

## Memorandum

**To** Margaret Coaster, Smart Metering Team Ofgem E-serve smartmetering@ofgem.gov.uk

**cc**

**Prepared by** [REDACTED]

**Subject: Response to Ofgem Smart Metering Implementation  
Programme Prospectus July 2010**

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Suggested Approach and Solution for Parts of the Smart Metering System</b>	<b>4</b>
2.1	Open Modular Interface, for meters, gateways, IHDs and appliances	4
2.1.1	UMI - Contribution and Offer from Cambridge Consultants	5
2.2	HAN Lifetime	6
2.2.1	Licensed v Unlicensed RF Bands	6
2.3	HAN Ownership, Two HANs, Gateway Interfaces.	7
2.4	Security	9
<b>3</b>	<b>Risks to The UK Smart Metering Programme</b>	<b>10</b>
3.1	Reliability of the HAN solution	10
3.2	Achieving sufficient energy reduction to justify the national investment	10
3.3	Inadequate Definition and Testing of the Smart Metering System Security	11
3.4	Full Interoperability of Equipment and Systems is not achieved	12
3.5	The Organisation and contribution to the Programme not optimal	12
3.6	Consumer Acceptance – Risk of Rejection	13
<b>4</b>	<b>Response to Specific Questions Raised in the Prospectus</b>	<b>14</b>
4.1	Prospectus – 28 September and 28 October	15
4.1.1	CHAPTER 2, The Consumer Experience, Questions 1-5	15
4.1.2	CHAPTER 3, Industry Roles & Responsibilities, Questions 6-15	16
4.1.3	CHAPTER 4, Implementation and Next Steps, Questions 17-20	37
4.2	94a/10, Consumer Protection - 28 October	40
4.2.1	CHAPTER 2, Developing services for consumers, Questions 1-5	40
4.2.2	CHAPTER 3, Prepayment and remote disconnection, Questions 6-15	40
4.2.3	CHAPTER 4, Vulnerable consumers and fuel poverty, Question 16	41
4.2.4	CHAPTER: 5 Cost recovery and monitoring of costs, Question 17	41
4.3	94b/10, Statement of Design Requirements - 28 September	42
4.3.1	CHAPTER 3, Overview of the Smart Metering System Functional Requirements Catalogue, Questions 1-6	42
4.3.2	CHAPTER 5, Achieving Technical Interoperability, Questions 7-10	43
4.4	94c/10, In-Home Display - 28 October	45
4.4.1	CHAPTER 2, Functional Requirements of the IHD, Questions 1-6	45
4.4.2	CHAPTER 3, Nature of the Mandate on Suppliers in relation to the IHD, Questions 7-8	46
4.5	94d/10, Communications Business Model - 28 October	47
4.5.1	CHAPTER 2, The Scope of DCC, Questions 1-4	47
4.5.2	CHAPTER 3, The Structure and Realisation of DCC, Questions 5-8	49
4.6	94e/10, Data Privacy and Security - 28 October	51
4.6.1	CHAPTER 3, Data Privacy, Questions 1-4	51
4.6.2	CHAPTER 4, Smart Metering System Security, Question 5	51
4.7	94f/10, Implementation Strategy - 28 September	53
4.7.1	CHAPTER 2, Programme management and governance, Question 1	53
4.7.2	CHAPTER 3, Programme activities, Question 2	53

## Memorandum

4.7.3	CHAPTER 5, Proposals requiring changes to the regulatory framework, Questions 3-8	54
4.8	94g/10, Rollout Strategy - 28 September	56
4.8.1	CHAPTER 2, Approaches for Rollout, Questions 1-3	56
4.8.2	CHAPTER 3, Mechanisms for General Consumer Engagement, Questions 4-5	56
4.8.3	CHAPTER 4, Obligations on Suppliers to Complete the Rollout, Questions 6-9	57
4.8.4	CHAPTER 5, Prioritisation of Specific Consumer Groups, Question 10	57
4.8.5	CHAPTER 6, Reporting Arrangements, Question 11	57
4.8.6	CHAPTER 7, Consumer Issues, Questions 12-13	58
4.9	94h/10, Regulatory and Commercial Framework - 28 October	59
4.9.1	CHAPTER 2, Smart Metering Regulatory Regime, Question 1	59
4.9.2	CHAPTER 3, Smart Energy Code, Questions 2-4	59
4.9.3	CHAPTER 4, Roles and responsibilities at customer premises, Questions 5-7	59
4.9.4	CHAPTER 5, Other regulatory and commercial issues, Questions 8-11	61
4.9.5	CHAPTER 6, Impact on wider industry processes, Questions 12-15	62
4.10	94i/10, Non-Domestic Sector 28 October	63
4.10.1	CHAPTER 3, Flexibility for installations of advanced and smart meters, Questions 1-3	63
4.10.2	CHAPTER 4, Use of DCC to communicate with meters in the smaller non-domestic sector, Questions 4-8	63
4.10.3	CHAPTER 5, Other issues related to non-domestic customers, Questions 9-11	64

## Memorandum

### 1 Introduction

This memorandum presents Cambridge Consultants response to the Ofgem Smart Metering Implementation Programme Prospectus published in July 2010.

There are three main sections :

- Section 2 describes our suggested approach and solution for certain parts of the overall Smart metering system and programme. These are in line with the Prospectus documents but do not correspond one-to-one with particular section of questions asked.
- Section 3 lists our concerns on the major risks to the UK Smart Metering Programme.
- Section 4 gives our response to the 28 September deadline questions including the Functional Requirements Catalogue.

In this later version of the document our response to the 28 October deadline questions has been added to Section 4.

Change bars on the left side of the page indicate where text has been added since 28 September 2010 version eSmart-TM-025 v1.1.

## Memorandum

## 2 Suggested Approach and Solution for Parts of the Smart Metering System

Here are a few key design ideas that we think should be considered for UK smart metering.

### 2.1 Open Modular Interface, for meters, gateways, IHDs and appliances

Starting the smart meter roll-out before the DCC is in place has created an explicit requirement for the early installed meters to have the capability to change their WAN interface to that specified by the DCC. The Prospectus describes the need for the programme to define with stakeholders the WAN communications module including the interface between the module and the metering system. (The "Communications Business Model" document on pp.6).

