SMETS and CHTS have been incorporated in the SEC, and so will be subject to the Code Modification Procedures. As the body responsible for authorising material Code modifications, Ofgem would notify the revised SMETS and the CHTS to the European Commission as required under the Technical Standards and Regulations Directive[12].

99 Initially DCC - via its CSP(s) - will only be required to deliver single-band, 2.4GHz-based communications hubs, as this is the only HAN solution currently identified in the CHTS. When the additional HAN solutions are developed, the CHTS will be amended (as described in paragraph 98) to identify variants of the communications hubs that provide these HAN solutions. The DCC's CSP(s) will be required to offer terms for the provision of each of these communications hub variants, which suppliers will be able to order based on their commercial and operational preferences. This framework will allow the market to decide the balance of communications hubs installed in GB properties. We consider that this is the most appropriate solution, as the market is best placed to understand and balance the installation, equipment and logistical costs they will bear by choosing particular communications hub variants.

100 Charging arrangements for communications hubs will be consulted on during the drafting of the SEC. We intend to propose that charges should reflect the differential costs between single and dual-band communications hubs. This will incentivise suppliers to optimise their ordering procedures while still providing the commercial choice to opt for dual-band communication hubs.

Reserved Spectrum

101 Ofcom has recently completed a consultation on whether spectrum at 870 – 876MHz (as well as at 915 – 921MHz) should be sold or pursued as licence exempt, subject to any Government decisions on whether to reserve this spectrum.

102 The Ofcom consultation noted a preference to release this spectrum as license exempt, as this approach would be the most likely to generate greater value for the UK economy. Ofcom noted the CEPT[13] vision for this band and its use as licence exempt and the substantial value offered by potential uses including smart metering. Ofcom has now announced[14] that the 870-876 MHz band will be made available on a licence exempt basis. Ofcom aims to

[11] Smart Meters Implementation Programme: Government response to consultation on information requirements for monitoring and evaluation, DECC, December 2012: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43136/7206-gov-resp-cons-sm-monitor-evaluation.pdf

[12] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services

[13] The European Conference of Postal and Telecommunications Administrations

[14] http://stakeholders.ofcom.org.uk/consultations/872_876_mhz/

consult further on the technical requirements later in 2013 following further CEPT work on this band and aim to make the necessary exemption regulations by spring 2014.

103 A small number of responses were received to the DECC consultation question considering the compatibility, and potential value, of the reserved spectrum. Most suggested that that there were merits in exploring the benefits of this option further. A minority argued that uncertainty about the availability and benefits of dedicated spectrum would distract from development of 868MHz-based solutions.

104 Following further consideration, we have concluded that reserved spectrum is not necessary to support our preferred HAN deployments. The 863-870MHz spectrum specification options already have the potential to deliver our identified functionality requirements. Similarly, the technical rules (e.g. power levels) adopted by Ofcom at 870-876MHz could equally support smart meter deployments in terms of HAN coverage, whether reserved or set as license exempt.

105 Modelling also suggests that in-band interference risks can be minimised through solution design at 868MHz, whilst the risk from out-of-band interference remains similar whether spectrum is reserved or not. Finally, the reserved spectrum offers no timescale advantages over existing 868MHz options.

Government Conclusion

As noted in Part 1 of the Consultation Response, our HAN strategy allows for the inclusion of an 868MHz-based solution as this becomes available. We have concluded that energy suppliers have a clear incentive to initiate the development of an 868MHz-based solution and we welcome the steps they are taking. Suppliers will be required to report progress on their HAN strategies (including 868MHz-based solution development) as part of their annual reporting to DECC.

The first generation of communications hubs will be single-band, 2.4GHz-based models. When the CHTS is amended to include additional HAN solutions, the DCC's CSP(s) will be required to provide communications hub variants that reflect these options and the commercial and operational preferences of suppliers.

Reserving spectrum in proximity to 868MHz is not needed to support an optimised smart metering HAN strategy. It does not offer any significant advantages in either technology or timescales.

HAN Physical Layer – Installation Obligations on Suppliers

Summary of issue under consideration

The consultation sought views on a proposal to place a 'fit for purpose' obligation on suppliers, to ensure that the solution they install at any property is capable of serving all the smart metering equipment in that property (Question 10).

Government consideration of issue

106 Respondents to the consultation, including energy suppliers, were split between those who agreed and disagreed that a fit for purpose condition was necessary or would be effective.

107 Opponents argued that compliance with the condition could be difficult to achieve in a subset of properties (for example, high-rise flats), could only be judged subjectively (as it is unclear how suppliers would test whether the 2.4GHz solution was capable of providing a reliable communications link to all the smart metering equipment in the premises) and would likely lead to a number of disputes. They were also concerned that such a requirement could prevent early installations at sites where 2.4GHz would work for the electricity meter and the IHD, but not the gas meter, even where the customer has agreed that a partial installation could go ahead.

108 Supporters felt that a fit for purpose requirement was necessary to avoid the risk of needing two communications hubs and two In-Home Displays (IHDs) in split fuel households, and so lead to a better consumer experience and reduced roll-out costs. They also argued that the requirement would encourage the early development of the 868MHz HAN solution.

109 The initial 2.4GHz HAN solution is unlikely to be appropriate for use in up to 30% of properties in GB. While the signal from the communications hub to the electricity meter should be sufficient (as they will nearly always be co-located), in certain properties the 2.4GHz signal may not propagate sufficiently to serve the gas meter and / or the IHD throughout the property.

110 In advance of the development of alternative HAN solutions (see paragraph 119 *et seq*), suppliers have indicated that they are targeting properties where the 2.4GHz HAN is most likely to serve all smart metering equipment. However, there are expected to be instances where suppliers initiate installation visits at properties where 2.4GHz may not serve the IHD or the gas meter. We have therefore considered the case for a fit for purpose obligation in each of these instances.

111 Considering first cases where 2.4GHz is unlikely to serve the IHD throughout a consumer's premises: the in-home display licence condition requires that suppliers offer an IHD to domestic consumers when a smart metering system is installed (or if requested within a year of the installation) [15] and the Operational Licence Condition requires that suppliers take reasonable steps to maintain the communications link with this IHD. The Smart Metering Installation Code of Practice requires that the IHD is located in an appropriate location, as the benefits of the IHD are dependent on regular consumer interaction with consumption information[16].

112 Where a communications link does not initially form with the IHD, suppliers may overcome these issues by moving the IHD closer to the electricity metering point or using signal boosting technologies. However, it is only

[15] Condition 40 in the electricity supply licence and condition 34 in the gas supply licence contain the IHD provisions www.ofgem.gov.uk/Licensing/Work/Pages/licence-conditions-consolidated.aspx

[16] Condition 3.5.1 - www.ofgem.gov.uk/Sustainability/SocAction/Publications/Documents1/Smart_Metering_Installation_Code_of_Practice.pdf

appropriate to do this when the IHD will be served in an appropriate location for the consumer. Given that an IHD must be offered, that reasonable steps must be taken to form a communications link and that there are existing requirements relating to IHD location, we do not consider that introducing a fit for purpose condition would lead to significantly different outcomes in terms of where the 2.4GHz solution will be installed.

113 Secondly, considering the scenario where a 2.4GHz communications link can be formed between the communications hub and the IHD, but not with the gas meter: it is unlikely that moving the meter or the use of booster equipment will offer a practical or economically efficient resolution of this issue. Therefore, suppliers will have to decide whether to install no smart metering equipment or, if the IHD can be served by 2.4GHz, install only the electricity metering system.

114 Whilst undertaking a partial electricity-first system installation in split fuel households may lead to additional costs (as the gas supplier will potentially have to install a communications hub and provide an IHD that utilises an alternative HAN solution), the consumer and electricity supplier will begin to accrue benefits from the smart electricity meter from the point of installation. We expect on average that these earlier benefits from the smart electricity meter will outweigh the additional costs[17].

115 In addition, there would be difficulties in enforcing a fit for purpose obligation as it would require the electricity supplier to test whether a reliable 2.4GHz communications link could be established with the gas meter. Suppliers raised such concerns in their consultation responses and noted that they would seek considerable guidance on how they should test if their equipment was fit for purpose. Given that environmental and behavioural factors could influence propagation results, disputes would be likely. In the light of these economic and practical considerations, we have concluded that a fit for purpose requirement should not be introduced in advance of alternative HAN solutions becoming available.

116 In premises where a single supplier provides both gas and electricity, the installer may choose to delay the installation of a full smart system until such point in time when an alternative HAN solution is available. This approach is expected to be more cost effective, as meter reading costs for the gas meter would continue to be incurred. The additional costs for an alternative HAN solution to service the gas meter at a later date would also be incurred by the same supplier.

117 When alternative HAN solutions are available, suppliers will be able to choose the HAN solution that is most appropriate for each property. A fit for purpose requirement applied at this stage would experience the same limitation identified above. However, consideration should be given to the incentivisation of cost-effective behaviour.

[17] In line with existing IA assumptions, the additional cost of an early smart electricity installation (i.e. extra communications hub and IHD) can be offset by the benefits delivered by the electricity meter (e.g. avoided electricity meter reads for supplier and electricity consumption savings for consumer). This is the case if the gas smart meter installation occurs at least around two years after the electricity smart meter installation. Whilst this is not expected to be fulfilled in every premise, on average and across the population there is no strong rationale to prohibit the early installation of electricity meters.

118 Therefore, we propose to consult on changes to the charging methodology related to communications hubs that the DCC's CSP(s) will provide, including consideration of whether installing suppliers should pay the incremental cost of dual-band communications hubs. This consultation will form part of the wider consultation on legal drafting of the SEC. The consultation will consider if provision needs to be made for split-fuel households (for example, providing a rebate of any incremental costs to the communications hub installer), where the installing supplier may not be subject to the benefits of installing a dual-band (or single-band 868 MHz) communications hub. On the basis that there is no evidence to suggest that the installing supplier would not install the communications hub that is most appropriate for that property, we currently do not intend to introduce a rebate or make other provisions for split fuel households within the charging regime.

Government Conclusion

A fit for purpose requirement will not be pursued for now. Existing regulatory requirements should ensure that IHDs are appropriately served by the HAN solution that the supplier installs in each property. In advance of alternative HAN solutions being available, there are also economic benefits in allowing suppliers to install electricity metering systems and IHDs in properties where 2.4GHz will not serve the gas meter, and these are expected to outweigh the additional costs for additional communication hubs.

Changes to the charging methodology will be considered to ensure that it appropriately incentivises optimal outcomes (i.e. shared communications hubs and IHDs) when alternative HAN solutions are available.

Wired HAN

Summary of issue under consideration

Alternative HAN solutions will be required in properties where standard wireless HAN solutions will not work, for example high-rise flats. These solutions could encompass wireless technology only, wired technology or a combination of wireless and wired. In addition they could require additional equipment and / or infrastructure.

The consultation sought views on the proposed approach to undertake a trial with industry to explore technologies for wired HAN in properties where standard wireless solutions will not work and then to develop options for further work.

Government consideration of issue

119 The SMIP carried out a radio frequency (RF) HAN trial[18] in 2012. This identified that, without the use of repeaters or other equipment, wireless solutions were unlikely to work in some properties, particularly those where

[18] The report from this trial can be accessed at https://www.gov.uk/government/publications/availability-of-technologies-for-provisioning-home-area-network-han-connectivity-to-electricity-and-gas-metering-equipment-communications-hub-and-in-home-devices-in-cases-where-a-2-4ghz-zigbee-wireless-han-will-not-work-effectively

there are large distances and or multiple walls between the gas meter and/or IHD and the electricity meter (co-located with the communications hub).

120 The consultation asked for views on proposals to undertake a trial to examine technology options for properties where standard wireless solutions will not work. These technologies would use the existing electrical wiring in the property and were referred to as 'wired HAN' solutions.

121 A majority of respondents including energy suppliers and meter manufacturers favoured a wired HAN solution being developed as quickly as possible. In addition, many respondents suggested that potential solutions should be trialled. A number of respondents said they were willing to support such trials.

122 Some respondents also commented that a wired HAN solution was essential to avoid discrimination against consumers in buildings such as high-rise blocks of flats. One respondent noted that a wired HAN solution might find wider application beyond such buildings.

123 A small number of respondents including energy networks and communication and technology providers caveated their support for the development of a wired HAN solution with comments relating to interference with existing wired and wireless networks, propagation concerns and the need to use an internet protocol (IP) based solution.

124 Since the consultation, further work has been undertaken in relation to wired HAN. This has involved:

- an industry-led characterisation trial to measure performance of signal transmission over existing electrical wiring to determine whether a wired HAN would provide a suitable transport layer for smart metering signals. Measurements of signal passage were performed in different types of property likely to experience wireless problems - high rise flats and long low rise flats. The measured parameters included signal loss of the channel, background interference and crosstalk (interference between multiple users). These parameters are important in determining how wired HAN technologies would perform; and
- issuing an information request to explore wired HAN technologies and other solutions that could be available to address difficult buildings[19].

125 The characterisation trial was carried out in early 2013 and was led by Energy UK (EUK), supported by other stakeholders. We are very grateful for the work EUK has carried out.

126 Evidence from the trial demonstrated that high or low frequency signals can be passed along existing wiring (power cables) from a distant meter (e.g. in a basement) to the consumer's flat. The measured signal loss indicates that a number of technologies should be viable. However the trial did not examine the potential impact of the coexistence of multiple wired HAN systems and different interference sources. Further work will be needed to quantify these.

[19] an open invitation for interested parties to propose alternative technologies that may be incorporated into a HAN solution, published on DECC's website: https://www.gov.uk/government/publications/availability-of-technologies-for-provisioning-home-area-network-han-connectivity-to-electricity-and-gas-metering-equipment-communications-hub-and-in-home-devices-in-cases-where-a-2-4ghz-zigbee-wireless-han-will-not-work-effectively

127 We published the results of the trial in an information request to explore the availability of wired and non-wired technologies which could support the smart metering roll-out in buildings where standard wireless solutions would not work. Over 25 responses have been received.

128 Further work is currently being undertaken to assess these options and consider how this work should best be taken forward, and who will be best placed to lead it. Consideration will also be given as to whether any regulatory intervention is required, and if it is, what form the regulations should take.

Government Conclusion

An industry-led characterisation trial has been completed and has demonstrated that signals can pass along existing wiring in a range of different types of properties. Further information has been received from technology providers setting out a range of possible wired and non-wired HAN technologies which could support smart meter roll-out in difficult buildings.

Further work is in hand to explore these options and consider how they should best be taken forward in the future. Consideration will also be given as to whether any regulatory intervention is required, and if it is, what form the regulations should take.

Communications Hubs - Functionality

Summary of issue under consideration

The consultation sought views on the proposed communications hub functionality, including connections to the WAN and the HAN, and message handling, data storage and processing functions. Respondents were also asked to propose any additional functionality, and to set out the business case for this (Question 12).

The consultation also noted that a communications hub may be standalone, or fitted directly to the electricity meter via an 'intimate interface', and sought views on the specifications for this (Question 13).

Government consideration of issue

129 The majority of respondents were supportive of the proposed scope of communications hub functionality. A very small number of alternative views were submitted, but either did not meet existing standards and protocols, or did not advance sufficient argument to justify any move away from our position on the overall communications hub / meter design published in the April 2012 response to the Roll-Out consultation[20].

130 A wide range of responses were submitted on additional communications hub functionality. However, most of these were not supported by evidence of impact on the programme's business case.

[20] https://www.gov.uk/government/consultations/smart-metering-implementation-programme-draft-licence-conditions-and-technical-specifications-for-the-roll-out-of-gas-and-electricity-smart-metering-equipment

131 We have concluded that in addition to the functionality already set out in the Consultation Document, the CHTS will also:

- require communications hubs to support wireless firmware updates to HAN-connected devices, and the buffering of firmware upgrades for gas meters;
- mandate the ability for the communications hub to detect and record power outage and restoration events (see paragraph 156 *et seq*). ;
- mandate that the communications hub operates using a DC power supply; and
- require the communications hub to support wireless connection of Hand Held Terminals (HHTs), but not a physical interface between the HHT and the communications hub.

132 As part of our work on the CHTS, we have also considered the minimum number of devices that a communications hub should be required to support.

133 Based on our current understanding of the possible future needs of a smart meter system, the communications hub might need to support up to 16 HAN-connected devices. This reflects:

- the consultation responses to Question 29, which suggest that up to four electricity meters may be needed - one conventional and a further three for microgeneration (details at paragraph 198). In addition, a gas meter, and a gas proxy device will be required;
- analysis suggesting a need for up to five HAN-connected Auxiliary Load Control Switches (ALCS), for example one control for hot water, two for space heating circuits, one for an electric vehicle and a spare. Provision for five ALCS will provide future flexibility[21];
- an understanding that up to two prepayment meter interface devices may need to be supported, one for each of gas and electricity. The provision of PPMID is currently an option within SMETS 2; and
- provision for up to three CADs may be needed, including one In Home Device.

134 Respondents to Question 29 suggested that a move from six to eight devices would have no incremental cost; existing communications hubs available in the marketplace already have this minimum capability. They noted that a small increase beyond this number would not incur significant cost (pence, not pounds). However, they confirmed that, at some point, the requirement for extra devices will create a step-change in costs when extra processing power or extra storage is required.

135 The BEAMA Communications Hub Working Group has separately confirmed that the ZigBee chip set currently in widespread use is not limited to 16 devices. However, beyond 16 devices, its performance may degrade. To

[21] SMETS 2 requires as a minimum that an electricity meter must support at least five HAN-connected Auxiliary Load Control Switches – with manufacturers able to support more at their own discretion. This decision was based on discussion with industry representatives who demonstrated this would provide flexibility to cover existing uses as set out here, and additional capacity for future uses. In addition, one HAN-connected ALC may connect to multiple devices responding at the same time, for example two electric vehicle charging points. In parallel, we are also supporting the use of CADs. Allowing the consumer to control devices based on price signals and other triggers should also provide another route for the future flexible use of energy.

address this would require additional components at a significantly higher cost.

136 In the light of responses to the SMETS 2 consultation, and subsequent industry discussions, we have decided that CHTS will specify that a communications hub supports up to 16 HAN-connected devices.

The CHTS will provide a minimum specification for communications hubs, including connections to the WAN and the HAN, and message handling, data storage and processing functions. Communications hubs will include the ability to detect and record power outage and restoration events, and will operate using a DC power supply.

The CHTS will state a requirement for communications hubs to support up to16 devices. This is based on our current understanding of the future needs of the smart metering systems, including support for the development of smart grids.

Communications Hubs - Intimate Communications Hub Interface

Summary of issue under consideration

The consultation noted that a communications hub may be standalone, or fitted directly to the electricity meter via an 'intimate interface', and sought views on the specifications for this (Question 13).

Government consideration of issue

137 The majority of respondents felt that an intimate communications hub and electricity meter should be supported, arguing that this would reduce the complexity and thus cost of installation, and space requirements. Some responses were caveated with the statement that a standalone communications hub installation must also be supported – for example, for 'gas first' installations, and circumstances where it is not possible to install in intimate mode. A number noted that the meter and the communications hub must remain separable to allow for 'plug and play' replacement of either entity.

138 Respondents were near unanimous that a common physical interface should be mandated. They noted its design should provide for interoperability and security.

139 We consulted industry experts further on the options for an intimate interface in December 2012. Suppliers stated their expectation that between 80% and 90% of communications hubs would be installed in intimate mode. On this basis, suppliers recommended that all communications hubs should have an intimate interface.

140 We support this recommendation for the use of intimate communications hubs and electricity meters, as it is likely to introduce significant efficiencies for meter installation and maintenance. Therefore we will mandate, through the CHTS, that DCC communications hubs include intimate interface requirements.

141 Consideration was also given to whether the DCC should also be required to make a standalone communications hub available. Suppliers have indicated that a standalone communications hub would be used only in a small number of properties. In these instances the intimate communications hub and a hot shoe[22] could be used instead of a standalone communications hub.

142 While the component costs of a dedicated standalone communications hub are likely to be lower than for the combination of an intimate hub with a hot shoe, unquantified benefits are associated with supply chain simplification and field force operation efficiencies. Furthermore, a universal intimate communications hub avoids the CSP(s) from investing in (and charging for) the development of an integrated standalone hub which might only be used in very low volumes (again this benefit is unquantified).