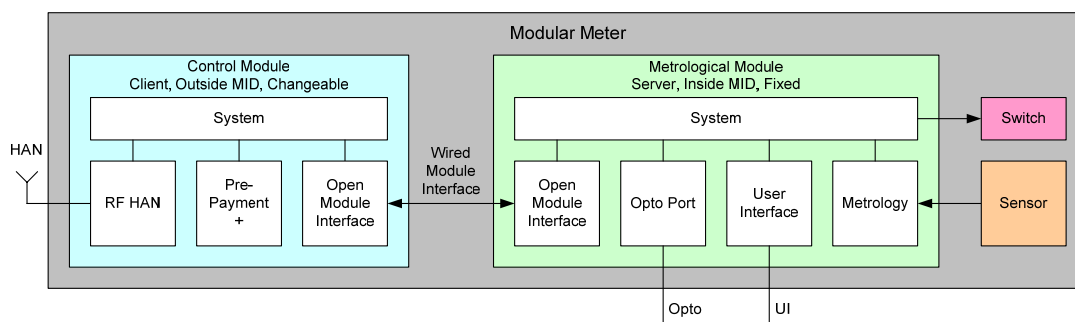
There are many technical challenges in this interface including:

- Security (a module interface provides a vulnerability point)
- Low power (Meter may be battery powered and the overall power budget for the metering system is low)
- Data representation. There are many different standards for the representation of meter data including DLMS, Zigbee SE and propriety. The interface must have an efficient and agnostic way of handling these
- Physically Robust. The module should be replaceable in the field
- Low cost. The module must be value engineered so it does not add significant additional cost compare to a non-modular solution.

The development of an interface standard and solution to these will take considerable engineering effort and time, at a critical stage in the Smart meter implementation programme when the Technical Specification must be defined before roll out can start.

UMI (Universal Metering Interface) is an existing open standard that meets all the requirements of the WAN module described in the Prospectus.

Our proposal is that the programme considers adopting UMI as a solution to the WAN module requirement and also for modularity on the HAN if required. This will save time and effort in the technical definition which is a priority for the overall programme. The diagram below shows how a modular meter could be developed :



## Memorandum

The requirements for all the modules on the right are stable, so that they can be developed now with a reasonably high degree of confidence. By contrast, the Control module on the left contains application, security and communications functions where the requirements are not at all stable yet. The Metrological module must be MID-approved, but thereafter will remain quite stable. The requirements of the Control module may continue to change for a long time, but they are all outside the metrological seal so that such changes never require any re-certification at the MID. The Metrological module acts as a Server to the Control module (which acts as a Client). The Metrological module operates correctly whether a Control module is fitted or not.

Such an architecture for a modular meter requires a defined wired interface between the two modules. It is best if this interface is open. UMI (Universal Metering Interface) is such an interface. We are happy to make the UMI specifications available to DECC and Ofgem for use in the UK Smart Metering project.

UMI can be used in meters, gateways, IHDs and appliances. Wherever there is a need to separate the stable functions from the unstable. It also helps European meter suppliers to manufacture their base products over a wider region and market. The metrological part of a meter can be constant across Europe, while the Control module can be varied from one region to another.

### **2.1.1 UMI - Contribution and Offer from Cambridge Consultants**

- UMI consists of 3 specifications that are available free. They are for :
  - Wired module interface (50 x 40 x 20 mm module based on SPI).
  - Opto interface (based on EN62056-21 FLAG port).
  - Security interface. Scheme 1 is symmetric (not preferred). Scheme 2 is asymmetric (preferred, but requires the system to contain at least one Certificate Authority).
- UMI has been developed by Cambridge Consultants and is being used in a major new smart gas meter for the European Market.
- UMI is owned by Cambridge Consultants but is open and free for organisations to use. Around 25 companies are using and/or evaluating UMI.
- Ownership of UMI will transfer to an independent non-for-profit Alliance when the users request this.
- UMI can be adopted by the UK Smart metering programme. The UMI Alliance will be formed to own and manage the standard for the stakeholder organisations in the UK programme. This is a genuine and open offer from Cambridge Consultants to the UK Programme. The standard has been developed specifically for Smart metering and we would like to Programme to benefit from this. It has been optimised for ultra-low power, as required by gas meters and other battery-powered devices.

## Memorandum

- The UMI specifications are already well developed and proven in a product. We are able to respond further if there are realistic extra features that would help the UK Smart Metering Programme
- Summary information on UMI is available at:

<http://www.cambridgeconsultants.com/umi>

[http://www.cambridgeconsultants.com/downloads/literature/UMI\\_overview.pdf](http://www.cambridgeconsultants.com/downloads/literature/UMI_overview.pdf)

The full specifications can be made available on request and we would be pleased to make a presentation, have calls or meetings as required to provide more information on the standard to the UK Programme and relevant expert groups.

## 2.2 HAN Lifetime

The Metering HAN should be backward compatible for 2 or 3 meter installations. i.e 30-45 years.

We don't think many people are thinking on this timescale yet.

### 2.2.1 *Licensed v Unlicensed RF Bands*

We are concerned that this timescale for backward compatibility might not be possible if the HAN is based on an un-licensed RF band, such as 868 MHz or 2.4 GHz.