143 We agree that a single interface specification – the Intimate Communications Hub Interface Specification (ICHIS) – should be prepared, and referenced from the CHTS. We consider that the DCC and its CSP(s) are best placed to develop and maintain the ICHIS, as they will be developing detailed communications hub designs, and will be able to undertake prototype testing of the ICHIS to ensure that the design is robust and fit for purpose.

144 In developing the specification, the DCC and CSP(s) will be required to consult with suppliers and industry. The DCC will only be able to finalise the ICHIS (and thus designate the CHTS) when the Government or Ofgem confirms that this development process has been completed. We will set these requirements out in the SEC.

145 The CHTS will require that all communications hubs are provided with an ICHIS-compliant interface. The SMETS will require that suppliers provide at each smart metering installation an electricity meter with an intimate interface or a hot shoe that complies with the ICHIS.

146 Suppliers will be required through SMETS 2 to provide a 12v DC power supply to communications hubs (either via the intimate electricity meter or the hot shoe).

147 Suppliers have confirmed that they expect to deploy the intimate option in the vast majority of cases, and we expect the components to be cheaper than previously envisaged.

Government Conclusion

The CHTS will require that communications hub include a standardised physical interface. The specification for this interface – the ICHIS – will be developed by the DCC and its CSP(s), in consultation with industry. It will be mandated for electricity meters with intimate interfaces and hot shoes, and notified as part of the second iteration of SMETS 2.

Suppliers will also be required to provide a 12v DC power supply to communications hubs (either via an intimate electricity meter or a hot shoe).

[22] A hot shoe would provide an alternative means, to the intimate electricity meter, to provide an unmetered power feed to the communications hub.

Communications Hubs – Opted Out Non-Domestic Consumers

Summary of issue under consideration

Energy suppliers have the option of operating smart meters at smaller non-domestic sites either through DCC or through an alternative operator (e.g. their own solution or that of an outsourced service provider). The consultation sought views on the Government's proposal that opted out non-domestic sites should not be required to install a CHTS-compliant communications hub (Question 15).

Views were also sought on the proposal that the registered supplier (likely to be the gaining supplier) should bear the cost of installing a new communications hub (Question 16) at opt in and opt out.

Government consideration of issue

148 The great majority of respondents agreed that CHTS-compliant communications hubs should not be mandated for opted-out non-domestic consumers. They argued that this approach will support a competitive market between Energy Suppliers on the one hand, and Meter Operators and Data Collectors on the other, which operates efficiently and facilitates the provision of energy data in a format that can better suit non-domestic consumers. Respondents noted that non-domestic consumers were not likely to be disadvantaged, particularly as well-established advanced metering arrangements are in place, and are delivering benefits.

149 Respondents also noted that non-domestic consumers are informed buyers who will have opted out in full knowledge of the consequences of this choice and mindful of any potential impact on their business. In addition, a number of respondents noted that by providing change of supplier processes and mandating that the opted-out supplier bears the costs of installation of a CHTS-compliant communications hub in cases of new supplier opt-in, the case for complexity and costly change of supplier processes is mitigated.

150 By contrast, a small minority of alternative views suggested:

- potential inefficiencies if a clear change of supplier process, and responsibilities for quick and cost effective replacement of the communications hub on opt-in, are not in place;
- that consumers without a CHTS-compliant communications hub (and possibly a HAN) will not be able to access consumption data via a CAD unless alternative capabilities are provided;
- the likelihood that a proliferation of bespoke solutions might lead to a situation where not all suppliers can support those solutions, and thus potentially weaken market competition; and
- the need to ensure non-domestic opt-outs are aware that they may be limiting the benefits of smart metering.

151 The majority of respondents agreed with the proposal that the relevant supplier[23] should bear the costs of installing a replacement communications hub. A number of respondents commented that:

- in cases of opt-out at change of supplier, a clear process and arrangements could be put in place by the DCC to levy an early removal charge on the removing (i.e. losing) supplier to recover any stranding costs; and
- clear and documented processes for removal and return of communications hub equipment to the CSP(s) should be agreed and in place.

152 A small minority of respondents disagreed with the proposed approach, principally in line with their overall opposition to non-domestic opt-out, and noting the potential impact on customer service (costs, potential disruption and loss of interoperability).

153 We consider the potential opted-out non-domestic market is likely to be an informed one. Combined with clear responsibilities for replacement of communications hubs on change of supplier, and in line with the majority views submitted in response to the consultation, opted-out non-domestic consumers will not be required to install CHTS-compliant communications hubs.

154 We will require the DCC to socialise any stranding costs resulting from the early removal of communications hubs associated with opt-out, across the non-domestic sector. In practice, our expectation is that opt-out is expected to occur infrequently, and thus the materiality of this approach is low.

155 In addition, processes are being put in place to regulate removal and replacement of communications hubs between suppliers and the CSP(s)[24].

Government Conclusion

Opted-out non-domestic consumers will not be required to install CHTS-compliant communications hubs. Procedures will be established to mitigate change of supplier cost and complexity. The DCC will socialise any stranding costs resulting from the early removal of communications hubs, and the registered supplier (likely to be the gaining supplier) will be mandated to bear the site visit costs of any requirement for a replacement communications hub.

[23] The relevant supplier is the gaining supplier at a change of supplier
[24] CSPs will also be required to recondition and recycle all communications hub (removed for whatever reason) where it is economic to do so, as set out in paragraph 355 *et seq.*

SMETS Additional Capabilities – Outage Management

Summary of issue under consideration

The detection and reporting of power outages has been identified as a significant benefit arising from the roll-out of smart meters. Under a CSP-led model for communications hub ownership, the consultation sought views on the proposal that that the design and implementation of outage reporting functionality should be assigned to the CSP(s), and documented in the CHTS (Question 17).

The consultation also sought views on the proposal that meters operated outside DCC (e.g. Foundation meters or opted-out non-domestic sites) should not be required to implement outage reporting (Question 18) as this would require additional communications links between them and the appropriate DNO.

Government consideration of issue

156 The great majority of respondents agreed that the design and implementation of outage reporting functionality should be assigned to the CSP(s). However, a substantial number caveated their responses by questioning whether this functionality should sit in the communications hub and be reflected in the CHTS, or elsewhere in the CSP's physical infrastructure, and hence not referenced in the CHTS.

157 Several respondents drew a distinction between outage detection (determining that power has stopped), and outage reporting (sending an alert in relation to outages longer than three minutes). They argued that the communications hub is the logical place to provide outage detection. However, outage reporting would require the communications hub to operate without an external power source for a short period. This would therefore require either a battery or a super-capacitor to be built into the communications hub, which would have cost implications.

158 Respondents noted that the CSP could use other elements of the CSP WAN infrastructure to deliver outage reporting. For example, the WAN infrastructure may recognise both the loss and the restoration of power to communications hubs, and thus could determine centrally, and report, when an outage has occurred.

159 Respondents who raised this concern agreed that the CSP(s) should decide on the optimum approach to outage reporting, as they would be best placed to determine the most effective solution.

160 Two respondents disagreed with the proposed scope. One did not accept the need for outage reporting, although we have previously decided that the case has been made[25]. A second believed that the meter should have responsibility for outage reporting, not the communications hub. No further evidence was provided to support either of these views.

[25] As set out in the April 2012 response: https://www.gov.uk/government/consultations/smart-metering-implementation-programme-draft-licence-conditions-and-technical-specifications-for-the-roll-out-of-gas-and-electricity-smart-metering-equipment

161 Our assessment of consultation responses has highlighted the need to draw a distinction between outage detection and outage reporting (as set out in paragraph 157). We agree that the communications hub should be capable of detecting and recording power outage and restoration information, and so have included this functionality in the CHTS.

162 We have also concluded that the CSP(s) should be responsible for outage reporting, with the provision to filter these at higher volumes to facilitate manageable delivery, but that it should be left to them to determine where best in their infrastructure this should sit (either in the communications hub or in the CSP network). Therefore the outage reporting requirements will be reflected in the SEC, and the DCC contract(s) with the CSP(s). The CHTS will not contain any mandatory requirements for outage reporting.

163 A small majority of respondents supported the proposal that meters operated outside the DCC should not be required to implement outage reporting, noting:

- the complexities of implementation (including communications arrangements), particularly across a potentially highly variable population of meters and non-CHTS compliant communications hubs;
- half-hourly meters do not support outage reporting; and
- 100% coverage of outage reporting is not required – adjacent meters will act as a 'proxy' (particularly if the opted-out non-domestic population remains at the current small percentage of overall consumers). This approach also has potential to reduce network traffic during an outage.

164 A significant minority of alternative views were received, the majority from network operators, or industry bodies, who noted:

- their preference that all meters have the capability of outage reporting such that a network operator has complete visibility of the status of a customer's supply. If the customer is opted out, suppliers should be obliged to highlight this, and ensure that they are aware that they will manually need to contact the DNO for notification of any unplanned outages;
- business customers may particularly benefit from the visibility to the network operator of an outage occurring outside normal working hours;
- a general concern over the customer experience (c.f. the operational difficulties of fault finding and service restoration); and
- in some low voltage network faults, the difficulties of confirming outages or power restorations in areas of high opt-out.

165 We acknowledge the potential complexities which may result from any requirement that all opted-out non-domestic consumers implement outage reporting. To implement this would require special (and potentially costly) arrangements to be put in place for every opted out non-domestic consumer - either via a direct interface from the smart meter operator to every DNO, and / or through individual communications arrangements direct to the DCC.

166 In addition, we note the widely submitted view that 100% coverage of outage reporting is not required. In the light of this, and the majority response to the consultation, outage reporting will not be mandated for opted-out meters.

Government Conclusion

The CHTS includes a requirement for power outage and restoration detection. The SEC will require that the DCC provides outage reporting. This will be delivered through the CSP(s) and so will be reflected in the CSP contracts. It will be for the CSP(s) to decide where in their end-to-end infrastructure this best sits. Power outage reporting will not be mandated for opted-out meters.

Interface Requirements – Consumer Access Devices

Summary of issue under consideration

An increasing number of Consumer Access Devices (CADs) are likely to become available to assist consumers in managing their energy use. On their first use, CADs need to be securely connected to the HAN in a process known as 'pairing'. Once paired, these devices will have 'read-only' access to energy usage and tariff data held in smart metering equipment.

The consultation noted that two options exist to initiate pairing. Under the locally-initiated pairing option, the consumer would initiate pairing by entering information locally e.g. via their meter. There is also an option for remotely-initiated pairing, where the consumer would initiate pairing by providing information (including information to verify that they live in the property) to a nominated SEC party - for example via an online portal or over the phone – who would then send a command to the customer's smart metering equipment via the WAN to set-up pairing.

The consultation sought to establish respondents' preferences for either option (Question 24), and if a remotely-initiated pairing option were selected, the obligations which should be placed on energy suppliers to support this process (Question 25). Finally, the consultation asked whether any other options for pairing should be considered (Question 26).

Government consideration of issue

167 A Consumer Access Device (CAD) is any device which can be connected to a customer's smart metering system via the Home Area Network (HAN). Once connected, a CAD will be able to receive 'read only' gas and electricity consumption and tariff data from smart metering devices. A CAD can then be capable of many uses:

- it may display information directly to the consumer (e.g. an enhanced IHD);
- it could act as a conduit to send the data up to the cloud (e.g. dongle/router);
- it could use the information to affect its behaviour (e.g. smart appliances); or,
- it could act as a home energy 'hub' which uses consumption and tariff data in combination with non-energy data (such as temperature or

information from motion sensors) and consumer preferences (either configurable or 'learnt') to manage energy use throughout the home.

168 A strong uptake of CADs would empower consumers, allowing them better to manage their energy use, and supporting the wider adoption of demand response technologies. A strong market for CADs could also spur innovation across the board; from design and manufacturing to new services, delivering significant benefits to consumers and to the GB economy. To enable this, it is important that consumers are able connect CADs in a way that is secure and accessible. We hope this will encourage customers to use CADs and drive opportunities for new energy management products and services.

169 In order to pair:

- the CAD must be within range of the smart metering equipment, specifically the communications hub;
- in some cases confirmation is needed that the person trying to connect a device is entitled to do so[26]; and
- information must be provided between the smart metering equipment and the CAD to identify the CAD to be paired to the HAN.

170 Pairing can be initiated by provision of information locally (i.e. the consumer inputting information into the smart metering equipment) or remotely (i.e. the consumer providing information via an internet portal or by telephone). The consultation sought views on both approaches.

171 The majority of respondents to Question 24 were in favour of remotely-initiated pairing. However, a significant minority supported locally-initiated pairing. These options are explored further below.

172 A third group of undecided respondents to Question 24 focused on the need to address the underlying technical issues (including security) before any approach to the requirement for, and provision of, a pairing service could be decided.

173 Considering Question 26, very few respondents identified other installation options for CAD pairing. Those which were raised included the inclusion of an additional HAN module in all communications hubs to support a separate consumer HAN (an option rejected in a previous consultation), potential for Near Field Communications (NFC), or a push button on all devices.

174 NFC and push buttons introduce additional security considerations, equipment costs and operating costs (additional power consumption by NFC radio). In addition an NFC solution would only be accessible to consumers with NFC compatible devices. Given that other technical options are available which do not incur these additional costs, we have decided not to include support for NFC or push buttons in the minimum requirements for SMETS 2 equipment.

[26] Remotely initiated pairing options all require the user of the service to verify that they are the Energy Consumer. Under locally initiated pairing options, where a meter is not in a shared space, in most cases access to the meter will be sufficient to verify that the person trying to pair is the relevant Energy Consumer. Where the meter is in a shared space the 'pairing function' on a meter will be protected by a Privacy PIN which will be set by the Energy Supplier and provided to the consumer.

Remotely Initiated Pairing

175 Respondents who supported remote pairing suggested that it would be the most secure option, and consistent with the process for pairing meters and the IHD on install. However, there were some concerns, particularly that remote pairing:

- would introduce one or more third parties into the system, and place an obligation of 'customer authentication' upon them;
- would take more time to establish than local pairing; and
- would introduce a need for a new, high-priority, near-real-time messaging requirement on the DCC and its Service Providers.

176 Respondents to Question 25 were evenly divided on any requirement for energy suppliers to support remote pairing, with a third group commenting but stating no preference. None of the three groups showed a bias of responses from a particular sector.

177 Those in favour of a supplier-based option noted that the supplier is the party with the existing consumer relationship - and this approach may provide an opportunity to strengthen this. They are already trusted to manage consumer data in a secure and private manner. This model has also already been shown to work in other international markets.

178 Others stated that this option placed an unbounded responsibility (including potentially increasing workload and costs) on the supplier, noting that this should be a straightforward commercial service, capable of being offered alternatively via the CSP, DSP or other SEC party.

179 Some respondents raised the concern that, if CAD services are administered by suppliers, then this may also raise issues on change of supplier and that unless additional data flows are added to the change of supplier process, then a consumer may need to re-pair devices on change of supplier. This could raise the actual and / or perceived barriers to switching.

180 We have considered all responses to the consultation, undertaken additional work to look at the available options, and looked at experience in other countries where consumers are able to pair CADs to smart metering equipment. The latter in particular shows that remotely-initiated pairing has been rolled out successfully elsewhere, and feedback from consumers who have connected CADs is that they are happy with this pairing process. One of the reasons cited is that it does not require them to interact with their metering equipment – all data entry is via a familiar interface (i.e. their computer or the telephone).

181 Having considered the options, we conclude that remote pairing will be supported. Requirements to support remote pairing will be included in the SMETS 2, the GBCS and in the CHTS. The SEC schedule of core communication services has also been updated to allow any DCC User to use a DCC service to initiate CAD pairing and de-pairing.

182 To allow consumers to pair or de-pair remotely, additional services are required prior to the issue of a DCC pair (or de-pair) command. All of these additional services could be provided by the party offering the pairing service

(e.g. CAD provider, supplier or other party); alternatively some of these services could be added to the scope of the DCC's services.

183 We are not yet in a position to identify what obligations should be placed on energy suppliers to support the pairing process. We will undertake further work[27] to identify the required supporting business services, and determine how best these could be delivered, including any options for regulatory intervention. These additional services include:

- verification of the identity of the consumer;
- a service allowing the consumer to provide information identifying themselves, their HAN and their CAD; and
- consumer support.

Locally Initiated Pairing

184 A number of respondents favoured a local pairing option. They noted that the requirement for CAD pairing is likely to increase through time. The process must therefore be quick and easy, and capable of completion without having to contact a SEC party, or needing a WAN connection.

185 However, other respondents noted that local pairing presents significant issues. These include security and the practicality for the consumer e.g. through the management of passkeys[28] and providing a simple interface e.g. keypads on CADs and a button on communications hubs.

186 Respondents also noted that allowing for local pairing would reduce but not remove the need for the DCC to undertake some activities. As examples, these include

- sending messages to reset passkeys / PINs on smart metering equipment;
- potentially offering a consumer-friendly way to view details of CADs currently connected; and/or
- de-pairing CADs.

187 We are keen to encourage as broad an uptake of CADs as possible, and to pursue the opportunity for customers to pair CADs prior to DCC go-live without having to go through their supplier. This will allow CAD manufacturers to test, trial and roll out new products to customers with SMETS 2 meters without relying on supplier cooperation or availability of a DCC service to initiate pairing.

188 Having considered the options, we conclude that local pairing should also be supported. We will work with industry and consumer experts to look at the best option for local pairing, balancing ease of consumer experience with the cost and time required for technical development[29]. The requirements to support local pairing will then be included in the SMETS and the GBCS.

---

[27] We will be inviting suppliers, CAD manufacturers, consumer representatives and others to be involved in this work and would welcome further engagement. If you would like to be involved please contact smartmetering@decc.gsi.gov.uk.
[28] A short numeric code unique to that consumer. Work is ongoing to define the required length of a passcode, but it is unlikely to exceed eight digits.
[29] As mentioned above, if you would like to be involved please contact smartmetering@decc.gsi.gov.uk

189 We will also consider what wider support for pairing could be offered, for example pairing support, and the process for customers to reset the Privacy PIN on their electricity meter if seeking locally to pair to a meter that is located in a shared space. Whilst looking at these options we will consider what impact they have on access to the market for providers wishing to provide CADs and related energy services, and links to the smart metering policy on third parties wishing to retrieve consumers' data via the DCC.

Government Conclusion

SMETS will specify that smart metering equipment must be capable of supporting both remotely and locally initiated processes to allow consumers to pair and de-pair CADs to their HAN. Requirements to support both processes will be included in the SMETS and the CHTS. They will also be included in the GBCS for 2.4GHz, and in any future Companion Specifications. No other feasible pairing options have been identified.

The SEC schedule of core communication services has been updated to allow any DCC User to use a DCC service to initiate remote CAD pairing and de-pairing. Users of this DCC service will be subject to a general requirement to verify the identity of the energy consumer from whom they have obtained permission to initiate CAD pairing, in line with good industry practice.

It is anticipated that DCC Users may need to offer additional services to support both remote and local pairing. Further work will be undertaken to determine what these services should be and who would be best placed to deliver them.

Interface Requirements – Prepayment Interface Devices

Summary of issue under consideration

A Prepayment Interface Device (PPMID) would provide functionality to facilitate the use of prepayment services by consumers whose meters are in locations which are difficult to access. The consultation sought views on the proposed scope of PPMID functionality, including the ability to add credit, activate emergency credit, and re-enable supply following remote disablement (Question 27). Respondents were also asked whether the proposals to re-enable supply via a PPMID were safe and cost-effective (Question 28).

Government consideration of issue

190 Respondents were strongly supportive of the inclusion of provisions for a PPMID (an optional smart metering device) in SMETS 2, noting that this would provide a more accessible interface to prepayment functions than that available through the meter itself.

191 One respondent suggested the interface could be achieved using a smart phone or supplier's portal. However, we consider this would not meet the needs of prepayment customers where:

- they have no access to a mobile phone or web site;
- they are without power when they need to add credit; or

- the WAN connection to the communications hub is not working.