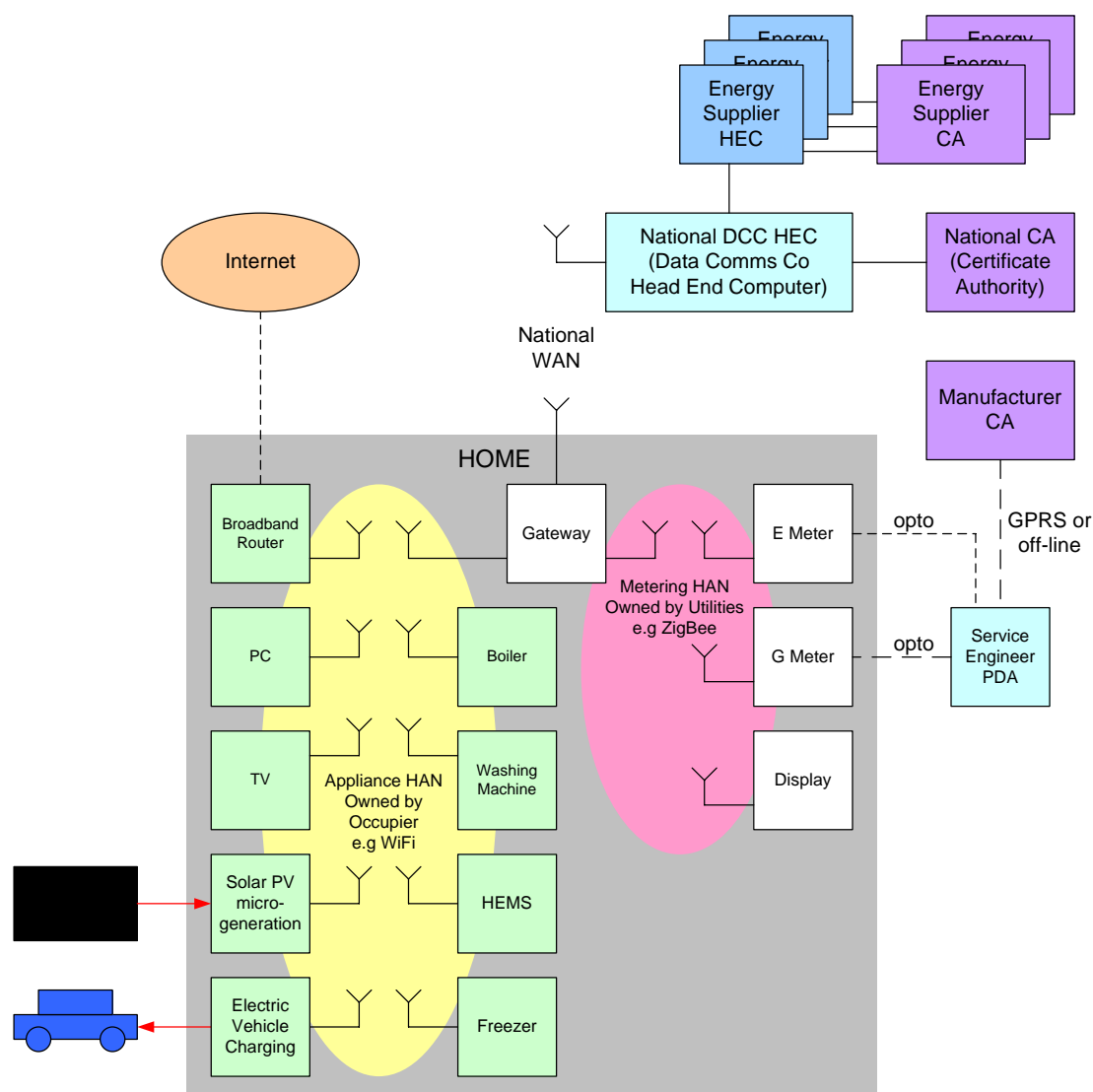
## Memorandum

### 2.3 HAN Ownership, Two HANs, Gateway Interfaces.

We think that a few years after the smart metering roll-out, a UK home might operate as shown in the diagram below.

The white boxes are not owned by the occupier. They are owned by a Utility or comms supplier. They are the smart metering devices that will be rolled out first. All homes will have them.

The green boxes are owned by the occupier. They are smart appliances that make use of the information from the new smart metering network. The smart appliances will vary from one home to another. Some homes will be early adopters, others will not get any smart devices.



It is important to note that the owner of a network has the right to turn it off or break it. This raises some interesting consequences as to how the networks should be organised in the home.

## Memorandum

In the diagram above, we have shown two separate HANs for these reasons of ownership :

- The pink network is the Metering HAN. This cannot be owned by the occupier. The Utility cannot allow the occupier to turn off the Metering HAN, so he cannot own it.
- The yellow network is the Appliance HAN. We think that many occupiers will not want to run their smart appliances on a HAN that they don't own. They will be scared of 'Big Brother' behaviour from the owner of the Metering HAN, who has the right to turn it off. The occupier will be much happier to run his own equipment on a network that he controls and owns. He might want to extend his existing WiFi network for this purpose.

We think that UK smart metering will not be a real success unless it achieves genuine reductions of energy and greenhouse gas. We don't think this will be achieved long time just through customer engagement via the IHD. We think that there needs to be more smart appliances that make more intelligent decisions by using the new information from the smart metering network. So it is vital that the smart metering network puts the technical and commercial hooks in place that encourage :

- Suppliers to offer new products and services for smart energy. We think it will be easier for them to do this if it is based on a HAN that doesn't require certification from the Utilities (which would be the case on the Metering HAN). There will be many more products and services developed if the barrier to entry is low. The Appliance HAN does this.
- Customers want to buy the above new products and services. We think that most will want to use a network that they own, so it can't be the Metering HAN. This implies that there must be another HAN, which is owned by the occupier. We have called this the Appliance HAN.

So we think that the Gateway should provide 3 defined interfaces :

- WAN. End point.
- Metering HAN. Network Coordinator.
- Appliance HAN. End point.

This is different from the proposal in the Prospectus, but we think that it should be considered seriously. We think it will lead to :

- Greater reductions of energy and greenhouse gases.
- Increased economic stimulation and growth of UK PLC.



## **Memorandum**

### **2.4 Security**

Clearly the security design for UK smart metering is of the utmost importance. As the meters have off switches, the potential consequences of a security breach are even more dire than they would otherwise be. We do not want a terrorist organisation to be able to crack the security system and then turn off every domestic electricity and gas meter in the UK !

Here are a few fundamental principles that we think will need to be adopted in the final security solution :

- Security should be based on an asymmetric key system, where every device has its own private & public key pair.
- Asymmetric cryptography should be used for :
  - Signatures
  - Key exchange (to establish a temporary session key)
  - Authentication
- Symmetric cryptography should be used for :
  - Encryption using the above temporary session key.
- UK should set up a PKI (public key infrastructure) to support smart metering.
- The DCC and other organisations (energy suppliers, equipment manufacturers, etc ) should each have their own CA (Certificate Authority). The hierarchy of trust between these CAs will have to be decided. We know that Europe is considering developing its own Super-CA that they hope would be trusted by each of the national CAs.
- UK should consider adopting ECC 256-primes for the asymmetric cryptography. It is used for the biometrics in European passports.
- UK should consider using AES-128 for the symmetric encryption (based on a session key set up by the ECC 256-primes).

## Memorandum

### 3 Risks to The UK Smart Metering Programme

We are concerned that there are still significant risks to the UK Smart Metering Programme. We have listed these here.

#### 3.1 Reliability of the HAN solution

The wireless communication standard/solution for the HAN network is undefined and it is not clear from the Prospectus what will be defined in the Technical Specifications. There is an indication that no choice will be made on standards, but that requirements will be stated and Industry will then decide on the solution(s) in the short period between completion of the Technical Specifications (Autumn 2011) and start of roll-out (Summer 2012). This approach creates a significant risk that the HAN solution(s) adopted will not be reliable when deployed on a large scale.

There are a large number of factors which effect the HAN's reliability, these can not be assessed, and a reliable solution chosen, without significant large scale trials. Unpredictable factors include:

- Building structure and the immediate installation surroundings for the meters – proximity to other equipment and structures.
- Radio interference from other existing or future equipment in the home
- Radio interference and saturation with other smart metering equipment in high density housing
  - The risk of both these factors is greater if an unlicensed radio band is used.
- Data bandwidth and response times are reduced with high density traffic and/or interference
- Battery life for non mains powered equipment connected to the HAN could be substantially reduced by operating the HAN in a non-ideal RF environment

The Programme should include a large scale trial activity to prove the chosen HAN solution before the mass roll-out commences.