192 Respondents queried whether credit could be transferred securely between a PPMID and the smart metering system over the HAN. The PPMID (and associated interface) will be required to comply with the overall smart metering security model. In addition, we have addressed this concern by using a 20 digit local UTRN, which meets security advice, and on which industry (including suppliers and meter manufacturers) have been consulted[30].

193 Respondents were strongly in agreement that a consumer's electricity supply could safely be re-enabled using a PPMID wirelessly via the HAN. However, significant concerns were raised over the extension of this functionality to gas. Respondents noted risks around both security and safety, and in general suggested that the provision of remote enablement for gas over the HAN would require conclusive demonstration of the safety case – although a range of example gas deployments in other parts of the world were noted.

194 Very little evidence was presented on the cost impact of PPMID provision. One respondent queried the overall case for prepayment functionality, when the costs of the additional equipment needed within the meter to support this type of tariff are taken into account alongside any requirement for PPMIDs.

195 We agree that minimum specifications should be set out for a PPMID and included in SMETS 2, and that a supplier has the option to install a PPMID conforming to SMETS 2 for a consumer with an inaccessible or hard-to-reach meter, providing that such installation is consistent with Ofgem's guidance on what is safe and reasonably practicable[31]. This will ensure a common consumer experience, and will allow a new supplier to use a PPMID installed by a previous supplier.

196 A PPMID specification is currently in development and due for inclusion in the second iteration of SMETS 2[32]. Any PPMID which meets this specification will have the capability to:

- activate emergency credit for both gas and electricity;
- enable the electricity supply; and
- display a range of pre-payment data which is also available on the meter, including the meter balance, emergency credit balance, aggregate debt and debt recovery rate.

197 The case for gas enablement has not been made, and will not be included in the current version of the SMETS.

Government Conclusion

Suppliers will optionally be able to provide consumers with a prepayment meter interface device (PPMID), which must comply with the SMETS. The PPMID will have the capability to activate emergency credit for gas and electricity, enable the

[30] A range of UTRN lengths was considered. Twenty digits was selected as this is an industry standard token length, and the minimum length which meets minimum security and business requirements. Longer UTRNs are likely to become increasingly less usable by consumers.
[31] http://www.ofgem.gov.uk/Sustainability/SocAction/Publications/Documents1/Modification%20Direction.pdf
[32] If you would like to be notified when the PPMID specification is available, please contact smartmetering@decc.gsi.gov.uk

electricity supply when the supply is armed, and display a range of pre-payment data which is also on the meter.

Interface Requirements – Microgeneration Meters

Summary of issue under consideration

A SMETS-2 compliant electricity meter could be used as a microgeneration meter – measuring energy generated by small-scale renewable technologies such as photovoltaic cells. The Government proposed that CHTS-compliant communications hubs should support multiple SMETS-compliant electricity meters (Question 29). This would provide the capability to link microgeneration meters into the HAN as and when DCC develops elective services to support them. Respondents were also asked how many smart electricity meters a communications hub might be required to support.

Government consideration of issue

198 The great majority of respondents confirmed that communications hubs should be capable of supporting multiple smart meters, arguing that this is essential to enable the industry to deal with an increasing range of microgeneration deployments. Only one respondent disagreed with the proposed approach, arguing for a single meter per hub on the grounds of cost and complexity.

199 The question about how many meters should be supported was deliberately open, and encouraged a wide range of responses, from zero to unlimited. Two broad groupings emerged: the great majority of those who responded were in favour of no more than four meters–per-hub, and based this on current market / operational experience. The remaining respondents favoured between eight and an unlimited number of meters.

200 No respondent directly mentioned cost as the deciding factor, the main concerns being the practicalities of implementation on the ground, and the typical number of meters found in consumer premises.

201 We have considered the responses and concluded that a communications hub should support at least four electricity meters. This has been reflected in the CHTS. This aligns with current business demands and provision, and the BEAMA Communications Hub Interest Group has confirmed that this can be achieved by the majority of equipment available today, and so is broadly cost neutral.

202 Furthermore, it should provide for significant future flexibility in the support offered to households. The communications hub will be able to support up to 16 devices and with the exception of the one channel which has to be 'reserved' for the gas proxy device, the mix of devices is fully interchangeable (within the total processing power). This approach maximises future flexibility and provides the customer with considerably more choice on the smart home functions they take up.

203 It should be noted that microgeneration meters will only be supported after the Feed In Tariff (FIT) registration data becomes available to the DCC, as described in the SMETS 2 consultation. The decision set out here to support four devices is a technology enabler, rather than a complete solution.

Government Conclusion

The CHTS will specify that a communications hub must support a minimum of four electricity meters, in order to support an increasing range of microgeneration deployments.

Interface Requirements – Handheld Terminals

Summary of issue under consideration

Energy suppliers have suggested that handheld terminals (HHT) could support their meter installation processes, or be used to configure meters where there is no WAN connection (temporary loss of WAN service or areas of no WAN coverage). In suggesting this they also noted that a standard HHT interface to the HAN should be specified to achieve interoperability.

The consultation sought views on the need to specify an HHT interface to the HAN, the functions it would need to support, and the scenarios under which it would be used (Question 30).

Government consideration of issue

204 The great majority of respondents supported the specification of an HHT interface to the HAN. A small minority disagreed, principally on the grounds of potential security issues, and also arguing that more efficient and cost effective ways of installing smart meters were available (although they did not set these out).

205 A wide range of possible functionality was suggested, and the scenarios under which it would be used. As a broad summary, there was strong support for the following:

- a capability to support installation processes with the PPMID where the WAN is not present;
- a capability to support maintenance processes with the HHT where the WAN is not present; and
- the provision of an interoperable interface to all SMETS equipment through the communications hub.

206 We have considered possible options for supporting installation and maintenance processes where no WAN is present. We note that the same processes would also be possible when the WAN is available, though maintenance and installation functions may be more efficiently performed through local HHT support, rather than through the WAN. In all cases, we note that:

- any solution must not compromise system security; and

- a requirement that all actions performed on the smart metering equipment are authorised by the supplier.

207 Interfaces to smart metering equipment will be defined in the GBCS for 2.4GHz-based solutions.

208 We have concluded that:

- the communications hub will support a HHT interface; and
- the interface will support the delivery of commands from the supplier, with the same security requirements for signing as commands delivered through the WAN.

Government Conclusion

An HHT interface to the HAN will be specified in the CHTS and the GBCS. It will be capable of supporting connections to the HAN for 'pass-through' of all supplier commands.

4. Governance and Assurance of Security

209 Security objectives are relevant to all parties, even though their own responsibilities may be restricted to particular installations or areas of operation. For example, at change of supplier, the gaining supplier will inherit devices procured by the losing supplier and all users of DCC's services will be reliant on its systems and processes.

210 The consultation sought views on how security requirements should be governed, and the regimes that will be required to provide appropriate levels of assurance.

211 Our conclusions set out in this section relate only to the period following commencement of DCC services. Security in the period prior to this milestone was the subject of a separate consultation[33], the response to which was published in December 2012, with new supplier licence conditions for security coming into effect in March 2013[34].

Governance of Security Requirements

Summary of issue under consideration

Smart metering security requirements will need to be reviewed and modified over time to reflect changing circumstances. The consultation sought views (Question 31) on the Government's proposal that the maintenance of smart metering security requirements will best be performed by a technical sub-committee to the SEC Panel, comprising security specialists from Government, industry and other interested parties, and drawing on input from SEC parties. Respondents were also invited to propose any alternative arrangements, supported by appropriate evidence.

Government consideration of issue

212 Respondents across all stakeholder groups were broadly supportive of the proposed approach to the governance of security requirements; only one respondent disagreed.

213 Respondents expressed general agreement for the creation of a technical sub-committee (proposed to be known as a Security Sub-Committee) to maintain security requirements, with a number providing recommendations relating to the governance of the SEC Panel and Security Sub-Committee. In some cases this extended to suggested membership of the panel.

[33] https://www.gov.uk/government/publications/smart-metering-licence-conditions-for-consumer-engagement-strategy-data-access-and-privacy-monitoring-and-evaluation-and-security-risk-assessments-and-audits-in-the-period-before-the-dcc-provides-services

[34] https://www.gov.uk/government/consultations/smart-metering-security-risk-assessments

214 Two small suppliers expressed concerns over the financial implications of the proposed approach, asking that consideration be given to the running costs of the panel and the benefit that the panel would provide.

215 Given the dynamic risk landscape, the security requirements developed by the SMIP and transcribed into the SEC will need to be kept under review to ensure they remain proportionate to the risks and meet the wider objectives of the SEC. We consider that this role would be best achieved via the proposed Security Sub-Committee.

216 In order to maintain the right balance between the risks to the smart metering system and the obligations placed on SEC parties, we propose to give each member of the Security Sub-Committee the right to raise modifications to the security arrangements in the SEC. The Security Sub-Committee will also be tasked with assessing the impact of proposed SEC modifications to the security arrangements and advising the SEC Panel accordingly.

217 To inform the need for any changes to code modifications to accommodate new or changed security threats and requirements, ensuring that these are appropriately balanced against SEC objectives, the Security Sub-Committee will:

- monitor the threat landscape to identify emerging privacy and security threats;
- maintain the end-to-end smart metering system risk assessment to identify new or changed security risks;
- maintain a set of security requirements that seek to mitigate risks to the end-to-end system that have been identified in the risk assessment; and
- maintain a risk treatment plan.

218 The wider responsibilities of the Security Sub-Committee will also include:

- assisting DCC and DCC Users with determining the cause of security incidents, in a non-operational capacity; and
- assisting the SEC Panel with the resolution of technical disputes in relation to compliance with the security requirements between SEC parties.

219 Membership of the sub-committee will be drawn from security experts of SEC Parties including the DCC. It is proposed that there will be a seat for a DECC representative with specific responsibilities to be defined. The Committee will also be able to call on technical expertise from other relevant non-SEC Parties (e.g. meter manufacturers) as required, and will be overseen by an independent chair. We plan to consult separately on the legal drafting for the SEC, which will discuss our proposal for establishing this sub-committee, including its membership.

220 Given its responsibilities and the likely size of this new sub-committee we expect the annual running costs to be in the region of £500,000. This covers remuneration for the chair, time of participants (preparation and attendance), reimbursement of travel costs for attendants, procurement of external experts' advice as well as an allowance for resourcing the continual oversight roles of the committee (e.g. maintaining the end-to-end risk assessment). The SEC Panel will decide on the membership of the Committee, based on the need to

provide the appropriate level of technical expertise. The SEC Panel will also decide its governance arrangements.

221 In addressing small suppliers' concerns over the cost implications of the proposed arrangements, it needs to be recognised that the responsibility for security risks will be shared amongst the various bodies participating in smart metering. As the security arrangements in the initial SEC will be subject to change, all SEC parties will have an interest in ensuring that they remain fit for purpose. Therefore we consider that the running costs reflect the important role that this sub-committee will play in ensuring that the enduring security arrangements continue adequately to protect the system against new threats and are proportionate to the risk.

222 The SEC Panel will be responsible for ensuring that arrangements under the SEC continue to be efficient. This includes keeping under review the arrangements for the operation of Security Sub-Committee.

223 We plan to consult separately on the legal drafting for embedding these arrangements into the SEC.

Government Conclusion

A Security Sub-Committee will be created under the SEC Panel to keep security arrangements under review and consider whether they continue to be appropriately balanced against the SEC objectives and the wider threat and risk landscape. This approach will allow the security arrangements to reflect changing circumstances and provide effective coverage of evolving risks.

We will consult further on the legal drafting for embedding the arrangements for the Security Sub-committee into the SEC.

Assurance of Security Requirements

Summary of issue under consideration

When DCC is operational, security of the end-to-end smart metering system will rely on components supplied by a number of different parties. The consultation proposed that independent assurance procedures be put in place to demonstrate that elements of the solution have achieved a known level of compliance with published security requirements. This would include a requirement for re-testing of DCC, and DCC Users' systems, at set intervals, and also when significant changes to systems or to security requirements are introduced.

Views were sought on the proposed approach (Question 32), including cost estimates. Comments were also invited on the impact and benefits of the proposed approach on small suppliers.

Views were also sought on the proposed approach to re-testing (Question 33).

Government consideration of issue

224 The majority of respondents were supportive of the proposal to establish independent assurance procedures for DCC and DCC Users[35] noting that it would provide an important level of consistency when demonstrating compliance, whilst instilling confidence in the security of the wider smart metering system.

225 While the respondents offered support for independent assurance, they expressed mixed views on the use of both time and event-based testing. Several respondents were content with annual re-testing, but meter manufacturers and some energy suppliers in particular favoured an approach which based the frequency of testing on pre-determined criteria or a risk assessment. Other respondents suggested that re-testing should only be required in response to significant changes.

226 Responses addressing the proposed independent assurance arrangements tended to focus on DCC Users. However a small supplier expressed concerns over the potential costs of independent assurance regimes.

227 A minority suggested that an annual supplier self-assessment should be sufficient where there had been minimal change to previously-certified systems and processes, and the commensurate levels of risk did not justify the additional costs of time-based testing. Some respondents noted that the proposed intervals and the term 'significant change' needed to be defined.

228 Addressing the consultation's proposals that DCC Users be independently assured on a role-based approach, a number of stakeholders, including large energy suppliers, were concerned that this might result in reduced security obligations for smaller suppliers. Some respondents felt that a role-based approach in isolation was inadequate but did not provide evidence to support this position. Other respondents questioned whether there was a discernible difference between the role-based and risk-based approaches.

229 Due to the interconnected nature of the smart metering system, each SEC Party will want assurance that other parties are compliant with their security obligations and are operating secure systems. The use of independent assurance schemes provides a common and consistent set of arrangements to assess and monitor compliance of the DCC and DCC Users. Having such arrangements in place will provide confidence that the appropriate security controls have been implemented and that the end-to-end smart metering system is secure.

230 To demonstrate the DCC's compliance with its security obligations, we will use the Service Organisation Control 2 (SOC2[36]) standard. SOC2 is the reporting standard typically used by providers of outsourced services to give assurance to their service users that security obligations have been fulfilled in line with the service user's expectations. In the context of smart metering, a SOC2 report will provide assurance to DCC Users that the DCC has deployed

[35] DCC Users include any one of three categories: Energy Suppliers, Network Operators, or other DCC Users as defined under the SEC

[36] The Service Organisation Control 2 (SOC2) standard, as defined by the AICPA until such time that the equivalent ISAE standard is in place.

effective controls which appropriately mitigate security risks and maintain compliance with security obligations. SOC2 is a widely recognised standard and will avoid the potential need for each DCC User to perform separate audits of the DCC.

231 The SEC Panel (advised by the Security Sub-Committee) will be responsible for setting the scope of the SOC2 audit. It is considered that this group will be best placed to represent the interests of the stakeholder community. The DCC will be responsible for communicating the scope of the assurance exercise to its Service Providers to allow them to provide the evidence required by a Competent Independent Organisation (CIO) to complete the assessment and prepare the SOC2 report.

232 SOC2 reporting costs for the DCC and its Service Providers are expected to be in the region of £250,000 per report, with one report anticipated per annum.

233 Recognising that it is more efficient for non-compliance to be identified and addressed prior to a system being implemented, arrangements will also be put in place to ensure that SEC Parties are provided with assurance during the initial design, build and test phases of the DCC's systems. DCC's compliance with its security obligations will provide SEC Parties with confidence that the appropriate security controls have been implemented. Taking advice from the security expertise at its disposal, the SEC Panel will be responsible for setting the scope of this work.

234 Under the approach for assurance of DCC Users, each user will be required to conduct an independent security assessment against a security controls framework that will be tailored according to their SEC role code[37]. This approach will enable the assessment to be proportionate and tailored to the capabilities of DCC Users, and avoid a generic approach that would potentially subject some DCC Users to a disproportionate assessment.

235 Addressing the issue of the difference between a role-based and risk-based approach, we are of the view that the different DCC User roles will have different degrees of risk. For example, the ability to issue a supply disablement command is a function of an entity's SEC role code. Parties that can perform such a command present a greater level of risk than those whose role code does not permit this. By adopting a role-based approach, the assessment will be tailored to the capabilities of DCC Users and, therefore, the risks they pose to the system.

236 We consider that a purely risk-based approach would require DCC Users to comply with a set of security obligations in accordance with predefined risk criteria. Thresholds would need to be built into this model to ensure that the necessary obligations were proportionate to the size and capabilities of the DCC User. However, this could result in DCC Users purposely limiting their operations to within a particular boundary to avoid compliance with an alternative set of security obligations. For example, any supplier who inherits a significant volume of new customers over a short time period may be

[37] Under a role-based approach, DCC users would be subject to a targeted assessment, based on their powers and obligations under the SEC, as indicated by their 'role codes' (e.g. energy supplier, network operator, authorised third party).

required to comply with an extended set of obligations for which they are not prepared.

237 Every SEC party has an interest in making sure that other parties are compliant with their security obligations. Accordingly, there is a need for a central body to represent the views of the broader stakeholder community. Mirroring the arrangements for DCC security assurance, the SEC Panel (with advice from the Security Sub-Committee) will assume the responsibility for this role.

238 We anticipate that the costs associated with these assessments will be proportionate to the size of both the DCC Users' smart metering systems, and the rights and capabilities associated with their SEC role code. Drawing on available evidence about similar security audit requirements we expect the cost per assessment, per organisation, to range between £10,000 and £15,000. This includes time for planning, onsite and offsite evidence review, and the completion of the report.

239 There is a risk that the longer systems are in use, the greater the chance that new threats to these systems will emerge. This reflects a wider trend that suggests technologies such as smart metering systems can be susceptible to compromise as the capabilities of attackers improve over time. Re-assessment at set intervals will ensure that DCC and DCC Users continue to operate securely, and that systems are protected against emerging threats and vulnerabilities.

240 With regard to the length of time between re-assessment, the SEC will require both the DCC and DCC Users to be reassessed annually to provide confidence that emerging security weaknesses are identified and treated in a timely manner. For DCC Users an assessment demonstrating compliance with security obligations will first be required as part of the DCC User Entry Process.

241 An annual assessment is considered proportionate given that many of the DCC and DCC User systems that will form part of the end-to-end solution will be newly commissioned, and are likely to face a range of new and emerging threats. The option to amend this time period through a modification to the SEC is available should this be deemed appropriate in the future.

242 In discussions with the SMIP, large and small-sized DCC Users both set out their expectations that annual assessments of this nature would be conducted alongside their existing annual financial audits, therefore potentially realising cost savings. Similarly for the DCC, the annual SOC2 report should align with other independent audit processes (for example, statutory audits) that the DCC will need to support. Thus there is potential to realise economies of scale, reducing the resource cost of this annual exercise.

243 Using knowledge of their internal environments, individual DCC Users, and the DCC, are best placed to determine when they are making a significant change to their systems, as a result of a change in security requirements or otherwise. Both the DCC and DCC Users will require suitably designed internal security assurance arrangements to be in place to ensure compliance with the SEC is maintained when system changes are made.

244 Independent security assurance as a result of changes to systems or to security requirements is not considered proportionate, with subjecting the DCC and DCC Users to an annual independent security assurance considered to be sufficient to provide SEC Parties with the confidence they require that systems remain compliant over time.

245 Further detail on how these arrangements will be realised in regulation will be provided in a consultation on the legal drafting for the SEC.

Government Conclusion

The DCC and DCC Users will be subject to independent assurance processes. For DCC Users, security assurance will be dependent on their SEC role code, whereas DCC will be audited in accordance with SOC2. The DCC and DCC Users will be subject to time based testing.

This approach will provide confidence of compliance with security controls and that emerging threats are being appropriately managed in accordance with security good practice.

Further detail on how these arrangements will be realised in regulation will be provided in a consultation on the legal drafting for the SEC.

Independent Assurance of Smart Metering Equipment

Summary of issue under consideration

An independent security certification regime will be needed to provide assurance that SMETS 2 equipment capable of enrolment into the DCC complies with the smart metering security requirements. The scheme would be set up by the SMIP, with any subsequent modifications governed through the SEC. The scheme could also be leveraged to assess whether SMETS 1 meters meet the security requirements, and are thus eligible (on the grounds of security criteria) for enrolment into the DCC.

Views were sought on the proposed scheme, including the likely costs and timelines, both for set up and for submission of equipment for security certification (Question 34).