#### 3.2 Achieving sufficient energy reduction to justify the national investment

The ability of Smart Meters to enable most consumers to save sufficient energy and hence justify the national investment is not proven. There are a range of technical and behavioural approaches being developed by many diverse organisations and the final solution will come from these and future developments. Parts of the overall solution are coming from large internet companies like Google, small start-ups with new

## **Memorandum**

technology, more traditional appliance and home equipment suppliers and the energy companies themselves.

The Prospectus neither identifies the uncertainty in how the energy savings will be achieved and nor the need to make the Smart Metering system accessible and flexible to allow these solutions to develop in time. More specifically there should be:

- Technical requirements and associated solutions to make the full capability and information available in the Smart Metering system accessible to all the innovation, product development and delivery community so they can contribute and their solutions can be tested in the market. Of course information availability from the Smart Metering System would be subject to the necessary privacy and security requirements.
- An extended programme of trials should be undertaken to test approaches on all sectors of the community, assess and analyse results and provide guidance and recommendation on solutions that are effective. Providing that the metering system is accessible then the private sector will contribute significantly but the regulated nature of energy supply and need to involve all consumers will require some centrally and public controlled activity.

### **3.3 Inadequate Definition and Testing of the Smart Metering System Security**

Weaknesses in security have been a significant reason to stall Smart Meter roll-out and in some cases require their recall and replacement. This has been a particular problem in the US where Smart Meter roll-out is more advanced.

Weaknesses in Security are always a significant risk in any major system deployment but there are a number of factors in the Smart Metering Programme which increase the risk.

- The distributed ownership (technical and commercial) of different parts of the system. The Smart Meter equipment (which itself may have multiple owners), the central communications and the energy companies backend billing and customer services systems are all separate but must work together as a single secure system.
- The staged roll-out and in particular the DCC following the Smart Meter roll-out. How can the meters be secure if the system they will be communicating with is not fully defined?
- The lack of detail in the overall specification of the system and the associated independent review. There is a reluctance from the Programme to specify technical detail, and in particular aspects of the design, because this may imbalance commercial positions, but robust security requires the consideration, in depth analysis and design ownership of the whole system throughout its lifetime.
- The accelerated timescales reduce time for design, review and testing.

## Memorandum

### 3.4 Full Interoperability of Equipment and Systems is not achieved

If full and seamless interoperability between in-home equipment, communications and back-end systems is not achieved then:

- The full potential for energy saving will not be realised because solutions can not be deployed in all homes.
- Investment in innovation will be limited. The bigger the market for a single specification and associated products the larger the investment will be.
- Consumers will have restricted choice because the products and services they receive are not fully transferable when they move home or energy supplier.

The Prospectus does not identify or define a mechanism to ensure interoperability. Also the definition of what is meant or required for interoperability is very limited. Mechanisms to ensure interoperability include:

- The extensive and detailed definition at all levels of the interfaces between equipment and systems which have different ownership and suppliers.
- Establishing and running of a comprehensive programme of interoperability testing and certification.

### 3.5 The Organisation and contribution to the Programme not optimal

The Programme is very complex and ambitious and it is not clear from the Prospectus that the organisation and corresponding contribution is sufficient to ensure its success. Specific areas of concern and associated risk are:

- The lack of overall Technical Authority and Ownership of cross cutting areas like Security and Interoperability. This must be throughout the system's life.
- Visible mechanisms for Industry and other experts to contribute. The Prospectus and associated briefing discusses the need and desire for this contribution but is not clear how it can be made. Experts groups for the Smart Meters and DCC will be set-up but the chairmen of these groups say they are already established and full !!
  - Regardless of the value of any contribution that is being lost there is a risk of alienating a significant part of the Industry which is required to invest in the roll-out.
- The co-ordination, scheduling and split of responsibilities is not clear going forward. How will the Programme be managed from a traditional Project Management perspective – Who does What When and How do you ensure the required progress is being made?

## Memorandum

### 3.6 Consumer Acceptance – Risk of Rejection

The Programme includes activities to ensure consumers' rights are not broken and that consumers are not exploited. It also considers how Smart Metering and its benefits should be promoted to consumer but it does not address the explicit risk of rejection, either at an individual consumer level, or at a larger level in terms of "Public Outcry" and the press. There are a number of reason customers could reject Smart Meters. These include:

- There will be an additional cost to consumers to cover the new equipment. Regulation will prevent charging upfront costs but consumers know they will ultimately pay. (This is being funded by Energy Suppliers whose revenue is from the consumer.)
- Their bill will go up. Accurate billing is a major benefit but if there is a perception of higher bills (maybe caused but a catch-up from estimated readings) then a negative view will follow. This has been a problem in the US where consumers attributed higher bills to Smart Meters.
- They can have their supply switched off outside of their control. All meters will have pre-payment capability (switches and valves) enabling remote disconnect even if a customer is not on a pre-payment scheme.
- A raft of other reasons: social stigma, health risk from radio links, "Big Brother" is watching you - could all turn consumers against Smart Metering.

## Memorandum

### **4 Response to Specific Questions Raised in the Prospectus**

Each sub-section corresponds to each of the Prospectus documents and in each sections the question from the document are repeated with our responses below. Not all questions are answered. There are two response deadlines 28 September 2010 and 28 October 2010. Each section or individual question has an indication of the deadline. The document has been updated after 28 September 2010 with additional responses for the 28 October 2010 deadline.

## Memorandum

### 4.1 Prospectus – 28 September and 28 October

All questions require responses by the 28 October deadline unless stated otherwise.

#### 4.1.1 CHAPTER 2, The Consumer Experience, Questions 1-5

**Question 1:** (28 Oct) Do you have any comments on the proposed minimum functional requirements and arrangements for provision of the in-home display device?

##### Response

We agree that the consumers may want to add other devices purchased from the consumer market to the system (paragraph 2.13) and also that they would like to access their historic consumption data (paragraph 2.15). This will lead to increased engagement with the system and deliver further benefits in terms of energy saving, customer engagement and economic stimulation via a free market to supply products and services. If this extended use of the system can only be via the energy suppliers this will limit its uptake and not provide consumers with a transparent and independent way to invest in energy saving.

This open access should be fully defined as part of the GB technical specification and included in the regulatory requirements for Smart metering from the start of roll-out.

What information consumers require and how it is presented and accessed will change as the use of smart meters develops. Also it will vary between consumers. The IHD will be a programmable device running firmware and it would provide flexibility and added value if this could have a firmware upgrade capability (in a similar way to the meters). This would allow the IHD to be

**Question 2:** (28 Oct) Do you have any comments on our overall approach to data privacy?

##### Response

**Question 3:** (28 Sep) Do you have any comments on the proposed approach to ensuring customers have a positive experience of the smart meter rollout (including the required code of practice on installation and preventing unwelcome sales activity and upfront charging)?