Government consideration of issue

246 The majority of respondents agreed with the proposal to establish an independent security certification scheme for smart metering equipment. Broadly, respondents recognised that the proposed approach was reasonable and would provide a consistent standard of security for SMETS 2 equipment.

247 Whilst in agreement with the overall proposal, two meter manufacturers were concerned about the impact of using The National Technical Authority's (CESG) Commercial Product Assurance (CPA) scheme (provided as an example of the type of equipment certification scheme we are considering) given it would require testing against security characteristics that have yet to be developed. Other points raised included:

- whether existing certification schemes (such as the Common Criteria Protection Profile developed by the German Federal Office for Information Security) could be leveraged;
- that certification should not be limited to a one-off process;
- the expected cost of certification;
- that assuring independent components of the smart metering system was inadequate, and consideration should be extended to end-to-end testing of the overall solution; and
- how the suggested certification scheme might be used to assess the eligibility of SMETS 1 meters for enrolment in the DCC.

248 Respondents were also concerned that an adequate number of CESG-approved test houses, which would be used to provide CPA certification testing, be available. Too few could result in delays to the certification of equipment, owing to supplier demand. A wider range of test houses would allow competitive and skilled services to be procured. One respondent suggested that existing manufacturer certification processes should be used in preference to independent test houses.

249 Smart metering systems will rely on components from a number of different entities and suppliers. We consider it paramount, therefore, that an effective independent security assurance regime is in place to enable a consistent approach to security across smart metering equipment. This will provide the necessary confidence to smart metering stakeholders that a unified level of security is being achieved by smart metering equipment.

250 Accordingly the CESG's CPA – Foundation Level scheme has been selected as the means for providing assurance to smart metering stakeholders that SMETS and CHTS equipment is compliant with security requirements. We consider that as all equipment should be capable of being enrolled in DCC in a consistent way, the requirement for CPA certification should be embedded in SMETS 2 and the CHTS.

251 In terms of the equipment that will be subject to the CPA – Foundation Level scheme, Type 1 devices[38], if compromised, have the potential to impact smart metering systems as they are relied upon to enforce specific security controls in the end-to-end architecture and will have the ability to issue commands to other devices on the HAN.

252 By comparison, Type 2[39] devices are effectively 'read only' devices as they are unable to issue critical commands to other devices on the HAN. They are also not relied upon to enforce security controls in the end-to-end architecture. As such, they are considered to have a lower potential capability to impact the security of smart metering systems.

253 We consider, therefore, that Type 1 devices should be subject to CPA – Foundation Level security certification. Type 1 devices comprise:

- Gas Smart Metering Equipment (GSME);

[38] A device connected to the HAN that is allowed to issue or perform a range of HAN Interface Commands and can access the information stored in Gas Meters, Electricity Meters, or a Gas Proxy device.
[39] An IHD or any other device connected to the HAN that provides consumer access to the information stored in Gas Meters, Electricity Meters, or a Gas Proxy device.

- Electricity Smart Metering Equipment (ESME);
- Communications Hub;
- Gas Proxy Device (GPD – part of the Communications Hub);
- Pre-Payment Interface Device (PPMID); and
- HAN Connected Auxiliary Load Control Switches (HCALCS).

254 By comparison with other certification schemes, we consider that the CPA scheme provides the flexibility to be tailored to meet the requirements of the GB smart metering model. Furthermore, the development of the regime will enable a proportionate level of security assurance to be achieved in accordance with the risk profile of SMETS and CHTS equipment.

255 We recognise respondents' concerns that it is difficult to assess the suitability of the tests which are yet to be defined. We have appointed a CESG accredited test laboratory to develop the smart metering Security Characteristics, in collaboration with a specialist stakeholder working group comprising industry security experts, and we will continue to engage with industry and CESG in developing appropriate test criteria.

256 Other schemes do not reflect the unique characteristics of the GB smart metering deployment. However, the smart metering Security Characteristics will take into account evidence from existing equipment certifications and industry best practice standards (such as FIPS 140-2 and Common Criteria).

257 CESG is committed progressively to align the CPA scheme with the Common Criteria scheme. This should provide confidence to the wider stakeholder community that every effort has been made to ensure CPA certification is a holistic process, and avoids duplication of existing certification achieved through other recognised schemes.

258 We are in dialogue with CESG to ensure that an adequate number of test houses are available for smart metering equipment certification. In addition, we expect the number of CPA registered test houses to increase in accordance with market demand.

259 We have considered the concern that testing of independent components will not assure the end-to-end smart metering solution. Independent assessment of the DCC and DCC Users is designed to provide assurance of the wider smart metering system, whilst independent certification of equipment will assure specific components of the solution. This holistic approach to assurance will ensure a consistent level of security is achieved across the end-to-end smart metering system.

260 It is recognised that within the lifetime of a smart device there are likely to be changes to the external threat landscape and to the devices themselves. As smart metering systems will rely on services and components from a number of different entities and manufacturers, we consider that a robust assurance regime should be developed that allows for focused re-testing around significant areas of the equipment that have changed (i.e. event-based testing).

261 Event-based re-testing will be required in response to a material change to the Security Characteristics, as a result of changes in the external threat

landscape (e.g. the discovery of a new method of attack), or where the manufacturer has made a significant change to a device.

262 When making a change to a device, the manufacturer would refer to their 'Assurance Maintenance Plan' (AMP) agreed between the manufacturer and the CESG Test Lab when the device was originally certified. The AMP defines the components and manufacturing processes considered as vital for security (e.g. the cryptographic routines) that, if changed, could present a risk to the security of the device and therefore end-to-end smart metering system. The AMP enables the manufacturer to understand whether a change is regarded as 'significant' and would require event-based re-testing (i.e. recertification).

263 Routine changes (e.g. changes the layout of the digital display) which do not significantly impact the security of the device are assured through a 'Build Standard' certification for each equipment manufacturer, which attests to the manufacturer's competence in manufacturing and maintaining equipment to a secure standard. Routine changes do not require the product to be recertified.

264 In addition to event-based testing, we are considering what periodic re-testing is required. The default CPA – Foundation Level scheme requires periodic re-testing to ensure that all changes to the equipment (routine and significant) made in that period are assessed against the latest Security Characteristics. Time-based testing focuses on the product as a whole, rather than a subset of the device affected by a significant change. The Test Lab would re-assess the manufacturer's compliance with the Build Standard, and re-validate whether the device still satisfies the Security Characteristics, and is therefore protected from emerging threats.

265 Time-based testing provides assurance to the wider smart metering community that equipment continues to be compliant with the relevant CPA Security Characteristics and that the manufacture remains compliant with the Build standard.

266 Under the current arrangements for the CPA – Foundation Level scheme, the CESG default is for equipment to be recertified every two years to remain as a 'CPA certified' device. However, we are discussing the proposed time period with industry to understand whether two years is appropriate for smart metering.

267 Having evaluated the available options for equipment certification (including Common Criteria) we consider that the CPA scheme will provide a cost effective, flexible and proportionate certification regime to meet the security assurance requirements for smart metering deployment. We expect the cost for a first certification of a unique piece of equipment to be in the range of £30,000 to £50,000.

268 Subsequent re-certifications (i.e. time and event-based re-testing) are generally expected to incur lower costs, ranging from £5,000 to £50,000, depending on the nature of the change for time or event-based recertification, or how the equipment and the manufacturing organisation have developed since CPA certification was first achieved. This recognises that changes may

have been made to the device that did not qualify under the AMP, but still need validating as part of the time-based assessment.

269 If the manufacturer continues to operate to the same engineering and product development principles, and the device remains largely unchanged since it was last certified, the cost associated with recertification is expected to fall towards the lower end of the scale. If, on the other hand, significant changes have been made to either the product or the principles, the cost of recertification may reach the upper end of the scale to reflect the need for a more involved assessment.

270 The approach to enrolling SMETS 1 equipment is set out in our response to the consultation on the Foundation Smart Market, published on 10 May 2013[40].

Government Conclusion

A mandatory CPA security certification scheme for Type 1 SMETS 2 equipment will be established. Recertification will be required periodically in accordance with the requirements of the CPA scheme or in response to a significant change. We will discuss further with industry whether the default of two yearly re-certification is appropriate for smart meters.

Non-Compliance with Security Requirements

Summary of issue under consideration

As failure by one SEC Party to comply with security requirements could cause others to incur loss and the consultation proposed that sanctions should be applied to the non-compliant party, including withdrawal of DCC services to a DCC User or to specific devices.

Views were sought on the inclusion of such sanctions within the SEC, and on the nature of sanctions which might be imposed (Question 35).

Government consideration of issue

271 The majority of respondents expressed broad support for the introduction of specific sanctions for non-compliance with security requirements.

272 Respondents suggested that the way in which sanctions are applied should be transparent and encourage self-disclosure. The impact on the consumer should also be considered before a sanction is applied. A number of stakeholders also emphasised that speed of remediation could also be considered as a factor in determining the sanction imposed, whilst others suggested that sanctions should be hierarchical, with revocation of DCC services being the final and most extreme option.

[40] https://www.gov.uk/government/consultations/smart-metering-implementation-programme-foundation-smart-market

273 A small number of respondents requested that matters relating to compliance with other legislation, such as the Data Protection Act 1998, should not be subject to sanctions under the SEC.

274 Alongside the SMETS 2 consultation, we sought views on the sanctions framework through the SEC Stage 1 consultation[41]. The majority of respondents to this and the SEC Stage 1 consultation expressed broad support for the introduction of specific sanctions in events of non-compliance with SEC obligations. However, a small minority of respondents to the current consultation disagreed with the proposal to have specific sanctions for non-compliance with the security requirements, noting that sanctions were unnecessary if certification was performed correctly.

275 We consider that specific sanctions applied in an event of non-compliance with the security requirements over and above any resultant liabilities are necessary to discourage default, encourage prompt rectification and prevent reoccurrence of the breach. While the certification requirements will play a vital role in ensuring compliance, breaches of the security obligations should attract appropriate sanctions, in line with procedures to address breaches under standard contractual arrangements, and with how non-compliance is dealt with in other industry codes.

276 The November 2012 response to the SEC Stage 1 consultation set out the available sanctions, which include the ability to suspend any Party's rights to participate in SEC governance arrangements, and to receive core, elective or enrolment services from the DCC. In extreme cases, persistent and material non-compliance could lead to expulsion from the SEC.

277 Because breaching security requirements may affect the security of the system, material breaches of the security requirements should attract appropriate sanctions. We consider that the same sanctions as those discussed in the SEC Stage 1 consultation response are adequate to discourage non-compliance with the security requirements.

278 We agree that when applying sanctions, due consideration should be given to the possible consequences discussed above. In order to ensure transparency and proportionality of the way in which sanctions are applied under the SEC, to encourage self-disclosure and prompt rectification, the SEC Panel should be able to use its discretion when applying sanctions.

279 In an event of a breach, Ofgem would also need to decide whether to take further action to enforce compliance with any relevant conditions of a licence.

280 The SEC will contain a number of obligations which SEC parties will need to comply with insofar as it relates to the relationship between the DCC and DCC Users. Matters subject to compliance with other legislation, such as the Data Protection Act 1998, will be dealt with by appropriate bodies responsible for administering the relevant legislation, in this case the Information Commissioner's Office.

41 https://www.gov.uk/government/consultations/stage-1-of-the-smart-energy-code

Government Conclusion

Sanctions for non-compliance with security requirements will be provided in the SEC. These are likely to be proportionate to the materiality and severity of a breach, and could take into account both remediation of security issues, and the impact on consumers, before they are imposed.

Security for Smart Meters Not Enrolled in the DCC

Summary of issue under consideration

Even after the commencement of DCC services, smart metering systems will continue to be operated outside DCC, for example opted out non-domestic sites and SMETS meters awaiting enrolment to DCC. To reflect that the responsibility for end-to-end security of these lies with energy suppliers, the consultation proposed that security obligations be set out in licence conditions or the SEC. This would effectively extend the arrangements already proposed for smart metering installations during the period before DCC provides services. These require suppliers to carry out a number of recognised industry good practice disciplines for identifying and managing risks to the security of their systems.

Views were sought on the proposal to extend the arrangements already in place, to provide evidence of the costs which might be incurred, and of the impact on small suppliers (Question 36).

Government consideration of issue

281 The majority of respondents agreed that security-specific obligations should be placed on non-domestic suppliers operating SMETS equipment outside of the DCC. Some noted that this would promote standardisation across installations and benefit interoperability. Others highlighted that the reputational risk of a security breach involving smart metering equipment, would be the same, irrespective of the operator of the equipment, thus reinforcing the case for consistent security obligations.

282 Two respondents set out an overlapping view that smart meters that were operated outside DCC needed to be secure, but posed little risk to the market. Therefore the approach should be proportionate in order to provide sufficient protection, but not to impose unnecessary security burdens on the non-domestic sector in response to challenges faced by the domestic sector. Any requirements should also not restrict access to consumption data, as this will be core to the on-going provision of competitive energy services.

283 A number of meter manufacturers and large energy suppliers asked that the scope of the proposed arrangements be clarified, with many suggesting that suppliers operating non-SMETS equipment outside of DCC should not be subject to any smart metering-specific assurance obligations. Others proposed a tiered approach to the security arrangements, with security obligations being dependent on level of risk that each party poses to the wider smart metering system.

284 A minority of respondents disagreed with the proposed approach, suggesting that:

- it was of little apparent benefit;
- the consultation was premature in its engagement of stakeholders before the certification processes were fully established; or
- the proposal would result in the retrofitting of security requirements to non-SMETS 2 equipment.

285 We agree that in order to support interoperability and protect the interest of consumers, a consistent level of security, proportionate to the risk is essential across the smart metering system. Accordingly, we are of the view that the suppliers who have opted out of enrolling their smart metering systems with the DCC should develop their own detailed security arrangements proportionate to the risk. However to make sure that they achieve a consistent level of security, the development and implementation of their arrangements needs to be supported by high level principles relating to the security of their systems.

286 These high level principles are likely to require suppliers to carry out a number of recognised industry good practice disciplines for identifying and managing risks to the security of their systems.

287 Because breaches of the high level security principles are likely to have a material impact on the consumer due to their broadness, we consider that they should be dealt with by Ofgem. Therefore we conclude that placing these high level security principles on the face of the licence, rather than the SEC, will achieve this outcome. This approach will enable suppliers operating SMETS equipment outside of DCC to achieve risk-based solutions, and is likely not to impose an unnecessary financial burden on them. This in turn will achieve a better outcome for the consumers.

288 Placing security licence obligations on energy suppliers operating SMETS equipment outside of the DCC will, in effect, extend the arrangements that have been put in place for the Foundation Phase (i.e. Smart Metering Licence Conditions for Security Risk Assessments and Audits in the period before the DCC provides services[42]).

289 For opted-in suppliers, we are developing a set of detailed security requirements that will be transcribed into the SEC and be subject to SEC governance. To reflect and underpin the detailed security requirements, we are minded to place a specific obligation on suppliers in relation to the security of their smart metering systems, through a new licence condition. This condition would reinforce the responsibility for suppliers to maintain the security of their smart metering systems in the event that a deviation existed against security provisions in the SEC.

290 We will consult further on the content of the enduring licence conditions for both suppliers operating SMETS equipment outside and within the DCC.

[42] https://www.gov.uk/government/publications/smart-metering-licence-conditions-for-consumer-engagement-strategy-data-access-and-privacy-monitoring-and-evaluation-and-security-risk-assessments-and-audits-in-the-period-before-the-dcc-provides-services

291 There will be no requirement to apply CPA equipment certification to SMETS1 equipment.

292 The approach to enrolling SMETS 1 equipment is set out in our response to the consultation on the Foundation Smart Market, published on 10 May 2013[43].

Government Conclusion

All suppliers will have security-related obligations. The obligations on the suppliers operating SMETS equipment outside the DCC will be based on high level principles and will be set out in the licence, while those suppliers that enrol smart metering systems with the DCC will have detailed security obligations in the SEC, supplemented by a general licence obligation to maintain the security of their systems.

We will consult further on the content of the enduring licence conditions.

[43] https://www.gov.uk/government/consultations/smart-metering-implementation-programme-foundation-smart-market

5. Assurance of Smart Metering Equipment Interoperability

293 Many participants including energy suppliers, communications service providers and meter asset providers, will play a role in the procurement and deployment of smart metering equipment. It is in the interests of all parties that equipment from multiple manufacturers interoperates seamlessly within customers' premises so that equipment does not have to be replaced, adding cost and creating disturbance for customers.

294 The consultation sought views on how interoperability requirements should be governed, and the arrangements that will be required to provide appropriate levels of assurance of compliance with these requirements. This includes the inter-changeability of certified equipment between suppliers and the interoperability between DDC Users, the DCC and equipment.

Summary of issue under consideration

While the roll-out licence conditions require that all smart meters comply with SMETS and the DCC will be required to provide communications hubs that comply with the CHTS, the consultation proposed that equipment should also be certified against the GBCS.

The consultation also proposed that an 'approved products list' of equipment that has been GBCS and CPA certified should be maintained by the SEC Panel. The DCC would only enrol equipment that was on the approved product list.

Views were sought on the role of interoperability and the governance arrangements most appropriate to ensure smart metering equipment compliance (Question 37). Comments were invited on the proposal to introduce an 'approved products list' (Question 38), and on the proposed protocol certification (against the GBCS), and any additional assurance testing which might be required (Question 39).

Government consideration of issue

295 A large majority of respondents were in agreement that:

- interoperability is important and so should be subject to assurance;
- an 'approved products list' should be introduced, although respondents noted that processes were also needed to ensure it is kept up to date; and
- the SEC panel should establish and maintain the 'approved products' list.

296 Respondents were divided on the approach to protocol certification. A slight majority noted that the certification processes embedded within the HAN protocols should, if appropriately updated, provide the assurance of interoperability. However, a substantial minority suggested that further measures would be required, including, for example, testing of the functional performance of the device, and that devices should be tested with other manufacturers' devices to ensure they interoperate.

297 As set out in Part 1 of the Consultation Response, we have chosen to use ZigBee SEP and DLMS as the HAN application layers. As with any standard,

the base specification for these products is maintained by open standards bodies comprising stakeholders who deploy products using the specifications. The base specifications for both DLMS and ZigBee SEP are currently being extended to include GB functionality. This work will complete in 2014, and we are grateful for the contribution from the SSWG[44] towards its advancement.

298 The base specifications for both these standards contain far more data objects, commands and associated test scripts than are required for GB. The subset (for 2.4GHz-based solutions) that must be used to support the implementation of smart metering in GB is to be defined in the GBCS, which will be developed from the ZigBee SEP and DLMS base specifications. The Programme intends to notify the GBCS to the European Commission in Q2 2014.

299 The standards bodies define testing regimes which are designed to confirm the interoperability of ZigBee and DLMS communications between in-home devices. In the case of GB smart metering, testing regimes will be aligned to the ZigBee and DLMS use cases which will be referenced in the GBCS. Successful completion of the testing regime will result in protocol certification.

300 As explained in the response to Question 32, the Commercial Product Assurance (CPA) – Foundation Level Scheme has been selected as the means of confirming compliance with the security characteristics defined for each item of equipment. Satisfactory compliance testing through an independent test laboratory will result in CPA certification.

301 Suppliers and the DCC will be required to ensure that ZigBee, DLMS and CPA certificates are provided to the SEC Panel for SMETS and CHTS equipment installed in consumer premises. When these certificates have been obtained, the SEC Panel will add details of that equipment to the 'certified products list'. This is a change in the nomenclature from 'approved product list' that was the subject of Question 38 at consultation but, from wider discussions on testing and certification, we believe that the 'certified' label is a more accurate and factual description of what has been achieved. SMETS 2 equipment which is not on the certified product list will not be automatically enrolled into the DCC.

302 A significant minority of respondents to Question 39 noted that whilst it is an important component of assurance testing, protocol certification on its own was not sufficient. Some argued that protocol testing will show that communications within the device work, but not that a device has performed the correct functional action. We agree that the functional performance of the equipment should be tested to provide assurance that the meters correctly interpret the content of messages communicated via the DCC User Gateway and that they respond correctly and effectively. We understand that individual suppliers may have different functional requirements beyond those defined in SMETS. Our view is that functional testing is best undertaken by suppliers to provide them, and their meter asset provider, with assurance that the meter performs functionally to their satisfaction. Since this is a key business

[44] Smart Specifications Working Group

dependency for suppliers, we expect that functional assurance will not require regulatory intervention, as occurs in the meter market at the moment.