##### Response

In general consumers feel more positive if they have a choice. In the initial stages of roll-out customers should be able to request a Smart meter. Then based on their positive experience others will request/accept the change.

We don't think that customers will like it if they all have the same type of in-house display. Customers like to differentiate themselves. If they all have the same device it

## Memorandum

will feel too utilitarian, or even communist. Customers will prefer to receive their new smart metering and smart energy information on their television, computer or mobile phone. These devices have much higher quality user interfaces and allow the customers to differentiate themselves from each other. The BBC Canvas project may provide an interesting method for displaying energy information on small windows on the television screen. Many homes have a TV in the kitchen. The concern is that TVs and computers consume too much power in themselves.

We are concerned that many customers will not like changing to a meter that can be switched off remotely. Most customers are good payers. They will not like the 'big brother' feeling that their energy supplier will have the ability to disconnect them with their new meter. As a result they may be obstructive at installation time and prefer to stick with their old dumb meter.

The customers will not feel that the new meters do very much for them. They should enable them to control costs better, which will be popular if energy prices rise. They will also enable them to feel a bit 'greener'. They may not believe that the new meters will really enable them to reduce costs by much. So the perceived advantages to the customer are very small when compared to the switch to digital TV (where the customer could access many more channels).

**Question 4:** (28 Oct) Have we identified the full range of consumer protection issues related to remote disconnection and switching to prepayment?

### Response

The inclusion of a switch or valve in every meter increases the potential for unintended disconnect. Human error, software bugs, faults in equipment or malicious attack are all more able to result in a disconnection. It is important that measures are introduced that recognise this can occur and there is a clear and fair resolution for the consumer. Disconnecting the energy supply can result in financial loss and/or health implications for the consumer.

**Question 5:** (28 Oct) Do you have any comments on the proposed approach to smaller non-domestic consumers (in particular on exceptions and access to data)?

### Response

## 4.1.2 CHAPTER 3, Industry Roles & Responsibilities, Questions 6-16

**Question 6:** (28 Sep) Do you have any comments on the functional requirements for the smart metering system we have set out in the Functional Requirements Catalogue?

The 'Functional Requirements Catalogue' is Appendix 2 in 94b/10 "Statement of Design Requirements".



## **Memorandum**

### **Response**

Cambridge Consultants has developed an interface called UMI (Universal Metering Interface). This defines interfaces for :

- Modules. 50x40x20 mm PCB with a 10-pin connector. Interface based on SPI.
- Opto interface based on EN62056-21 (FLAG port).
- Security interfaces. Scheme 1 is symmetric (not preferred). Scheme 2 is asymmetric (preferred but requires a Certificate Authority in the smart metering system).

The specifications and licence to use UMI are free. See :

- [www.CambridgeConsultants.com/umi](http://www.CambridgeConsultants.com/umi)

UMI has been optimised for ultra-low power consumption, as required for a battery-powered gas meter operating outdoors over a wide temperature range (where there will be condensation, which can easily flatten a battery).

UMI is already being used in various smart metering products, including the new smart gas meters from Elster.

UMI addresses many of the items listed in the 'Functional Requirements Catalogue', including :

- IM.2, IM.3, IM.5, IM.8, IM.9, OP.2, OP.7, SP.1, SP.2, SP.8, HA.12

Our responses to specific items are as follows. We have not commented on items that we fully agree with.

### **IM.2**

Do we want to enable remote software upgrade of functions inside the metrological seal ? Maybe IM.2 should distinguish between remote software upgrade of functions inside and outside the metrological seal. We believe that the MID does not allow remote software upgrade of functions inside the metrological seal yet. We hope that in future they will allow this, but it will require a very robust security system where the software upgrade must be accompanied by a signature and/or certificate from a trusted party (Certificate Authority) before the meter will allow the upgrade to happen.

This is one of the reasons why some meters are designed in a modular manner, with one module inside the metrological seal (that does not support remote software upgrades) and another module outside the metrological seal (that does support remote software upgrades).

### **IM.3**

We agree that it should be possible to change the WAN technology in situ. It might also be desirable to offer similar functionality for the HAN ? What is the expected life of the HAN ? Ideally changes to the HAN technology should be backward-compatible. If the HAN operates for 3 meter installations, that is equivalent to backward-compatible performance for 45 years !

## Memorandum

Unlike the WAN, the HAN will not need changing due to the DCC or changes in external technology; however there are a number of other reasons why it may need to change and a lifetime requirement and/or modular requirement should be stated.

- The components and technology become obsolete and it is no longer economic to build the meters. Wireless standards are constantly evolving and the markets they are used in can move to new technology.
- The unlicensed frequency band becomes too congested and the HAN stops working reliably due to interference. This is particularly vulnerable when using an unlicensed RF band (such as the 868MHz and 2.4GHz being considered for HAN solutions). Specifying a licensed RF band would avoid this risk.
- Different meters in the metering system will need replacing at different times. Without modularity all meters would need to be upgraded at the same time. The different timing of replacement is almost inevitable of other meters (e.g. water) or appliances are added to the HAN in the years following its first installation. If modularity for the HAN is not specified then an alternative approach to changing the HAN will be required.

## IM.5

It would be sensible to adopt the IEEE EUI-64 numbering scheme to electronically identify the components. The IEEE manage a scheme so that all devices in the world can have a unique 64-bit identification number. This consists of a 24-bit OUI-24 number that is allocated to a manufacturer. The manufacturer can then allocate their own unique 40-bit numbers to each device they produce. See :

- <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>

## IM.7

Having replaceable batteries in a product is a useful feature, but can make the product less reliable. Battery connectors are not as reliable as a battery that is soldered onto the PCB. Some gas meters prefer to have soldered batteries. When the battery runs out the whole meter is replaced in the field. The battery can be replaced back at the factory if the rest of the meter is still functioning correctly. The drive for in-field replaceable batteries seems to be coming from the energy suppliers.

## IM.8

The interface for local maintenance access should also be specified to ensure interoperability/commonality of maintainer equipment.

The inclusion of a specific maintainer interface e.g. a FLAG opto port (EN62056-21) should also be considered to allow access to the system when the HAN is not working.

## **Memorandum**

Replaced of batteries or communications modules in the field should be protected by a mechanical seal (not the metrological seal).

### **IM.10**

This might conflict with personal privacy.

### **IM.11**

After the devices have been installed in the home, they will have to be commissioned to connect them to the WAN and to the correct HAN, with the correct security features. It is important that the HAN devices connect to others in the same home, and not to any on neighbouring houses. This may require some manual entry or 'push-to-pair' functionality to support this. It may also be necessary to manually enter some security codes.