303 Other respondents questioned if protocol certification would provide assurance that in-home equipment will interoperate with the DCC's systems. The achievement of end-to-end interoperability of in-home equipment through the DCC is a key objective for the GB smart metering roll-out. Compliance with the GBCS should go a long way towards ensuring that in-home equipment interoperates with the DCC's systems as messages will be formatted in the correct HAN ready language i.e. GBCS compliant. However, the Government recognises that interoperability with DCC's systems will only be assured when the equipment is shown to operate as part of the end-to-end system.

304 We are developing an overall approach to testing with industry that aims to build confidence through incremental testing of components and leading to 'end-to-end' testing. The testing approach will encompass the certification of equipment and the testing of inter-operability and is expected to include requirements for:

- the DCC to undertake testing of its systems to ensure that they deliver the services defined in their licence, the SEC and their contracts as part of the end-to-end system;
- the DCC to use SMETS and CHTS compliant equipment when they undertake this testing;
- equipment to be enrolled in the DCC being interoperable with the DCC's systems, likely to be reflected in the enrolment criteria to be included in the SEC for suppliers and then separately in the CHTS, for communications hubs;
- suppliers and the DCC to undertake testing to ensure that they meet the inter-operability requirement; and
- large energy suppliers to be ready to participate in testing at the user integration stage.

305 To support this activity, we will require that the DCC provides an appropriate test environment for use by suppliers and manufacturers. However, we do not propose formal certification of DCC interoperability as a condition of enrolment.

306 We propose to require the DCC to create and maintain a 'deployed products list', which will be made available to SEC Parties. Over time there will be different variants of equipment, some with firmware upgrades that are deployed in different configurations and linked to different supplier's systems. The deployed products list should contain the details of the variants and combinations of equipment and systems that have been deployed in premises, and therefore give useful information about equipment configurations operating successfully in the live environment.

307 We will make a consolidated proposition for testing and certification available for further comment by industry in July 2013, and further detail on how these arrangements will be realised in regulation will be provided in a consultation on the legal drafting for the SEC.

Government Conclusion

Interoperability is key to the seamless end-to-end operation of smart metering, and will be subject to assurance. The GBCS will set out those elements of the base ZigBee and DLMS specifications which are applicable to the GB market and successful testing against these specifications will enable equipment to receive protocol certification. The equipment will also be security certified under the CPA – Foundation Level regime.

On achievement of both certificates, the equipment will be placed on a 'certified products list' to be introduced and maintained by the SEC Panel. SMETS 2 equipment that is not on the certified product list will not be eligible to be automatically enrolled into the DCC.

We are developing an overall approach to testing and certification with industry which will include:

- the DCC testing its systems to ensure that they deliver the services defined in their licence, the SEC and their contracts as part of the end-to-end system;
- the DCC using SMETS and CHTS compliant equipment when they undertake this testing;
- equipment to be enrolled in the DCC being interoperable with the DCC's systems;
- suppliers and the DCC undertaking testing to ensure that they meet the inter-operability requirement; and
- large energy suppliers being ready to participate in testing at the user integration stage.

The DCC will be required to provide a test environment that can be used to test the interoperability of in-home equipment with the DCC's systems and will be required to maintain, for information purposes, a deployed products list of the combinations of equipment enrolled in DCC including details of each device's configuration and version number.

Since the functional performance of the meter is a key business dependency for suppliers, we consider that functional testing is best undertaken by suppliers.

6. Next Steps

308 Following the notification of SMETS 2 in January 2013, a number of activities now need to be completed in the period through to the start of mass roll-out in late 2015. These include wider changes to the smart metering regulatory framework, finalisation of the GBCS, implementation of an assurance regime, and smart metering equipment manufacture and certification.

309 This section addresses a number of issues, the conclusions on which will inform the more detailed plans for this transitional period.

Regulatory Framework and Equipment Availability

Summary of issue under consideration

Views were sought on the proposed changes to the regulatory framework to reflect the CSP-led model for communications hub responsibilities, and whether any further changes to the regulatory framework were necessary (Question 45).

Comments were invited on the proposed timescales for equipment availability (Question 46). Views were also sought on the proposal that SMETS 2 should only be introduced into the regulatory framework when the Government has confidence that equipment to satisfy the new requirements is available at scale (Question 47), and whether a further period of notice is needed to ensure suppliers can manage their transition from SMETS 1 to SMETS 2 meters.

Government consideration of issue

310 The great majority of respondents agreed that the CSP-led model for communications hub responsibilities should be reflected in the DCC licence and the CHTS. A small minority of respondents did not support the proposed approach, in each case reflecting their overall disagreement that the CSP(s) should be responsible for the communications hub (Question 14).

311 We outlined the following equipment development and availability timescales in the SMETS 2 Consultation:

- 2.4 GHz GBCS available — Q3 2013
- First tranche of product testing completed — Early 2014
- SMETS 2 Gas and Electricity Meters available — Early 2014
- CSP communications hubs available for testing and trialling — Early/mid-2014
- CSP communications hubs available at scale — Late 2014

312 The majority of consultation responses stated that the timescales for equipment development were reasonable provided the dates set out in the consultation document for the completion of key activities did not slip.

313 In December 2012, we committed to review the programme plan and timetable during the first half of 2013. The consultation responses on the timetable, and subsequent discussions provided a key input into this review.

314 On 10 May 2013, we announced our initial findings from the review. We concluded that more time is needed for the design, build and test phases of

the end-to-end smart metering system if the mass roll-out is to get off to the best possible start and ensure a quality experience for consumers. As a result we announced that we now expect suppliers to be ready to start scaled roll-out by autumn 2015 and to complete roll-out by the end of 2020.

315 Further work is underway to review the detailed timescales and to develop a revised plan for the SMIP.

316 The consultation stated that the Government would use evidence on equipment availability and lead in time to introduce SMETS 2 'at an appropriate time'.

317 The majority of respondents agreed that SMETS 2 should only be introduced when the Government has confidence that equipment to satisfy the new requirements is available at scale. Respondents stated that, when SMETS 2 is introduced:

- equipment should be available from two or more manufacturers;
- interoperability of equipment should have been demonstrated through the testing and certification process; and
- ideally, the DCC should be in place.

318 A number of respondents also felt that there should be a transitional period of six to twelve months following the introduction of SMETS 2 to avoid stranding SMETS 1 meters.

319 We anticipate that suppliers will seek to install SMETS 2 metering equipment as soon as it is possible to do so. This is because SMETS 2 includes several requirements that enhance the functionality, security and interoperability of the equipment compared to SMETS 1. Ultimately these enhancements will benefit suppliers (and consumers and other SEC parties) by facilitating a more simple enrolment process and fuller service provision. The current regulatory framework allows suppliers to install SMETS 2 compliant equipment in advance of its inclusion in the regulatory framework, but as part of a SMETS 1 compliant system.

320 We also recognise the value of introducing SMETS 2 into the regulatory framework at the earliest possible stage. This should provide suppliers, manufacturers and financiers with increasing confidence as they seek to confirm their investment in the development and installation of SMETS 2 meters.

321 In advance of this we expect that the second iteration of SMETS 2 (including the GBCS and security certification requirements) will have been notified to the EC and end-to-end testing of the DCC's systems will be underway.

322 It is also our expectation that DCC communications hubs will be available to coincide with the availability of SMETS 2 equipment.

323 Finally we recognise that suppliers are interested in the date after which new SMETS 1 meter installations will not count towards their roll-out targets. At this stage, we do not consider that this date need necessarily coincide with the date that SMETS 2 is introduced into the regulatory framework. Our current expectation is that for a limited period, new installations of SMETS 1 or SMETS 2 will count towards suppliers' roll-out targets. A notice period will

be provided in advance of this date to allow suppliers to manage their SMETS1 and SMETS2, prepare their back office systems and retrain their installers as necessary.

Government Conclusion

The development and availability timescales in the original Consultation Document will be superseded by those due to be published later in the year following the re-planning exercise. This will outline our view of the equipment development and availability timescales.

We plan to introduce SMETS 2 into the regulatory framework at the earliest possible date. However, it seems reasonable that SMETS 1 metering equipment installed after this date should also count towards suppliers' roll-out targets for a limited period. We will give notice of the point at which new SMETS 1 installations will no longer count towards suppliers' roll-out targets. After this point all new installations will have to comply with SMETS 2 if they are to count towards suppliers' roll-out targets.

Governance of the Technical Specifications

Summary of issue under consideration

The general arrangements for modifications under the SEC were considered as part of the SEC consultation[45]. However, given their technical nature, it was noted that special provisions may be needed for modification of Technical Specifications (the SMETS and CHTS, including the GBCS and Security Characteristics).

The consultation proposed that modifications to the Technical Specifications should be assessed by a technical sub-committee within the SEC, reporting (in an advisory capacity) to the SEC panel. Two options were proposed: a standing sub-committee responsible for both modifications and assurance, or a non-standing sub-committee convened only when modifications to SMETS are proposed.

Views were sought on the date on which responsibility for the process of modifications to the Technical Specifications should pass from the Government to the SEC (Question 48), on two options for a sub-committee to assess proposed modifications (Question 49), and the areas of expertise that should be reflected in the sub-committee's membership, in order to fulfil its role (Question 50).

Government consideration of issue

324 The majority of respondents to Question 48 agreed with our proposals that responsibility for the Technical Specifications should lie with the SEC Panel when the criteria described in the consultation were met. Some argued that this should only take place once SMETS and CHTS compliant equipment had been deployed for a year or more.

[45] https://www.gov.uk/government/consultations/smart-energy-code-stage-1

325 We believe that the SEC Panel should have responsibility for maintaining and developing the Technical Specifications as soon as it is practical for them to do so. This will ensure that responsibility for the Technical Specifications rests with the SEC parties, who should also have access to the necessary technical expertise.

326 As part of our consultation on Stage 1 of the SEC, we have proposed specific provisions to be included in Section X of the SEC to enable the Secretary of State to introduce Technical Specifications and other technical and procedural documents into the SEC.

327 The exact timing of the incorporation of the Technical Specifications in the SEC is yet to be determined, but we expect this to coincide with the introduction of SMETS 2 and CHTS into the regulatory framework. By this time, the Technical Specifications for smart metering should be developed to the point that compliant equipment will have the technical capability that is needed to meet the business case for smart metering. (However, as noted in paragraph 98, we expect that amendments will be made after this point to introduce alternative HAN solutions to the Technical Specifications).

328 The great majority of respondents who answered Question 49 agreed that modifications of the Technical Specifications should be considered by a standing technical sub-committee, which would report (in an advisory capacity) to the SEC Panel. A number made the point that a standing sub-committee would be especially important in the initial period following the transfer of the Technical Specifications when the likelihood of modifications being raised could be expected to be higher. Some respondents expressed the view that the decision on whether this sub-committee should be standing should be left to the discretion of the SEC Panel once it is established. Attention was drawn to the need for the sub-committee to represent a wide range of expertise and the interests of SEC Parties. Reference was also made to the importance of retaining the knowledge and expertise that had been developed during the development of the Technical Specifications.

329 We consider that the standard SEC processes for code modification[46] can be relied upon to a large extent to manage change proposals for the CHTS and SMETS. They provide for a rigorous assessment of modifications and require that modifications must facilitate the achievement of the SEC's general objectives, including the efficient provision, installation, and operation of smart metering equipment, interoperability of equipment and delivery of consumer benefits.

330 However, given the highly technical nature of the Technical Specifications, we agree that some additional requirements should be added to the standard modification process. We have decided that the SEC Panel should establish a standing Technical Specifications Sub-Committee (TSSC), and should be required to consult it on proposed modifications to the Technical Specifications, and to any other SEC modifications which may have consequences for Technical Specifications. The TSSC would provide for

[46] Stage 1 of the Smart Energy Code: a Government response and a consultation on draft legal text: www.gov.uk/government/consultations/smart-energy-code

continuity of technical expertise and retention of corporate memory which might not be offered by ad-hoc working groups. The TSSC would also provide expert advice to the SEC Panel more broadly on issues relating to Technical Specifications, including an oversight function for end-to-end technical architecture.

331 The TSSC's role would include:

- advising the SEC Panel on the potential impact of any modifications on the architecture of the end-to-end smart metering system;
- reviewing and reporting, at appropriate intervals, to the SEC Panel on the effectiveness of the end-to-end system's technical architecture;
- maintaining an up to date view of the end-to-end technical architecture for smart metering;
- supporting, where appropriate, the SEC Panel in producing its Annual Report (as required under the SEC) on the implementation of the SEC and how it meets the SEC objectives;
- providing support to the SEC Panel to enable it to fulfil its obligation to advise Ofgem on the notification of modifications to Technical Specifications as required under the Technical Standards Directive; and
- advising the SEC Panel on resolution of any disputes concerning technical specifications.

332 The SEC Panel will decide on the membership of the TSSC, based on the need to provide the appropriate level of technical expertise. Governance arrangements for the TSSC would also be a matter for the SEC Panel.

333 The DCC will be required to provide evidence to the SEC Panel of any potential impact to its systems of modifications to the Technical Specifications. The SEC Panel will be required to obtain the advice of the Security Sub-Committee for modifications to the CHTS and SMETS, in order to determine their potential impact on the security of the end-to-end smart metering system.

Government Conclusion

The power to modify the Technical Specifications is expected to be incorporated in the SEC when SMETS 2 is introduced into the regulatory framework.

To a large extent the standard SEC procedures can be relied upon to manage modifications to the Technical Specifications, but a number of additions will be introduced in view of the highly technical nature of Technical Specifications. The SEC Panel will be required to establish an advisory standing Technical Specifications Sub-Committee which it will consult on proposals for modifications to the Technical Specifications. The TSSC's role will include considering the potential impact of any modification on the end-to-end smart metering architecture. It will also have an oversight responsibility for the end-to-end smart metering system. The DCC will be required to provide advice to the SEC Panel on any impacts of proposed modifications to the Technical Specifications on its systems. The SEC Panel will be required to consult the Security Sub-Committee on the impact of any modifications to the CHTS and SMETS on the security of the end-to-end smart metering system.

7. Other Matters

334 This section provides an update on the issues outstanding from the publication of Part 1 of the Consultation Response, and / or the first iteration of SMETS 2, and also sets out our position on communications hubs type faults.

Outstanding Issues from Part 1

Recycling of communications hubs

335 Where it is economic to do so, the CSP(s) are encouraged to recondition communications hubs that have been removed from a consumer premises and reintroduce them into the supply chain. The CSP(s) are required to recondition faulty communications hubs and reintroduce them into the supply chain if the cost of reconditioning is less than the remaining asset value of the device.

336 Where a communications hub is known to be working but is removed from a premises, for example as a result of a non-domestic customer opting out of the smart meter deployment or replacement of a one HAN variant with another, the CSP will receive only 80% of the remaining asset value of the communications hub, thereby incentivising it to recondition and resupply rather than dispose.

337 CSP bidders have been asked to set out a process that maximises the number of communications hubs that can be reconditioned whilst also minimising the costs associated with the reconditioning process. CSP bidders have also been asked to indicate the circumstances in which communications hubs could not be reconditioned on a cost-effective basis.

The requirement for keypads on meters

338 In Part 1 of the Government Response to the SMETS 2 Consultation, we set out our decision to include a provisional requirement for a keypad in the first iteration of SMETS 2 to facilitate consumer use. We explained that we were undertaking further work to assess the impact of including this requirement, including consultation with stakeholders and further analysis to assess whether this proposal was justified.

339 Under normal circumstances, the smart prepayment consumer will add credit to their meter remotely via the WAN. This will improve the prepayment experience as consumers will not have to interact with their meters to top-up. However, in the event that the WAN is unavailable, suppliers have the option to provide a Unique Transaction Reference Number (UTRN) to the consumer - a 20 digit one-time code that can be applied directly onto a meter in prepayment mode to add credit.

340 The provisional decision to mandate a keypad was made in the light of concerns that any requirement to input a long number to enable top-up using the standard two or three button meter interface might provide a poor consumer experience, and possibly be problematic for some consumers. Prepayment consumers might therefore be left off-supply if they were unable to top-up before their credit expired.

341 It is estimated that provision of a keypad on every meter would add £124m to the costs of the roll-out (as identified in the Impact Assessment published in January 2013[47]). The responses from suppliers made clear that mitigation of the risk of consumers being left off supply in instances of WAN failure can be met more cost effectively by allowing them the flexibility to adopt their own strategies to plan for and deal with such situations. Actions under consideration by suppliers include:

- installation of some meters with keypads;
- provision of Prepayment Interface Devices (PPMIDs);
- use of non-disablement periods and emergency credit; and
- (as a last resort) a home visit by suppliers to facilitate top-up.

342 In considering whether or not to mandate keypad provision, we also considered the role of the existing regulatory framework in protecting consumers. Supplier Licence Condition (SLC) 28 requires suppliers to undertake certain actions to ensure that it is safe and reasonably practicable for a customer to utilise a prepayment meter. The guidance accompanying this supply licence condition asserts the need for a supplier to be confident that any technological innovation they employ when utilising a prepayment meter will enable them to provide a supply to the customer at all times.

343 Following further analysis (including an information request and stakeholder outreach) we have decided that the decision to mandate a keypad on all meters cannot be justified by the available evidence and consideration of relevant costs and risks. The requirement for a keypad on the User Interface of gas and electricity meters will be removed from the next version of the SMETS. Suppliers will be given the flexibility to decide how to meet their obligations and requirements[48]. This will allow suppliers to tailor and adapt their approach taking into account consumers' circumstances and emerging evidence regarding types and lengths of communications issues.

344 Suppliers will need to have robust strategies in place to plan for and manage scenarios where there is a temporary loss of WAN coverage. We consider that suppliers should not rely solely on UTRN entry by prepayment customers via a two or three button interface. We expect these strategies to include plans and systems to communicate with consumers when the WAN fails and they try to top up, for example by text message or telephone.

345 We will work with suppliers to monitor approaches to mitigating this risk and any impacts of intermittent failures on consumers.

Operational Licence Conditions

346 Part 1 of the Consultation Response set out our policy on operational requirements, which will oblige energy suppliers to ensure that key smart metering functionality is made available to domestic and micro-business consumers. We confirmed that we would introduce licence conditions for operational requirements, as had been proposed in the consultation and was

[47] https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version
[48] Including but not limited to the requirement to provide a user interface which supports the entry of a 20 digit UTRN; and the obligation only to offer prepayment to a consumer where it is 'safe and reasonably practicable' to do so.

broadly supported by respondents. However, in response to comments from respondents, we said we would review the drafting of the licence conditions to ensure that they provide for all these requirements in a clear and coherent manner.

347 We laid licence conditions for operational requirements before Parliament on 10 May 2013[49] which will have the same effect as the consultation version but have been redrafted to improve clarity. Requirements will be placed on energy suppliers with respect to smart meters in domestic premises and in those micro-businesses where meters are enrolled with the DCC. The requirements will apply initially to smart meters that they have installed, and in due course to all smart meters in these premises.

348 Energy suppliers must take steps to link the smart meter to a communications network so that the meter receives and sends remote communications. They must also take steps to enable consumers to use CADs within their premises which allow them to access information that is stored in the meter, and to ensure that any IHD provided by a supplier for use with the meter in domestic premises enables the display of particular energy usage information.

349 Subject to the successful completion of the Parliamentary process, we expect the modifications to come into force on 14 July 2013, unless otherwise specified in the modifications.

350 It should be noted that our response to the Foundation Smart Market Consultation, published on 10 May 2013[50], included a consultation on a draft amendment to the operational requirements licence conditions arising from our decisions following the earlier consultation. It is expected that any licence condition modification would take effect in late 2013, subject to consultation and successful completion of the Parliamentary process.

Communications Hubs Type Faults

351 In Part 1 of the Consultation Response, we set out our decision that we would adopt a CSP-led model for communications hubs responsibilities. The majority of respondents agreed that this model should be reflected in the regulatory framework.

352 In the CSP-led model, we concluded that the DCC would procure communications hubs via the CSP contracts, and within each region the CSP would supply communications hubs to energy suppliers for installation and maintenance. This would operate under a general principle of 'costs lie where they fall', to avoid complex recharging arrangements for installation and maintenance.

353 Some suppliers raised concerns over the 'costs lie where they fall' principle, commenting that supplier responsibility for the costs of repair and replacement activity may not incentivise the CSP to procure equipment that is

[49] Licence Conditions for Operational Requirements and Accession to, and Compliance with, the Smart Energy Code: www.gov.uk/government/publications/smart-metering-implementation-programme-licence-conditions-for-operational-requirements-and-accession-to-and-compliance-with-the-smart-energy-code

[50] The Government Response to the Consultation on the Foundation Smart Market and Further Consultation: www.gov.uk/government/uploads/system/uploads/attachment_data/file/197877/FSM_Consultation_Response_FINAL_0900__10-05-13.pdf

fit for purpose. In order to address these concerns, we committed to providing further information on what constituted a 'type fault'. A type fault describes the circumstances where substantial numbers of communications hubs are deemed not fit for purpose. Through engagement with suppliers and the CSP(s), we have further developed our position on 'type faults' which is outlined below. Associated legal drafting will be subject to consultation in a future SEC consultation.

354 Responsibility for communications hub faults will either be allocated to the CSP or the relevant energy supplier. For example, the energy supplier would be responsible for physical damage post-delivery including any fault caused by the supplier or the customer. The CSP would be responsible for faulty equipment, for example where equipment fails to meet the requirements set out in the CHTS and the relevant Communications Services contract. Where a communications hub has failed and the fault is the responsibility of the CSP, there will be a threshold level of failures known as a fault threshold. The fault threshold will be measured as an annual percentage of communications hubs with faults that are the responsibility of the CSP. The fault threshold aims to protect energy suppliers while optimising the price of the communications hub.

355 Below the fault threshold, suppliers will not be able to recover field service costs. However, where the CSP faults exceed the fault threshold, the CSP will be required to pay a liquidated damage payment for these faults (i.e. for each faulty communications hub above the type fault threshold). The level of liquidated damage is intended to reimburse the affected suppliers for their field service costs of replacing the faulty communications hubs. The DCC will play a role in collecting the liquidated damages and allocating them across affected suppliers. Further detail on this will be provided in the SEC consultation.

356 In addition to the approach to type faults, we are proposing to include a process for compensation for batch faults, where a high percentage of devices fail within a single delivery. This process will provide a mechanism that will allow the DCC to recover liquidated damages from the CSP in a scenario where an individual batch or delivery of communications hubs suffers a high percentage of communications hub failures, but the volume of such failures is not sufficient to exceed the fault threshold on a regional level.

8. Smart metering elements of the EU Energy Efficiency Directive

Summary of Issue

The EU Energy Efficiency Directive (2012/27/EC) includes provisions which relate to the roll-out of smart meters in Member States. In December 2012, we consulted on options for the implementation of the Directive provision to provide domestic consumers with a smart meter with easy access to at least 24 months of daily/weekly/monthly/annual consumption data[51].

Background

357 The Directive applies to the roll-out of smart meters in the United Kingdom. This consultation response addresses the implementation in Great Britain. The transposition deadline for Member States is 5 June 2014, by which point any regulations to implement the Directive must be in force.

358 The Directive requires that where a domestic consumer has a smart electricity / gas meter installed in accordance with the Third Package, the consumer has the right to easy access to at least the previous 24 months of daily / weekly / monthly / annual consumption data. If a consumer has been with their supplier for less than 24 months then they have the right to access their data for the length of their supply contract.

359 We published a consultation on 12 December 2012, which closed on 6 February 2013, asking for views on whether the capability for daily reads should be added to SMETS 2 meters, and how suppliers should provide domestic consumers with access to their consumption data under the Directive provision.

Government consideration of the issue

360 The majority of respondents agreed with the proposal to include 24 months of daily reads in SMETS 2 meters and communications hubs.

361 Respondents had mixed views on the suggestion that suppliers should be specifically required to offer consumers access to the consumption data over the internet. Only a small number of respondents felt that it was necessary to specify that all consumers should be able to access their data via the internet, with the majority arguing that this was overly prescriptive. Overall there was a view that being less prescriptive, within the scope of the Directive, would enable suppliers to be more flexible as to how they offer data to consumers and enable innovation.

362 In the light of the consultation responses and further analysis, we have concluded that the capability to include 24 months of daily reads should be

[51] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/66616/7245-consultation-on-implementing-the-energy-efficiency.pdf

added to SMETS 2 meters. Suppliers will be required by licence condition to provide domestic consumers with access to their data either over the internet or via the meter interface. As the Directive does not require a set format for the provision of data, we do not intend to prescribe one in the licence conditions.

363 Our view is that this approach will give suppliers flexibility as to how to implement the Directive requirement. This will allow them to tailor their approach to their business model and it should minimise the overall cost of implementing the Directive provision.

Costs

364 The Directive requires that consumers must be provided with the data free of charge. Respondents did not provide significant information on the impact of implementing the Directive provision, but agreed that adding the capability to the meter (in terms of additional memory) would not have a significant impact on costs (although there may be some small additional costs from testing of functionality and interoperability).

365 In terms of providing consumer access to data, our expectation is that as a result of the 'midata' initiative (which requires suppliers to provide consumers with the information they hold on them in an electronic format), and also because of commercial drivers from growing awareness within the industry about the benefits of providing consumers with access to their consumption data, suppliers already plan to develop internet portals. In addition and as an alternative, suppliers also have the possibility to provide data by the meter interface or by email if they wish to do so.

Application to SMETS 1 meters

366 The Directive applies in respect of consumers with smart meters installed before, and from, the Directive implementation date. Therefore, as per the draft licence conditions in Annex 3, suppliers will be required to ensure that consumers with SMETS 1 meters can access their data either over the meter interface or over the internet (or both).

367 Suppliers will only need to start collecting 24 months of data at the point a consumer requests it. The minimum requirements for SMETS 1 meters do not include the capability to store 24 months of daily data, but suppliers may choose to upgrade SMETS 1 meters to provide this functionality. If the functionality is not available on the meter, suppliers will have to provide an alternative solution to ensure that they can meet the consumers request for access to 24 months of daily data.

368 If a SMETS 1 meter churns to a new supplier on change of supplier, that supplier will also need to provide data to the consumer on request, if the meter continues to be operated in 'smart mode' (i.e. the new supplier continues to use the meter with a functional communications infrastructure, either through the Data and Communications Company (DCC) or an Smart Meter Systems Operator (SMSO)). The new supplier will only need to provide data from the start of the supply contract.

Response to specific issues raised

369 In addition to stakeholder views on the preferred approach, a number of other issues were raised in consultation responses, and our response to these is set out below. Where relevant, we have reflected views expressed by some suppliers about how they might address these issues as an illustration of the actions suppliers might choose to take. This is not intended to constitute guidance on how Ofgem would interpret the licence conditions.

Replacement/failure of communications hubs/meters

370 A number of respondents asked what would happen where a communications hub/meter failed or needed to be replaced, if this affected the supplier's ability to collect the data. Under the roll-out licence conditions, suppliers are required to maintain smart metering equipment so that it complies with the SMETS. We also intend to require that similar provisions are applied so that the communications hub is maintained such that it continues to comply with the CHTS. This will be reflected in the SEC and the roll-out licence conditions when the requirement for DCC communications hubs to be installed is applied.

371 We do not see that there is a need to regulate to specify the action a supplier should take where a communications hub or smart meter failed or needed to be replaced. From discussions with stakeholders, it seems likely that suppliers would take steps to retrieve consumption data from a faulty meter, and would offer consumers who have requested 24 months of data the opportunity for a final data summary before their meter is replaced.

Change of tenancy/supplier

372 A number of respondents queried what would happen on change of tenancy or supplier. The Directive is clear that consumers should be able to access the previous 24 months of their consumption data, or consumption data for the length of their supply contract if this is shorter.

373 Again, discussions with some stakeholders have indicated that, where a consumer is leaving a supplier or is moving house and has already requested access to 24 months of consumption data, then a supplier would offer consumers a final data summary if the customer were to request it. It does not appear necessary to specify this in the licence conditions.

Data access and privacy framework

374 A number of respondents asked how the provisions in the Directive fit with the SMIP Data Access and Privacy Framework. Our view is that the right for consumers to access 24 months of historical data under the Directive provision is self-standing and separate from any choices consumers may exercise about supplier access to their consumption data.

375 Therefore, while a customer can ask a supplier to provide them with their consumption data (and suppliers operating SMETS 1 meters will need to make arrangements to collect and store this data), the consumer should be able to opt-out of allowing their supplier to access daily data for any purpose other than compliance with the Energy Efficiency Directive. Suppliers will need to make appropriate arrangements to comply with this.

Interaction with midata initiative

376 A small number of respondents asked about the relationship with the 'midata' initiative and whether it was sufficient to deliver the Directive provision. Our view is that this would not be sufficient to implement the Directive provision as it would not require suppliers to provide data stored on meters.

Consumer access to data

377 Some respondents asked whether suppliers needed to provide data to consumers who do not have the internet or who have accessibility issues. Our policy is that suppliers will be required to provide access to data either over the internet or via the meter interface. Suppliers are therefore not restricted to providing data over the internet and may choose to make data available over a meter interface instead.

378 Suppliers will also need to consider what adjustments are needed to ensure compliance with Section 29 of the Equality Act 2010. This requires suppliers of services to make reasonable adjustments to ensure that a disabled person is not put at substantial disadvantage in comparison with a nondisabled person. In particular, the Act requires that where a disabled person would be put at a disadvantage by physical equipment, that reasonable steps are taken to avoid that disadvantage, or to provide an auxiliary aid if this would avoid putting someone at a disadvantage. Information must also be provided in an accessible format where not to do so would put a disabled person at disadvantage.

Licence Conditions

379 We will be consulting on licence drafting conditions in due course so that they come into force for the implementation of the Directive provision in June 2014.

Government conclusion

The second iteration of SMETS 2 will include the requirement for the electricity meter to store 24 months of daily consumption data. The CHTS will require the communications hub to store 24 months of daily consumption data for gas.

A general requirement will be placed on suppliers in licence conditions to meet the Directive provision that consumers must be provided with consumption data over the meter interface or internet. This will come into force on 5 June 2014.

A requirement will be placed on suppliers in licence conditions to inform consumers that this data is available to them on request, to provide it to consumers who request it, and to ensure that it is provided free of charge. We will consult on this in due course.

Glossary

Advanced Meter

A meter which, either on its own or with an ancillary device, stores measured electricity or gas consumption data for multiple time periods, and provides remote access to such data by the licensee.

Application Layer

Application Layer, in this context, is taken from the ISO standard Open Systems Interconnection (OSI) model for communications systems. In the OSI model, the Application Layer is the layer which provides the functionality required to deliver the end service. For Smart Meters the Application Layer would facilitate, for example, the ability to read or set variables within a standard scheme of data items related to Smart Meter operation.

Assurance Maintenance Plan

This is the term within CPA which covers all of the processes and standards which keep product certificates relevant as products are updated.

BEAMA

The British Electrotechnical and Allied Manufacturers' Association, representing over 300 manufacturing companies in the electrotechnical sector across the UK and Europe.

Build Standard

A standard which describes properties of a developer's security engineering approach which is assessed as part of a CPA evaluation. This is used to gain confidence in the product developer's processes and to give assurance that the quality of a security product is not expected to decrease over the duration of a CPA certificate.

Commercial Product Assurance (CPA)

The CESG scheme for the evaluation and certification of commercial security-enforcing products, to be applied to SMETS 2 Type 1 equipment.

CESG

CESG is the UK Government's National Technical Authority for Information Assurance (IA), providing policy and assistance on the security of communications and electronic data.

Common Criteria

The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for computer security certification.

Communications Hub

A device or set of devices located at the customer's premises which will have the capability to communicate with the HAN and the WAN.

Communications Hub Technical Specification (CHTS)

The Communications Hub Technical Specification sets out the minimum physical requirements, minimum functional requirements, minimum interface requirements and minimum data requirements that will apply to a Communications Hub.

Communications Service Provider (CSP)

Bodies awarded a contract to be a service provider of the DCC's communications services.

Competent Independent Organisation (CIO)

A CIO is an organisation which has certain qualifications or characteristics such as being members of (or contain staff who are members of) CESG schemes, such as CCP[52], CLAS[53], CHECK[54] or CTAS[55], or a combination thereof.

Consumer Access Device

A device which will be securely connected via the HAN interface and will receive consumption and tariff information which it will use to assist consumers manage their energy use. A CAD may be one of a number of devices - such as an enhanced energy display, a smart appliance or a home automation controller.

Credit Mode

A mode of operation whereby consumers are generally billed for their energy use retrospectively.

Data and Communications Company (DCC)

The new entity that will be created and licensed to deliver central data and communications activities. The DCC will be responsible for the procurement and contract management of data and communications services for the end-to-end Smart Metering System.

Data Services Provider

The body awarded a contract to be a service provider of the DCC's data services.

DLMS / COSEM

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

Distribution Network Operators (DNOs)

Companies that are licensed to take electricity off the high-voltage transmission system and distribute it, over low-voltage networks, to consumers.

End-to-end Smart Metering System

The End-to-end Smart Metering System covers all relevant equipment, communication links and connections from every consumer premise through the DCC to suppliers, DNOs and authorised third-party service providers.

[52] CESG Certified Professional
[53] CESG Listed Advisor Scheme
[54] CESG IT Health Check Service Scheme
[55] CESG Tailored Assurance Scheme

Energy Service Company (ESCO)

A professional organisation, scheme or trust that delivers energy services and/or other energy efficiency improvement measures in a user's facility or premises.

Energy UK (EUK)

The trade association for the energy industry, representing over 80 companies across the broad range of energy providers and suppliers, and including companies of all sizes working in all forms of gas and electricity supply and energy networks.

Firmware

Software that is embedded in devices for the purpose of controlling that device. It cannot be changed under the normal operation of the device in which it resides.

Foundation stage

The period prior to the start of the Mass roll-out stage.

GB Companion Specification (GBCS)

The subset of the base specifications for ZigBee SEP and DLMS, which must be used to support the implementation of smart metering in Great Britain.

Hand Held Terminal (HHT)

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

Home Area Network (HAN)

The Home Area Network is the means by which communication between Smart Meters, IHDs and other smart metering devices in premises is affected.

In-Home Display (IHD)

An electronic device, linked to Smart Metering System, which provides information on a consumer’s energy consumption and ambient feedback.

Interoperability

The ability of diverse systems, devices or organisations to work together (interoperate).

Intimate Communications Hub Interface (Specification) (ICHI / ICHIS)

The ICHI Specification sets out the minimum requirements that will apply to the Intimate Communications Hub interface between the communications hub and the electricity meter.

Mass roll-out stage

The period between the date at which the DCC starts providing core communications services and the fulfilment of the roll-out obligation as specified in the roll-out licence conditions.

Network Layer

Network Layer, in this context, is taken from the ISO standard Open Systems Interconnection (OSI) model for communications systems. In the OSI model, the Network Layer is the layer which routes data packets across point-to-point links within a communications system that has multiple endpoints.

Network Operators

The companies that are licensed by Ofgem to maintain and manage the electricity and gas networks in Great Britain.

Outage detection

The ability for an electricity supply interruption to be identified and communicated to the WAN.

Physical Layer

Physical Layer, in this context, is taken from the ISO standard Open Systems Interconnection (OSI) model for communications systems. In the OSI model, the Physical Layer is an electrical, mechanical, and procedural interface to the transmission medium. It describes the shapes and properties of any electrical connectors, or for wireless technologies, the frequencies to broadcast on.

Prepayment Meter Interface Device (PPMID)

A prepayment meter user interface separate from, but connected to the meter via the HAN.

Prepayment Mode

The mode of operation whereby customers generally to pay for their energy before using it.

Privacy Pin

A number used by the Consumer to access Personal Data and functions on the User Interface of electricity and gas meters.

Security Characteristics

A standard which describes necessary mitigations which must be present in a completed product, its evaluation or usage, particular to a type of security product.

Smart Energy Code (SEC)

The Code, spanning gas and electricity, will be established to provide arrangements for the introduction and on-going operation of the end-to-end Smart Metering System. Among other things, the Code will detail the relationships between the DCC and the users of its services for the new data and communications activities. Suppliers, Network Operators and other users of the DCC's services will also need to comply with the Code.

Smart Grid

Building a ‘smarter’ grid is an incremental process of applying information and communications technologies (ICTs) to the electricity system, enabling more dynamic ‘real-time’ flows of information on the network and more interaction between suppliers and consumers.

Type 1 device

A Device connected to the HAN that is allowed to issue or perform a range of HAN Interface Commands and can access the information stored in GSME, ESME or a Gas Proxy Device.

Wide Area Network (WAN)

The network that is used for two way communication between smart metering systems and the DCC.

ZigBee Smart Energy Profile (SEP) v 1.X

An application layer protocol (version 1.X or as specified).

Annex 1: Responses received

AMO	Energy UK	Northern Power Grid
ARM Holdings	ESTA	Npower
Arqiva	EUA	NXP Semi Conductors
BEAMA	First Utility	Ofgem
BluePrint for Water	Gazprom Energy	Panasonic
BRE Global	Gemalto-Cinterion	Pilot System
British Gas	Gemserv	Scottish Power
Cable and Wireless	Gridmerge Ltd	Siemens
Cambridge Consultants	Haven Power Ltd	Smart Energy Network
CMAP	HP Enterprises	SP Energy Networks
Consumer Focus	ICoSS	SSE
DNV Kema Energy	IET	Supremacy Associates Ltd
E.ON	IPSO Alliance	Trilliant
EDF Energy	Joanne Green	UK Power Networks
Electrosensitivity UK	Landis+Gyr	Utilita
Elexon	McAfee-Intel	Waterwise
Elster Metering Ltd	Motorola Mobility UK Ltd	Western Power
EM-Radiation Research Trust, BEMRI.org, Mast Sanity, SSITA	National Grid	Which
Energy Network Association	Network Rail	

Annex 2: Summary of responses to Consultation Questions

Chapter 4 – SMETS 2 Development	
Q1	**Do you have any comments on the criteria used in the evaluation of the application layer standards?**
Q2	**Do you agree with the proposal to adopt ZigBee SEP / DLMS as the HAN application layer standards for GB?**
Q3	**Do you agree that equipment should be required to comply with SMETS and a GBCS for ZigBee SEP / DLMS?**
Q4	**Do you agree with the overall approach proposed in relation to the HAN physical layer? If not, please provide a rationale and evidence for your position.**
Q5	**Do you have any comments on the criteria used in the evaluation of the physical layer of the HAN?** These questions were addressed in Part 1 of the Government Response to the SMETS 2 Consultation.
Q6	**What are your views on the compatibility of the reserved spectrum 870-876MHz with 868MHz and the value of considering the use of this band?** The majority of respondents to this question agreed that the availability of the reserved spectrum should be explored. A minority disagreed, arguing that uncertainty about the availability of dedicated spectrum would distract from development of 868MHz-based solutions.
Q7	**Do you consider that additional measures should be taken to encourage the development of an 868MHz solution?** The majority of respondents to this question agreed that additional measures should be taken to encourage the development of an 868MHz-based solution, arguing that left to its own devices, the market will take a long time to develop such a solution, resulting in a significant increase in overall programme timescales. It may also lead to confusion, the potential use of many competing and non-interoperable solutions, and thus a poor consumer experience, especially for those that deploy smart in two phases e.g. electricity followed later by gas. Some respondents noted that it might be necessary to place an obligation on suppliers to replace a 2.4GHz-based communications hub with a dual-band one at the consumer's request (if, for instance, they wish to install 868MHz-based devices), and that this would stimulate market growth. Some supportive responses were caveated by a need to develop a wired solution in

	parallel. A significant minority disagreed with the proposal. Their views fall broadly into three groups: • small suppliers and some technology companies who state than an 868MHz-based solution is not needed; • meter manufacturers and other technology companies who consider that market forces will drive the timely delivery of an 868MHz-based solution; and • one respondent who opposed any use of a wireless HAN on health grounds.
Q8	**Do you agree with the approach to allow the market to determine the balance between 2.4GHz and 868MHz? If not, please provide rationale and evidence.** Respondents to this question were evenly split in their preferences. Paradoxically, most of the responses (from either side) were caveated, and picked up on a number of common themes. Many respondents focused on the earlier availability of a single-band 2.4GGHz-based solution. Combined with likely ease of installation and lower costs, this will result in it becoming the most widespread solution (although there is a related risk of abortive installation visits where such a solution cannot be used). In turn, 868MHz-based solutions are at risk of relegation to 'in-fill' solutions only, and therefore not reaching sufficient volumes to support the availability of a wide range of compatible equipment, and / or competitive pricing. To address this, some respondents noted that the CSP(s) should be mandated either to move to dual-band, as soon as such communications hubs become available, or to provide a minimum volume of same. They noted the lower cost, lower reliability of the 2.4GHz-based solution against the higher cost, higher reliability of an 868MHz-based solution, and advised a longer term approach focused on the latter (when available) should be preferred as a means of simplifying the roll-out and reducing customer confusion. Finally, one respondent noted that the challenges likely to be posed by a sub-gigahertz solution are not yet fully understood. In consequence, it is not possible at this point to mandate any form of market balance or roll-out strategy.
Q9	**What are your views on the costs and benefits of the three options identified for deploying wireless solutions (i.e. 2.4GHz as the default; dual-band communications hubs; or market led)?** Many respondents reiterated their responses to Q8 on the approach to market roll-out, rather than the relative costs and benefits of the three options. Very limited evidence was provided on either costs or benefits. The largest group of respondents (including a small number of suppliers, most meter manufacturers and some technology companies) supported a market led approach. They cited the benefits of avoiding the marginal costs of a dual-band communications hub where this was not required, and the flexibility to allow the market to evolve. Almost as many respondents supported a dual-band approach. This group included a mix of large and small suppliers, and technology and communications companies.