### **IM.12**

Energy suppliers have requested that electronic gas meters should close the valve just before the battery runs out. This could compromise public safety if it leaves the occupier cold on a winter's day.

### **OP.2**

Yes. We definitely agree and are very glad that you have made this point on UTC !

### **OP.3**

Last gasp functionality encompasses the meter, HAN, and WAN connection to the DCC. There should be sufficient level of specification before roll-out starts to ensure that meters installed before the DCC is in place will meet the last gasp requirement when the DCC WAN is up and running.

The hold up time for the last gasp will depend on how quickly the WAN connection can be made and the last gasp message is sent.

### **OP.4**

It is good to set a power limit for smart metering equipment, but 2.6W is actually quite high. With 26M homes, this means adding 68MW to the grid. Mains-powered devices (electricity meter, gateway) tend to be designed with less attention to power reduction than battery-powered devices (gas meters). Modern gas meters have an average power consumption of about 50uW, with HAN communications every 30 minutes.

### **OP.5**

## **Memorandum**

This time accuracy implies that the local real time clock in the meter should be re-synchronised about once per week. Clearly this must only be permitted by an external device that can present good security credentials (e.g signature or certificate from a trusted partner). If the UTC clock could be updated by the wrong parties it could be used as a means for fraud.

### **OP.7**

What is the requirement relating to Metrology software/firmware?

- Can this be upgraded with remote downloads?
- Must it be protected against any form of remote download?
- How should it be certified that the metering system upgrade does not affect the metrology?

Meters need to have enough memory to support a 'ping-pong' method for storing programs. If the meter is currently running from program A, then the download should go to program B. If the download is successful, the meter can switch to program B, if not it should continue to use program A.

### **DS.\***

We assume that this refers to the display on the meter (which is metrological) and not to the In-Home-Display (which is not metrological).

### **DS.2**

The requirement for log data seems to have recently increased from 3 months to 12 months. We believe this is because the Ofgem team have noticed the low cost of USB memory sticks and have assumed that similar amounts of memory could easily be added to a meter. We think this is a misunderstanding.

Low cost USB memory sticks are based on consumer NAND flash. Such consumer memories have quite short life cycles (12-18 months) are not appropriate for meters which need to keep the same Bill Of Materials for several years. In addition, NAND flash is not available as embedded memory in microprocessors. Microprocessors use NOR flash (needed for fast branch response during program execution). Typical sizes are up to 256 kB. To add really large memory sizes (MB to GB), NAND flash is needed and this has to be added as a separate chip, in addition to the microprocessor. This adds cost and power consumption to the meter.

In Holland the push has been in the opposite direction. Because of concerns over personal data privacy, they have been anxious to reduce the length of the log stored in the meter. We have heard of storage times as low as 1 week being suggested !

### **DS.5**

## **Memorandum**

Will the meter log and readings (sent back to the Gateway then DCC HEC) be in UTC? Should time-of-use price tariffs be in UTC ? Might it cause confusion if the time displayed on the meter is Local time ? In winter Local time and UTC will be the same. In summer they will be different. The MID requires that “there should be sufficient information under the glass of the physical meter for the customer to be able to resolve bill disputes”. This requirement becomes more complicated when time-of-use pricing is used. When we have time of use pricing, will the customer’s printed bills use UTC or Local time ? How will they deal with the hours lost and gained when we switch between UTC and BST ? Might there be a danger that the Local time on the meter display might actually confuse things ? The meter would certainly be simpler if it always displayed UTC (and indicated that it was UTC).

### **DS.6**

What security level will be required to erase the meter log ?

### **DS.8**

Are you suggesting that the meters installed in Wales should support English and Welsh ? If so, should they be different meters from those installed in England and Scotland, or should they all support Welsh ? How much extra cost is acceptable for a meter that supports Welsh+English over a meter that supports English only ?

Welsh has certain special characters (CH, DD, FF, NG, LL, PH, RH, TH). Is it acceptable to display each of these as two separate latin characters ? See :

- [http://en.wikipedia.org/wiki/Welsh\\_orthography](http://en.wikipedia.org/wiki/Welsh_orthography)

### **DS.9**

It is fine for the meter to clearly distinguish the separate registers. But with a small number of buttons (say 3) it might take a while to navigate the menus to access them.

### **IN.1**

Does the smart metering system need to support a switch from one WAN comms supplier to another. E.g when a regional franchise changes from one comms supplier to another ?

### **IN.2**

What should happen to the meter log and tariffs when a customer switches from one energy supplier to another ? Tariff 5 from EDF might have a different meaning to Tariff 5 from nPower. When the customer reviews a log at the meter, it might be misleading or even incorrect during the transition period from one energy supplier to another. If the log is 12 months, there is a long overlap period of such potentially false data.

## **Memorandum**

### **IN.3**

By what method or interface will consumers receive this data?

Will it be mandatory for this data to be made available?

Will the minimum content of the data be specified?

We recommend that Unicode character sets are used for all transfer of text. See :

- <http://en.wikipedia.org/wiki/Unicode>
- <http://www.unicode.org>

### **PC.1**

The industry's expectation is that a pre-payment download is for an amount of money, not for an amount of energy (kWh). If prices go up after the prepayment download, the customer will end up receiving less energy (and vice-versa). This could upset people if there are big energy price increases. Buying prepay energy is not the same as buying petrol for your car. This might upset some customers (and we are expecting more customers to use prepay in future).

### **PC.3**

How will the emergency credit function be defined so that it cannot be used as a fraud loophole ? How should the security system be used to enforce this ?

### **PC.7**

A gas meter can store data used for billing purposes for 3 months, but it cannot store the actual money values unless it knows the calorific value of the gas it has been measuring. Meter measure the volume of gas (in litres) and then adjust this volume to compensate for temperature and sometimes for pressure. However, the customer is charged for the number of kWh energy they use. The meter cannot know what the kWh value is until it knows the calorific value of the gas (which changes from region to region and from one time to another). Obviously the meter also needs to know the price to be used for each time period before it can calculate and display a money value.

### **PC.8**

It is OK for a meter to support block tariffs or time-of-use tariffs. It is difficult to define what is meant by a tariff that attempts to combine block and time-of-use behaviour. It would certainly be very confusing to the customer. So if we are going to support time-of-use tariffs, can we continue to use block tariffs as well, or would this confuse the customer too much ?

### **PC.10**

## **Memorandum**

What physical methods have been considered for this e.g. keypad entry on the meter or on the In-Home-Display ?

Would some credit enablement device connect to the HAN?

Would this functionality be in the gateway/WAN connection or IHD so it can be shared by both gas and electricity meters?

Without a WAN connection and without using physical tokens (PC.2) another means of the consumer connecting/interfaces to the meter will be required.

## **PC.11**

This will be determined by the latency of the HEC (that processes the remote top-up) + the WAN + the HAN.

## **ES.1**

Consider a smart metering system where the WAN goes into a Gateway that is separate from the Electricity meter. The Gateway and E-meter are both mains powered.

If the Electricity meter is operating in prepayment mode, then it will turn off the domestic electricity supply when it runs out of money. It is important that this does not turn off the Gateway, or there will be a bootstrap problem. The WAN must still operate so that a remote top-up can be downloaded to the Gateway and onto the Electricity meter, even when the domestic supply is turned off. This means that the Gateway should be powered by the un-switched supply and not by the switched supply. A good way to do this is to have a current-limited (to limit possible fraud) Auxiliary supply cable from the Electricity meter to the Gateway. This implies that the Gateway should be installed close to the electricity meter, probably on the same panel board (though this could be a problem if WAN RF reception is bad at that location).

## **ES.13**

Where will the physical switches be which respond to these commands be located?

Will they be in the meter, in dedicated switch module, in “Smart Appliances”?

If they are not in the meter how will the command be communicated to the physical switch and will this interface be defined (standardised)?

## **GS.4**

The gas meter has accuracy profiles for different flow rates. Bellows meters sense gas volume and generate pulses. Ultrasonic meters sense velocity and integrate that up to create volume. In both cases, sampling every 5 seconds is not enough to meet the MID's accuracy requirements. The accuracy needs to be specified in terms of

## **Memorandum**

volumetric error percentage at different flow rates. Simply specifying the sample rate is not enough on its own.

Gas meters cannot be expected to store log data at 5 second intervals. 30 minutes is the shortest time interval that is reasonable for the gas meter log.

### **GS.5**

The gas meter valve is still going to be a controversial issue.

Many good, paying customers will not want to move to a meter that can be remotely disconnected by the energy supplier. They will regard this as a retrograde step (compared to their existing dumb gas meter).

The valve also means that a security attack could have more serious consequences. If a terrorist organisation managed to break the security system, they could turn off the electricity and gas meters at every domestic home in Britain. If the gas meter did not have a valve, such a security breach could not have such a serious effect on UK security and on UK citizens.

### **GS.7**

Energy suppliers are saying that the valve must close just before the battery runs out. If the battery is also used for the metrology, then we don't think they will ever want the situation where the valve can stay open when the battery runs out (because then un-metered gas can flow through the meter).

### **DI.6**

Gas meters will typically use Lithium Thionyl Chloride batteries. Their voltage does not droop much during life, so it is very difficult to tell how many Ah are left in a battery from a direct reading of voltage (even if different load conditions are used).

So it is difficult to indicate how much lifetime is left in a battery. Measuring charge consumed as functions are executed is generally the best that can be done.

### **SP.1**

Access control will need to allow different users to have access to different data and functions in the metering system. Technicians, Energy providers, Manufacturers etc - not everyone who has access will have access to everything. Read and Write access levels need to be set at the level of data objects, so that different Roles can have different read and write access permissions to different data objects on the same smart metering device. It is not sufficient to control access levels only at the level of the device.

The Detailed Design Phase should consider the various users or roles in the system and provide a suitable definition for the subsequent implementation to work with.

As well as providing effective security this will be necessary for interoperability.



## Memorandum

Authentication, signatures, key exchange and certificates should be controlled with asymmetric cryptography (such as ECC or RSA). Each device should have a public and private key pair. The private key should never leave its device (preferably it should be stored in a hardware security module, such as the smartcard silicon used in bank and SIM cards). The public key can be sent over any communication link and does not need to be protected. i.e the security should be based on PKI (Public Key Infrastructure). Once a session key has been set up between two devices (by key exchange), it can be used to encrypt data between them with symmetric cryptography (such as AES-128).

It is too dangerous to build a system with symmetric cryptography (which requires all the keys to be protected as shared secrets). It will only be a matter of time before some of the shared secrets are found out. It is also too dangerous to build a system that requires the communication links to be secure. There will always be some security leaks somewhere in some of the comms links.

It is safer to build a PKI system, because that does not require the comms links to be secure. PKI systems require Certificate Authorities (CA) to be created. There may be separate CAs for the DCC, each energy supplier, each comms supplier, each equipment manufacturer and others. The CAs must be strongly protected, but this is easier to do as each CA can be concentrated in one secure computer installation. The CAs should issue certificates for major operations such as; meter installation and commissioning; remote software upgrade.

Having built such a PKI system, end-to-end security should be used wherever possible (e.g between the energy suppliers HEC (Head End Computer) and the meter). This can be used for robust transfers between the two (e.g meter reading upload, credit download, tariff download, software upgrade ...) without needing to trust any intermediate devices (e.g Gateway). If such intermediate devices need to be trusted they become an attractive security attack point. That's why it is safer in general if the Gateway is simply a router that passes messages on.

To use end-to-end signatures (e.g for a meter reading), the two ends (e.g meter and HEC) need to use the same data object formats as each other. If they don't there will need to be a translation point somewhere in between and that would break the signature, and so you wouldn't have an end-to-end link anymore. This is one of the reasons why it is so important to agree on application layer data objects, so that the same format can be used at both ends (e.g the HEC and the meter). Example data object formats are ZigBee Smart Energy and DLMS. They are both growing and neither of them support all the data objects that we need for UK smart metering yet.

It is important to define who is responsible for what. For example should remote software upgrade be the responsibility of the energy supplier or of the equipment manufacturer ? We think that this example should be the responsibility of the equipment manufacturer (just as Microsoft wants to take responsibility for remote software upgrades of Windows installed on PCs already in the field). But for every security example, it is important to define which organisation should be responsible for its correct operation.

## **Memorandum**

### **SP.2**

The cryptography algorithms and associated protocols will need to be defined in the next phase of the programme. Asymmetric cryptography should be used to cover the high integrity requirements. If only Symmetric cryptography is available then the risk of compromise of the shared keys is too high.

The following approach is proposed

Security is based on an asymmetric key system, where every device has its own private & public key pair.

- A PKI (public key infrastructure) should be set-up.
- The DCC should have a CA (Certificate Authority).
- ECC 256-primes should be considered for the asymmetric cryptography. This has already been adopted for other public security requirements e.g. the biometrics in European passports.
- The asymmetric cryptography should be used for all Authentication, key-exchange and Signatures.
- AES-128 should be considered for the symmetric encryption (based on a session key set up by the ECC 256-primes).

This proposal provides the more secure asymmetric encryption. There is no risk of permanent compromise if shared keys are intercepted. The DCC is the logical choice to be the Trust centre for the system and issue certificates to authorised parties that enable them to change meter access.