	They cited the benefits of logistics and flexibility in favour of this option. The small balance of respondents offered a range of views. Two favoured a 2.4GHz-based solution only, but did not acknowledge its restrictions nor say how these would be addressed. Two advocated a single-band 868MHz-based solution, but did not suggest an interim solution until this becomes available. One respondent advocated using a bridging device in cases where a 2.4GHz-based solution will not work. Finally, one respondent objected to the use of wireless solutions on health grounds.
Q10	**Do you agree with the proposal for a 'fit for purpose' installation obligation on suppliers?** A weak majority of respondents, including those from energy supplier, meter supplier and communications and technology stakeholders agreed with the 'fit for purpose obligation on suppliers', although many caveated their answer. Opinion was split between energy suppliers. The principal points made by those respondents in agreement included: • greater clarity is required as to how the obligation would work in practise, for example, the use of calibrated procedures and equipment as well as agreed criteria; • the obligation is especially important for situations where there are different suppliers for gas and electricity; • the obligation would be greatly facilitated if there were a wider range of solutions to choose from; • exceptions from the obligation would be required for 'difficult buildings;' and • the obligation could impact installation times. A small number of stakeholders across a number of sectors disagreed, citing: • additional installation costs due to the time taken to perform tests on site; • difficulty of enforcement if detailed procedures are not defined; • suppliers would be better obliged to install 'best available technology'; • the obligation should sit on the CSP; • requirements on siting the IHD should be less stringent; and • additional costs for single fuel (electricity) suppliers that do not have the expertise to undertake range tests for the gas meter.
Q11	**Do you have any views on the proposed approach to developing a wired HAN solution?** A majority of respondents comprising energy suppliers and meter suppliers favoured a solution being developed as quickly as possible. In addition, many respondents asked for trialling, and a number of respondents said they were willing directly to support such trialling. Respondents suggested that a wired solution was also essential to avoid discrimination against customers in difficult buildings such as purpose built high rise blocks of flats. Another respondent indicated that the use of a wired solution may find wider application beyond difficult buildings, and that any selection process should recognise this. A small number of respondents including energy networks and comms & technology

	providers caveated their answers with the following points relating to a wired solution, noting that: • it should be IP-based and secure; • it must not interfere with other PLC and RF networks; • it is too disruptive and costly - the data should be relayed over the WAN instead; and • it will not achieve satisfactory propagation.
Q12	**Do you agree with the proposed scope of functional requirements for a communications hub? Are there any other functions that should be included and what would be your rationale for including those functions (including estimated costs and benefits)?** The majority of respondents agreed with the proposed scope of functional requirements for a communications hub. However, four were in disagreement, in turn: • not supporting the decision to have peer-to-peer communications between devices on the HAN: • concerned about the ability of the BEAMA working group to define the requirements adequately, and seeking more involvement for the CSP(s); • concerned that the communications hub was becoming too complex; and • not accepting the separation of the communications hub from the meter. The second part of this question was deliberately open, and encouraged a wide range of responses. A number of common themes emerged (numbers in brackets indicate number of respondents supporting the proposed functionality): • provision of both 2.4GHx and 868MHz solutions (7); • provision of wired HAN (5); • support for wireless firmware upgrades to multiple devices (5); • ability to send outage reports (2); • use of an external power supply - typically a battery (2); • provision for an intimate communications hub (2); • ability to distinguish between network power failure and failure of the communications hub power supply (2); • provision of a physical interface for Hand Held Terminals into the communications hub (1); and • provision of a gas mirror within the electricity meter (1). No costs or benefits were provided for any of the above suggestions.
Q13	**Do you have views on the specification for an 'intimate' interface between electricity meters and communications hubs?** All respondents who addressed this question supported the provision of an intimate communications hub interface (ICHI). They noted that it has potential to reduce: • the complexity and cost of installation; • the physical space taken up; • the number of aborted or failed installations; and • the cost of the communications hub by removing the need for a separate power

	supply. A number of respondents caveated their support for an ICHI. The following broad themes emerged: • the design of the interfaces should be standardised; • a standalone communications hub installation must also be supported – for example for gas first installations and circumstances where it is not possible to install in intimate mode; • any interface must be physically secure and tamper-proof; • the interface must ensure interoperability with any electricity meter; and • the two physical entities (electricity meter and communications hub) must remain separable. Respondents' views differed on the features and functionality to be offered by an ICHI[56]. One respondent was concerned that standardisation would limit innovation, and felt that the benefits of an ICHI were being overstated. A second respondent supported the provision of an ICHI, but not the inclusion of a data connection across the interface (i.e. a wired data link between the communications hub and the electricity meter rather than the wireless link which is specified in SMETS).
Q14	**Do you agree with the Government's marginal preference for the CSP-led model for communications hub responsibilities, or do you prefer the supplier-led model? Please provide clear rationale for the advantages and risks associated with your preferred option?** This question was addressed in Part 1 of the Government Response to the SMETS 2 Consultation.
Q15	**Do you agree with the proposal that a CHTS-compliant communications hub should not be mandated for opted out non-domestic sites and that suppliers should be free to use whatever type of communications equipment best supports their processes and WAN service?** The majority of respondents agreed that opted-out non-domestic customers would not need to implement a CHTS-compliant communications hub. However, a wide range of caveats and comments were provided which indicate significant variations in the actual levels of support. Respondents in favour noted that an opt-out option is needed to reflect the diversity of metering arrangements in the current non-domestic market. They noted the need to recognise significant investments in advanced metering which have been installed to support the CRC obligations, the development of solutions to support specific business needs, and the requirement to avoid stranding these assets. The majority of respondents also noted that the competitive market operates efficiently, including supporting independent third parties such as Meter Service Providers. However, a small number of respondents offered a counter view – that a proliferation of bespoke solutions might result in actual, or perceived, customer lock-in, especially if change of supplier processes were not clear and efficient, and the

[56] The views set out here were provided in response to the SMETS 2 consultation. Respondents' views had further coalesced in support of an ICHI by the time of the ICHI summit meeting in December 2012.

	cost position on opt-in / opt-out well understood. In time, this may reduce competition in the non-domestic market as opted-out customer are reluctant to change supplier. Most respondents noted that the current arrangements facilitate the production of data to meet specialist customer needs, including web-based provision. One respondent noted that smaller non-domestic customers may not have access to specialist web-based provision of data, and therefore to accurate and up-to-date consumption data. Many respondents, both supportive and in disagreement, stressed the need to ensure opting-out customers were aware of the consequences, particularly in terms of data availability, and that the supplier may pass on the installation costs of a CHTS-compliant hub should they, or any subsequent occupant of the premises, decide to opt back in. (This point is explored further in Q16, below). Other points raised included: • the need for clarity of charging and a breakdown of costs to customers. One respondent was concerned that opted-in customers would face higher costs from the DCC (passed on via the supplier), and that these should be itemised to allow the consumer to weigh up the costs and benefits of opting-in / opting-out; • support for the proposed position, but that the requirement not to require CHTS-compliant communications hubs should be reviewed as the main phase of smart metering roll-out gains pace to check that the arguments supporting opt-out remain valid; and • a number of respondents noted concerns over power outage reporting. These are addressed in Q18 (below).
Q16	**Do you agree that the gaining supplier should bear the costs of installing an appropriate communications hub if they decide to switch between opted in and opted out?** The majority of respondents supported the proposal that the gaining supplier should bear the costs of a replacement communications hub, some noting that this incentivises overall process efficiency, and thus the quality of the consumer experience. Respondents in agreement also noted that the gaining supplier could consider enrolment of the opted-out communications hub in the DCC (rather than replacement), and also that CHTS-compliant communications hubs should not be removed at opt-out, but simply left dormant for potential opt-in at a later date. The small number of respondents disagreeing with this proposal did so on the grounds that they were not anyway in support of non-domestic opt-out (Q15). Therefore the need to switch communications hubs should not arise. They noted that an opt-in / out option might significantly impact the overall consumer experience, in terms of cost, continuity of service and loss of interoperability. A number of other points were raised by respondents from all categories: • that continued flipping between opt-in and opt-out could be extremely costly and disruptive, and to be discouraged; • the difficulties faced by the gaining supplier in passing on the costs to the consumer may cause the supplier to avoid that market sector and thus limit competition;

	• the gaining supplier may have no choice but to continue an opt-out arrangement if a separate long term contract with an MSP is already in place; • this is an intelligent and informed market sector, with significant investment in advanced metering. They will understand and accept a model provided it is fair and equitable; and • (in parallel to the response to Q15) the approach should be reviewed once the smart metering roll-out is underway and in the light of emerging experience.
Q17	**Do you agree that the design and implementation of outage reporting functionality should be assigned to CSPs, documented in the communications hub technical specification?** The great majority of respondents to this question agreed that the design and implementation of outage reporting functionality should be assigned to the CSP(s). However, a substantial number caveated their responses by questioning whether this functionality should sit in the communications hub, or elsewhere in the CSP's physical infrastructure, and hence whether it needed to be included in the CHTS. Several respondents drew a distinction between outage detection (determining that power has stopped), and outage reporting (determining that the outage has been longer than three minutes). They argued: • that the communications hub is the logical place to provide outage detection. However, this requires that the communications hub itself continues to operate with no external power source; • this requires either a battery, or a super-capacitor to generate a 'last gasp' alert; and • to provide either would increase the cost of the communications hub. At least four respondents believed this was a significant cost driver, adding pounds to the cost of the communications hub. The CSP would then use other elements of the CSP WAN infrastructure to deliver outage reporting. For example, the WAN infrastructure will recognise the last gasp alert, and will also recognise when power has been restored. These data points would enable the CSP to determine centrally whether an outage has occurred, and to report this. Respondents who raised this concern agreed that the CSP(s) should decide on the optimum approach to outage reporting, as they would be best placed to determine the least cost solution. Two respondents disagreed with the proposed scope. One did not accept the need for outage reporting and a second believed that the meter should have responsibility for outage reporting, not the communications hub.
Q18	**Do you agree that it would be inappropriate to require meters operated outside DCC to be required to implement outage reporting? Please provide rationale to support your views.** The small majority of responses to this question supported the proposal that meters operated outside the DCC should not be required to implement outage reporting. Many noted the complexities would make this impractical for opted-out non-domestic consumers. Others confirmed that 100% coverage of outage reporting is not required as outages affecting meters outside the DCC can rely on adjacent

	opted-in meters to act as a 'proxy' - especially if the opted-out population remains at its current low levels. One respondent argued that it would be more practical to fit only a proportion of meters (including the domestic population) with this capability to reduce the amount of traffic on the network and to keep costs down. Most of the dissenting responses came from DNOs or industry bodies, and focused on the benefits of outage reporting in fault management and resolution. In the event of a low voltage network fault, it is generally the non-domestic properties that are hardest to verify outage conditions or confirm power restorations. In addition, a partial data set reduces the effectiveness of fault finding and restoration planning. They also argued the potential customer service benefits which result from complete visibility of their supply status, especially for outages occurring outside business hours. Should a customer have a meter which is opted out and is incapable of outage reporting, suppliers should be obliged to highlight this arrangement and ensure that the customer is aware that they will manually need to contact the DNO to notify them of any unplanned outage. One respondent noted that a SMETS 2 meter may be enrolled into the DCC at any time in its lifetime (subject to complying with the adoption and enrolment criteria) therefore all meter points should include outage reporting functionality. However, that it should only be used when the meter is connected to the DCC.
Q19	**Do you agree that maximum demand registers should be included in SMETS? Please provide evidence to support your position and provide evidence on the cost implications of delivering this functionality via back office systems or via the meter.**
Q20	**Do you agree with the proposal not to include the capability to generate additional voltage alerts based on counter thresholds in SMETS 2? Do you have any evidence that could justify including this functionality in SMETS 2?**
Q21	**If DNOs were permitted to access remote disablement functions, should control logic be built into DCC systems or meters? If the logic should be built into meters, should the logic be specified in SMETS 2? Please provide rationale to support your position including estimates of the cost of delivering this functionality under the different options being considered and any evidence relating to safety issues associated with each option.**
Q22	**Do you agree that variant smart electricity meters should be specified in SMETS 2 and that the cost uplift for variant smart meters is similar to that for variant traditional meters? Please provide evidence of costs to support your views on cost uplifts.**
Q23	**Do you agree that randomisation offset capability should be included for auxiliary load control switches and registers as described above? Do you have views on the proposed range of the randomisation offset (i.e. 0 – 1799 seconds)? Please provide evidence on the cost of introducing this functionality.** These questions were addressed in Part 1 of the Government Response to the SMETS 2 Consultation.

Q24	**Do you support Option 1 or Option 2 for 'pairing' a CAD to the HAN? Please present the rationale for your choice and your views on the implications that these options have for the technical design of the solution.** The great majority of respondents supported Option 2 for 'remotely pairing' a CAD to the HAN, although for many it was a marginal decision, and significant caveats were noted. Respondents noted that Option 2 is potentially more secure, and follows the procedure for installing meters and the IHD. They also noted that Option 2 was the 'least worst' option, given a number of potential problems with Option 1 (local pairing), which would require: • a change to the current ZigBee security requirements, as these currently state that an install code and MAC address must come from a trusted device. Therefore a CAD cannot send its own pairing information. This is likely to impact programme timescales; • that suppliers maintain a database of passkeys and perform address verification for consumers who move house and / or forget their passkeys. This is an unknown, and potentially increasing, workload; • that a DCC service will still be required to send messages to reset passkeys on communications hubs; • all CADs have keypads, or a connection to a device with a keypad. Minimum specification IHDs could therefore not be connected without a supplier visit, and the opportunity for innovation in the market for 'simple' CADs and IHDs, limited; and • that a button is added to all communications hubs. A consumer group also noted that Option 1 would risk giving suppliers a competitive advantage in the market for energy servicers, as the consumer is likely only to request reissue of a passkey when they are interested in a new energy service from a third party. A small minority of respondents favoured Option 1. They noted that the requirement for CAD pairing is likely to increase through time (particularly with the advent of electric vehicles), and the process must therefore be quick and easy. Notwithstanding the need for security, Option 1 could offer a simple process to the consumer, by phone or internet, and that consumers are capable of handling their own keys with due diligence. By contrast, Option 2 would introduce one or more third parties into the loop, and place an obligation of 'customer authentication' upon them, would take more time, and would introduce a need for a new, high-priority near-real-time messaging requirement on the DCC and its Service Providers.
Q25	**If Option 2 were adopted, do you agree that obligations should be placed on energy suppliers to support this process by submitting 'pairing requests' to the DCC on request from their consumers?** Respondents to this question who expressed any preference were equally split, with a significant third group commenting on the different options but not expressing a choice. All showed a mix of responses from different sectors, and no one group showed any bias towards a particular one. Those supporting the proposal that an obligation should be placed on energy

	suppliers to support pairing noted: • that the consumer already has a relationship with their supplier – but not with any other potential party such as the DCC, DSP or CSP – and is therefore more likely to trust the process; • under their existing licence conditions, the supplier is responsible for managing all consumer data in a secure and private environment, an obligation which would apply to any data arising from pairing requests; • submission of a pairing request offers the supplier a further engagement opportunity to strengthen the consumer relationship; and • this model is already widely used in both Texas and Australia, which have a similarly deregulated utilities market. Although supportive of a supplier-based approach, a number of respondents noted the need to place an obligation on suppliers to operate a consistent, efficient and consumer friendly process for pairing requests. Others were concerned about address verification (noting that this issue would be more significant should an independent third party offer a pairing service). An equal number of respondents disagreed with the proposed approach. Some had supported Option 1 (local pairing) in their response to Q24, and therefore saw no need for a pairing service. Others argued that it was inappropriate to place an obligation on a supplier to take unbounded responsibility for the workload and costs of supporting what should be a commercial service. Respondents argued variously that this should instead be placed on the CSP, DSP, or supplied as a commercial offering via a SEC party. The third group of respondents who did not express a preference focused instead on the importance of understanding the underlying technical options for pairing (particularly the security issues), arguing that these needed to be agreed before the need, and responsibility, for a pairing service could be decided.
Q26	**Do you consider that other CAD installation options should be pursued? If yes, please explain the approach you favour and your reasons.** Very few respondents addressed this question. Proposals included: • a variant option for local pairing which would allow entry of a unique passkey and security codes on a trusted device (e.g. an electricity meter) to address security concerns; • pairing solutions based on Near Field Communications; • the provision of simple push button solutions on all devices; and • the inclusion of a consumer HAN chip in all communications hubs.
Q27	**Do you agree with the proposal to include in SMETS 2 a specification for a PPMID, connected via the HAN, as described above?** The great majority of respondents were strongly in support of including a specification for PPMID in SMETS 2. Respondents noted that this would provide a more accessible interface to prepayment functions than that offered by meters alone. Two respondents suggested that PPMID functionality could more economically be incorporated into the IHD. However, other respondents raised a range of concerns

	with this approach, including the potential difficulties in specifying such an option, and the poor economic case for the mass introduction of a requirement to serve only a small proportion of consumers requiring a PPMID. One respondent suggested that an interface could be achieved using a smart phone, or the supplier's portal. Two respondents questioned whether credit could be transferred securely through the HAN between a PPMID and the smart metering system.
Q28	**Would including the capability to enable gas and electricity supply through a PPMID connected via (a) a wireless HAN or (b) a wired HAN meet GB safety requirements? What impact would including this capability have on the cost of smart metering equipment? Please provide evidence to support your answers.** The great majority of respondents were strongly in agreement that a consumer's electricity supply could be re-enabled safely using a PPMID via the wireless HAN. However, respondents expressed significant concerns over the extension of this functionality to gas. One stressed the risk of enablement under software control, since this might increase the risk of malicious attach via the internet – allowing a hacker to deliberately disable and then re-enable a gas supply with the specific intent of causing gas to flow without a pilot light to consume it. Five respondents accepted remote enablement for gas if the safety case can be proven, whilst two additional respondents noted this is already the case with examples in many countries worldwide. Very few respondents discussed the cost impact on smart metering equipment. One respondent noted that more generally, the economic case for prepayment is poor when considering the additional costs of contactors and valves in meters, in addition to the provision of PPMIDs. One respondent suggested that a hardware security chip should be added to a PPMID, which would add to the component cost.
Q29	**Do you agree with the proposal that the communications hub should be specified such that it can support multiple smart electricity meters? How many smart electricity meters should be supported by each communications hub?** The great majority of respondents were in favour of support for multiple smart meters. They argued that this is essential to enable the industry to deal with an increasing range of microgeneration deployments. One respondent noted the importance of an appropriate security architecture, and a minimal data interface. One respondent disagreed with the proposed approach, arguing for a single meter per hub on the grounds of cost and complexity. The question about how many meters should be supported was deliberately open, and encouraged a wide range of responses, from zero to unlimited. Two broad groupings emerged: the great majority of those who responded were in favour of no more than four meters–per-hub, and based this on market / operational experience. The remaining respondents favoured between eight and an unlimited number of meters. No respondent directly mentioned the cost as the deciding factor; the main concerns

	being the practicalities of implementation on the ground, and the typical number of meters found in consumer premises. Respondents noted that there is little point in building in capacity which will never be used.

Q30	**Do you agree that a specification for a HHT interface to the HAN should be defined? If yes, please identify the functions that this interface would need to support and the scenarios in which such functionality could be required.**
	
	The great majority of respondents agreed that a specification for a HHT interface to the HAN should be defined. A small number disagreed, principally on the grounds of potential security issues, but also noting that more efficient and cost effective ways of installing smart meters were available.
	
	A wide range of functionality and the scenarios in which such functionality might be deployed were identified (numbers in brackets represent number of respondents identifying this option):
	
	• Connection to SMS
	  • HHT authentication, including NFC authentication of HHT [1]; a requirement to work when WAN not present to authenticate HHT [1]; and HHT authentication [2]
	  • HHT communications interface, including a separate interface for the HHT, not the HAN on the comms hub [1]; an optical HHT interface [4]; and a ZigBee interface [1]
	• Installation and maintenance
	  • Meter installations, including support for them [9]; that they are not required for installation [2]; to initiate the commissioning process and MPxN association [8]; to configure an auxiliary load control switch [1]; quick installation [1]; to decommission equipment [1]; and for local pairing of HAN devices / to configure HAN [7]
	  • Maintenance, including support for this activity [6]; restoration / configuration of meter settings [2]; SMS firmware upgrade [3]; read / write operations (both price changes and TOU) [1]; tariff configuration [1]; and fault diagnosis [2]
	• Prepayment
	  • Exclude function to apply credit [3]
	  • Emergency top-ups [3]
	  • Configure non-prepayment mode [1]
	  • Full prepayment support [2], including issue of new PAN number, debt amount and repayment rate adjustment, application of credit to meter, adjustment of emergency credit, wiping down a meter (COT etc), taking a meter ‘snapshot’, loading a new tariff configuration, resetting the meter bypass flag (Revenue Protection only function), changing / updating the internal meter clock, and opening / closing the gas meter valve.
	• Security
	  • Update security [1]
	  • List of functions tightly controlled, can only be performed by authorised HHTs [2]

	• Configure SMS security [1]
	• Security based on PPMID [1]
	• Exclude write functions [1]
	• Others
	  • Test mode [1]
	  • Involve games companies in developing HHTs with augmented reality features [1]
	  • Mirror all functionality of the DCC except UTRN [1]
	  • Support for HHT is optional [1]

Chapter 5 - Governance and Assurance of Security and Interoperability	
Q31	**Do you agree with the proposed approach to the governance of security requirements? If you propose alternative arrangements please provide evidence to support your views.** The great majority of respondents across all stakeholder groups agreed with the need for, and importance of, effective governance of security requirements; only one respondent (a small energy supplier) disagreed, expressing concerns regarding the demands the proposed approach would place on small suppliers. Respondents expressed general agreement for the establishment of a technical sub-committee to maintain security requirements. A number strongly emphasised the importance of representing both Government and industry as a whole within the committee, and for the technical sub-committee to perform in a more transparent way to how STEG is currently operating. Considering the governance of the SEC Panel and sub-committee, a number of respondents noted that measures such as definition of roles and responsibilities, approval and escalation processes, Terms of Reference and drafting of obligations, will be needed. Several respondents noted the need for focus on the significant potential security risks inherent within remote disconnection. Two respondents from the energy networks sector felt that little information had been provided on how security requirements were being mapped to risks, in order to ensure full coverage of the risks to smart metering, and that it would be useful to share this exercise with the technical sub-committee. Other points raised by respondents included: • concerns over the financial implications of the proposed approach on small suppliers, with a request that consideration be given to the running costs of the panel and the benefits it would provide; • that security requirements were not prescriptive enough; and • that the term ‘end-to-end’ needs clarification, specifically what the ‘ends’ of the smart metering system are considered to be and what impact this has on security.
Q32	**Do you agree with the proposal to establish independent assurance procedures for DCC and DCC users? Please explain your views and provide evidence, including cost estimates where applicable, to support your position. Comments would also be welcome in relation to the impacts and benefits of**

	the proposed approach with regard to small suppliers. The great majority of respondents were supportive of an independent assurance regime for DCC and DCC Users, with a number agreeing that it would provide an important level of consistency and confidence in the security of smart metering systems. However, several of the large energy suppliers and an industry body queried whether security obligations within the same role code would be scaled for smaller suppliers, whilst another respondent suggested that there should be a minimum level of requirements that all suppliers should be subjected to. The majority of stakeholders tended to focus on assurance procedures for DCC users, providing little comment (other than to express their agreement) with the introduction of assurance procedures for DCC systems and services. Some respondents, especially amongst the energy networks sector, queried the differences between a role-based and risk-based approach, and whether the two were mutually exclusive. Opposition to the proposed approach was minimal and from no one single group. Although generally supportive of independent assurance procedures for the DCC, a single small supplier expressed concerns over the potential financial implications of an independent assurance regime for DCC Users, and noted that existing supplier assurance methods should be sufficient. Others unsupportive of the proposal noted that a role based approach in isolation was inadequate, and that certification against security standards would only provide assurance that the certification process had been followed, but not that the system itself was secure.
Q33	**Do you agree with the proposal that re-testing should occur at least at set intervals and more frequently when significant changes to systems or security requirements are introduced? Please explain your views.** The great majority of respondents to this question were in agreement with the proposal for event-based testing triggered by a significant change, but were less supportive of re-testing at set intervals. Meter manufactures and energy suppliers in particular considered that any need for re-testing should be determined either through pre-determined criteria, or through a risk assessment. Some parties in favour of Government's proposal for time and event based re-testing (particularly those in the communications and technology sectors) expressed views that re-testing was necessary to identify emerging risks and threats that could impact smart metering. A small minority of respondents disagreed with the proposal. A large energy supplier suggested that the risks were not commensurate to justify the costs of time based testing, and that annual self-assessment should be sufficient where there had been no changes to previously certified systems or processes. A small energy supplier noted that existing supplier assurance measures should be sufficient. Some respondents also requested that Government define both the length of the proposed intervals, and 'significant change'.
Q34	**Do you agree with the proposal to establish an independent security certification scheme for smart metering equipment? Do you have any views on the proposed approach to establishing a certification scheme or evidence of the costs or timelines for setting up such a scheme or submitting products**

	for certification? The great majority of respondents to this question agreed with the proposal to establish an independent certification scheme for smart metering equipment, although meter manufactures and communication and technology bodies were the least convinced by the suggested certification approach. A sizeable number of respondents agreed with the importance of independent certification, but did not mention CESG's Commercial Product Assurance (CPA) scheme (given as an example of the type of equipment certification scheme Government is considering) directly in their answers. A few respondents expressed concerns over the impact of using the CPA scheme for which smart metering characteristics have yet to be developed, and noted their desire to consult with DECC further on the assessment of the eligibility for enrolment of SMETS 1 meters through the proposed certification scheme. Some respondents suggested that existing certification criteria (i.e. the Common Criteria Protection Profile developed by the German Federal Office for Information Security) could be leveraged by Government when considering the choices for a certification scheme. A number of respondents requested clarification of the cost of certification. Several respondents who were in favour of the proposal caveated their response, concerned that a limited number of CESG approved test houses could cause a bottleneck for suppliers seeking to certify equipment, and emphasising the potential resulting delay. Others suggested that the procurement of test houses should be a competitive process to facilitate the development of a range of cost effective and skilled providers. A small minority of respondents were undecided in their approach for certification. One communications and technology body felt that certification should not be regarded as a one-off process, and disagreed with the use of independent test houses. They argued that DCC systems would consist of complicated components, specific to the manufacturer that developed the equipment, and this would make it hard to develop a standardised test. A consumer body agreed with the need for independent certification but felt that assurance of independent components was insufficient, and a holistic approach to testing of the end-to-end smart metering system was preferable. Others suggested that the purpose of certification provided assurance both to the DCC, and to all other stakeholders.
Q35	**Do you agree that sanctions for non-compliance with security requirements should be included in the SEC? Do you have views on the nature of the sanctions that might be imposed?** The great majority of respondents to this question emphasised the importance of sanctions for non-compliance with security requirements, and agreed with the proposed approach. Respondents felt that sanctions should be proportionate to the risk, transparent, not discourage self-disclosure and that the impact to the consumer should always be considered before a sanction is applied. Some believed that rapid remediation of an issue should be the priority, and that the speed in which an issue was remediated could be a deciding factor in the sanction imposed. Some respondents noted the need for clear separation between the proposed sanctions and existing regulations,

	especially where liabilities are concerned. A number suggested a hierarchy of sanctions, with removal from the DCC being the final and most extreme option. Only one respondent disagreed with the proposal, suggesting that sanctions would not be required if certification were performed correctly.
Q36	**Do you agree with the proposal to, in effect, extend the arrangements already proposed for SMETS installations prior to DCC operation, to all installations being operated outside DCC? Please provide evidence of the costs that might be incurred and the impact of this approach on small suppliers.** The majority of respondents were supportive of the proposal that the existing security obligations for SMETS installations should be extended to all installations operated outside the DCC. Some noted that this approach would enable standardisation across installations and benefit interoperability. Others highlighted the reputational risk of a security breach involving smart metering equipment, regardless of whether the equipment was operated by the DCC or another party, thereby reinforcing the case for consistent security obligations. Some respondents sought clarification of the operation of the proposed arrangements. A number suggested that the obligations placed on suppliers operating SMETS equipment outside DCC should depend on the level of risk that they pose to rest of the smart metering system. A small number of respondents (particularly from meter manufacturers and large energy suppliers) were confused over the scope of the proposed extension of arrangements. For example, whether security obligations would be placed on non-domestic suppliers operating non-SMETS equipment outside of the DCC. A non-domestic supplier suggested that smart meters that were operated outside of the DCC posed little risk to the market and instead emphasised the importance of access to consumption data, stating that this would be core to the continued provision of competitive energy services. The respondent did however recognise the need for security, and recommended the approach be proportionate in order to provide sufficient protection, but not restrict access to consumption data. A non-domestic industry body agreed, emphasising that access to consumption data was key and suggesting that the approach to security for non-domestic suppliers should be proportionate so as not to impose unnecessary security burdens on the non-domestic sector in response to challenges faced by the domestic sector. Of the minority of the respondents that disagreed with the proposal, some were of the opinion that there was little benefit to the suggested approach, and others felt it was premature to review these arrangements before the equipment certification processes are fully developed. Some raised concerns around retrofitting security requirements to non-SMETS 2 equipment.
Q37	**Do you agree that interoperability is central to the development of a successful smart metering solution and that activities related to the assurance of SMETS equipment should be governed by SEC? Please provide views on the governance arrangements that would be appropriate for assuring interoperability of smart metering equipment.** All respondents who addressed this question agreed that interoperability is central to the development of smart metering, and all except one, that assurance should be

	governed by the SEC. A single respondent noted that the SEC is a natural place for such a governance body to sit. However, there is no immediate need for this, as the natural commercial incentives of the industry parties such as the CSP(s) and MAPs will ensure the right testing programme is in place. A range of views were submitted on the governance arrangements needed to ensure smart metering equipment interoperability. Manufacturers expressed a desire to be involved through industry bodies in the governance arrangements. Network operators wanted to include the physical dimensions in the specifications to further improve interoperability and replacement.
Q38	**Do you agree with the creation of an 'approved products' list and the requirement on suppliers and CSPs to obtain, retain and provide evidence of appropriate certification should apply regardless of whether they intend to enrol the equipment in DCC?** A majority of respondents agreed with the creation of an 'approved products' list, although a number noted the potential difficulties in keeping such a list up to date. Of the respondents who expressed any preference, the majority agreed with the proposal that suppliers and the CSP(s) should certify equipment regardless of their intention to enrol it in the DCC. However, the majority of respondents expressed no clear preference on this matter. One supplier noted that the onus should be on suppliers to provide evidence that they assure meters not enrolled in the DCC. Some respondents noted that the DCC / SEC should be responsible for creating and maintaining an 'approved products' list, and a supplier developed this point further that this responsibility should fall wholly on the DCC (and not on suppliers) as they will allow enrolment only if the equipment is on the approved list.
Q39	**Do you agree that protocol certification (against a GBCS) should provide adequate assurance that a product will meet interoperability requirements? Please explain your views and identify any additional assurance testing that you consider to be necessary and the rationale for including such testing.** Responses to this question were divided. A very slight majority of respondents agreed that protocol certification on its own would provide adequate assurance that a product will meet interoperability requirements. However, a significant minority noted that whilst it is an important component of assurance testing, protocol certification on its own will be inadequate to ensure interoperability. Views included: • other factors, such as functional performance, will be required in addition; • physical device / HAN / WAN unit testing should be conducted with devices from different manufacturers / suppliers – a number of / all use cases should be tested to guarantee interoperability as some incompatibility issues will only appear under certain conditions based on experience; • protocol testing will show that communications within the device work, but not that a device has performed the functional action; • a robust framework for parties to operate under will be needed to ensure protocol testing delivers in a joined up way; • retesting should be required after any hardware or software upgrades;

	• the certification body would need to be involved in developing the GBCS; and • all specifications need to be unambiguous, otherwise this could increase the risk of variation and reduce the likelihood of interoperability. One respondent argued that two protocol testing was not required, but provided no supporting evidence for this view.
Chapter 6 - Operational licence conditions	
Q40	**Do you agree with the Government's proposals to require energy suppliers to operate specific aspects of smart metering equipment functionality for domestic consumers? Please provide rationale to support your position.**
Q41	**Do you agree that the licence conditions as drafted effectively underpin the Government's policy intentions for consumer operational requirements?**
Q42	**What are your views on the Government's proposals to require energy suppliers to operate specific aspects of smart meter equipment functionality for micro-business, but not other non-domestic, customers?**
Q43	**What are your views on the Government's proposals for obligations to be included in the SEC for information to be made available to Network Operators and ESCOs via the DCC?**
Q44	**Do you agree with the Government's proposals for the timing of the introduction of operational requirements? Please explain your reasoning** These questions were addressed in Part 1 of the Government Response to the SMETS 2 Consultation.
Chapter 7 – Next Steps	
Q45	**Do you agree with the proposed changes to the smart metering regulatory framework to reflect the CSP-led model for communications hub responsibilities? Are any other changes necessary?** The great majority of respondents agreed that the CSP-led model for communications hub responsibilities should be reflected in the DCC licence and CHTS. A small minority of respondents did not support the proposed approach, in each case reflecting their overall disagreement that the CSP(s) should be responsible for the communications hub arguing that supplier provision of the communications hub would be more efficient (Q14). Respondents also noted that the DCC licence requirement would have to backed off through service provider contracts and that the roll-out licence condition should also be amended to reflect the requirement on suppliers to install the communications hub provided by the DCC. Suppliers repeated concerns relating to the maintenance of the communications hub which they also raised in response to Q14.
Q46	**Do you agree that the equipment development and availability timelines are realistic? Please give evidence.**

	The majority of respondents to this question agreed that the development and availability timelines set out in the Consultation Document were realistic. A number of caveats were raised by those that agreed, the main ones being: • supporting information may not be available in time (e.g. the release date of specifications); • certification and testing could take longer than expected (6-9 months); and • the possibility that there could be further security changes. One respondent stressed the importance of providing clear and updated timelines as soon as possible in the case of any changes to timelines, as this would allow stakeholders to assess the risks from a funding viewpoint in the event of a prolonged foundation period. A significant minority of respondents disagreed that the timescales were realistic. The main reasons given were: • the potential impact of emerging/changing security requirements; • a failure to take into account Suppliers' internal testing and trialling requirements; • the lack of availability of sufficient testing resources; • a lack of confidence in timescales for completion of Programme specifications; • insufficient time allowed for end-to-end testing.
Q47	**Do you agree that SMETS 2 should only be designated when the Government has confidence that equipment to satisfy the new requirements is available at scale? Should a further period of notice be applied to ensure suppliers can manage their transition from SMETS 1 to SMETS 2 meters?** A substantial majority of respondents agreed that SMETS 2 should only be introduced when the Government has confidence that equipment to satisfy the new requirements is available at scale. There were two main caveats around this agreement. The first of these was that there should be a clear definition of 'at scale'. Most respondents defined this as meaning that equipment would be available from two or more manufacturers and that interoperability of equipment would have been demonstrated through the testing and certification process. One respondent also believed that, ideally, the DCC should be in place as well. The second caveat was that there should be a short transitional period to avoid stranding SMETS 1 Meters; suggestions ranging from a period of six to twelve months. A number of respondents suggested that, rather than have a strict date after which SMETS1 meters would not count towards roll-out obligations, volume limits should be applied from that date for a set transition period. Some respondents suggested that the SMETS 2 introduction date should be decided as soon as possible, with provisions for the slippage of any dates in the plan. One respondent disagreed with the proposal, believing that SMETS 2 should be introduced now and transition encouraged immediately.
Q48	**What are your views on when responsibility for the SMETS modifications process should transfer from the Government to the SEC?** The majority of respondents to this question agreed with the Government's proposed approach of transferring governance of the SMETS to the SEC when a

	stable version of SMETS is available which can deliver the Smart Metering business case and when robust SEC governance structures are in place. A significant minority were of the view that the transfer of SMETS governance should take place at a later stage (although in the main did not say when this should be). Very few supported an earlier transfer. A number were of the view that transfer should be conditional on SEC governance being fully operational. Some also argued that responsibility should not be transferred until SMETS compliant equipment had been deployed for a period of a year or more.
Q49	**Which of the options (standing sub-committee or non-standing sub-committee) would you prefer in relation to modifications to the SMETS?** A substantial majority of respondents to this question favoured the creation of a standing technical sub-committee with responsibility for SMETS modifications within the SEC, and that this should be able to call on additional expertise where necessary. Respondents argued that a standing sub-committee would maintain core expertise and provide consistency and continuity. A number caveated their response by suggesting that these arrangements would be required at least in the initial period following transfer of SMETS governance to the SEC, as a high level of proposals for modifications to SMETS could be expected at this time. However, the SEC could consider moving to a non-standing committee at a later stage if the volume of proposals for SMETS modifications was to fall to a low enough level. Only a small proportion expressed a preference for a non-standing committee at the point at which SMETS governance is transferred to the SEC, on the grounds of cost issues and the possibility that a standing committee would be less open to innovation. A few expressed the view that the decision on whether this sub-committee should be standing should be left to the discretion of the SEC once it is established.
Q50	**Are there any particular areas of expertise that the sub-committee will need to fulfil its role, in terms of membership composition?** Respondents drew attention to the wide range of expertise that would be required for SMETS governance. Many recommended that membership should be carefully selected to represent interested parties and relevant skills while some noted that recognised experts could be called upon depending on the subject matter of the decisions that needed to be taken. The current SSAG, with its independent Chair and Secretary, was mentioned as a possible model for the sub-committee. Reference was also made to the importance of retaining the knowledge and expertise that had been developed during the lifetime of the Smart Metering Implementation Programme. A number of respondents identified the need for inclusion of the CSP(s) and DSP as well as representation from SEC parties in the sub-committee. Representation of meter and communication device manufacturers and asset providers and installers were also suggested. Others focused on required expertise rather than on involvement of particular bodies. Security was the most frequently occurring specialism identified by respondents, by a large margin, followed by testing and certification expertise.

	Other specialisms included metering and communication design and manufacturing, software and firmware design, wireless communication and communication standards, interoperability and systems integration, data privacy and equipment financing.

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

www.gov.uk/decc

URN 13D/006