Symmetric encryption is available to provide a low power solution for gas meters

The use of renewed session keys mitigates any long term security risk of key compromise.

### **SP.5 and SP.6**

The storage and management of security keys and certificates is one of the most significant potential risks to the whole national smart metering system. The next phase must develop the security solution and define who is (or are) the root certificate authorities and which devices and users in the system they certify.

Multiple root certificate authorities may be required. The candidate root certificate authorities are:

- The DCC, or a specified entity within the DCC, which can operate with a high level of security integrity.
- The Utilities particularly if the DCC has the lower range of scope described in the Prospectus. If the DCC scope is extended then the Utilities will only interact with local processed data held by the DCC. Utilities will not interact with other parts of the Smart metering system. Utilities may also wish to use their certificate authority to nominate authorised meter operators, that in turn

## Memorandum

can issue certificates to individual technicians to allow traceability of meter interactions.

- Manufacturers, who may interact with the metering system for certain maintenance and upgrade activities - For example major software upgrade.

The certificate authority structure will also have to cover the certification of technicians who will access Smart metering equipment directly during installation and maintenance.

For security keys and with an asymmetric scheme secure storage of the private keys locally within each device is essential. However, this is the only place in the entire system where the private keys are stored or used. Everywhere else in the system only needs to use the public keys and these do not need to be kept secret. It doesn't matter if other organisations (even bad ones) know the public keys. With no need for shared secure keys in this scheme the management of keys is lower risk.

### SP.7

Specific guidance and recommendations will be required on the hardening solutions that will provide the required level of protection. These are likely to add some cost to the smart metering equipment and so will be excluded by manufacturers if at all possible.

As an example considerably enhanced security and physical security for key storage is provided by HSM (Hardware Security Modules) but they add cost to the meter. The programme should consider whether solutions like this should be mandated. HSMs (normally smartcard silicon) are used in mobile phones, credit cards, satnavs, set top boxes, and other mass market consumer devices which are subject to fraud.

Candidate requirements (for discussion) that would both mandate hardware security at the meter as in other industries, and also enable end to end security (digital signatures) would be :

- The meter metrological processor (not the wireless node) shall apply a Qualified Signature (1999/93/EC) to meter readings.
- Bodies authorised to issue Remote Disconnect commands to in home devices shall apply a Qualified Signature (1999/93/EC) to remote disconnect commands before they leave their secure premises.
- Bodies authorised to approve over the air firmware upgrades to in home devices shall apply a Qualified Signature (1999/93/EC) to firmware upgrade binaries before they leave their secure premises.

### SP.8

A smart meter may contain several processors. Each processor may contain several modules that can be remotely upgraded individually. So there can be several different software images sent to a meter for remote upgrade. The meter must be able to distinguish one such module from another. Each meter should be able to check via certificates from a trusted Certificate Authority (probably the CA of the equipment manufacturer) that each upgrade has a suitable digital signature. It must be able to

## Memorandum

recover and run from the old software if the new software upgrade went wrong in some way. So the software images should have a good signature to check that the meter has received it completely and correctly.

### SP.9

As highlighted in the Prospectus many standard interfaces wired and wireless are insecure and vulnerable to attack. It is anticipated that standard interfaces will be used in the smart meter and so the level of security provided by this interface may not be sufficient.

An end-to-end approach to security should be adopted. In this approach data is digitally signed at source and digitally verified at its final destination. If there are weakness in the communications and interfaces data may be lost or corrupted but security is not compromised. With the staged roll out and DCC following the smart meters this approach may not be universally possible in the initial deployments but should be addressed in the overall system and rolled out through the deployment. The firmware upgrade capability can be used to update the security in the earlier systems to the final solution.

### SP.12

The Smart metering HAN must be a very secure and high integrity network. This will be compromised if a wide range of devices can be connected from a wide range of sources. Also if connection is made by a customer rather than skilled technician the ability to secure and prove that the extended network is reduced.

However the majority of benefits in reducing energy usage will only be achieved if a range of smart appliances and energy control devices are introduced the home.

To solve this conflict of requirements the implementation of the HAN should use two separate networks with a secure gateway between them. One network connects the meters, WAN, IHD and secure gateway and the other connects the Smart appliances and other customer equipment. From the customer perspective there is only one network which meets the Prospectus requirements.

The meter network will be highly secure and reliable and will only have equipment supplied/approved/installed by the utility. All the essential smart metering functionality would be on this network.

The gateway between the two networks will provide secure access between them and prevent any device on the customer side of the network accessing wrong data or corrupting its operation. This gateway functionality can be included in the same place as the WAN/HAN connection. This solution is similar to the MUC proposed for Germany's Smart metering system (which uses Wireless M-Bus for the Metering HAN and KNX for the Appliance HAN).

## **Memorandum**

### **HA.2**

This requirement is very well supported by the two network implementation just described as only a small number of devices would need to be authorised and these could all be installed at once by an approved technician. The devices are E meter, G meter, Gateway to WAN and IHD.

### **HA.4**

The network coordinator for the Metering HAN should be located in the Gateway.

### **HA.5**

The next phase of the programme must define what the interoperability requirements are and how devices will be certified.

We think that the next phase of the programme should define the test and certification processes and bodies that will be used for UK smart metering devices.

### **HA.6**

It would be safer if the Metering HAN was based on a licensed RF band than an unlicensed band. We think the Metering HAN should operate in a backward-compatible manner for 3 meter installations (i.e 45 years), so future legal RF interference is a real concern. It is unfortunate that most of the RF standards being considered do operate in unlicensed bands (mainly 868MHz and 2.4GHz).

To mitigate this, thorough empirical and theoretical (including simulation) tests should be run on the chosen RF standard to understand how serious legal interference could be in a future worst-case scenario.

### **HA.9**

If the HAN does have repeaters or boosters, who owns them and who pays for their power supply ?

### **HA.12**

Software upgrades should use end-to-end security from the HEC (outside the HAN) to the meter (inside the HAN). So the HAN cannot provide the end-to-end security itself. Therefore the HAN must provide a tunnelling mechanism so that the HEC and meter can send packets to each other using end-to-end cryptography. These packets will be tunnelled through the HAN. Some HANs do not support this tunnelling feature, which is a fundamental problem for the security strategy.

## **Memorandum**

### **HA.13**

What form this gateway/bridging interface will take is unclear from the Prospectus. This should be addressed in the next stage of the programme.

Adopting a dual network implementation would provide this functionality so that the consumer can access data from the metering part of the network. The appliance part of the network could be based on a widely used consumer network such as WiFi and benefit from considerable existing infrastructure. This would accelerate the overall roll out and reduce its cost.

We like this bridging approach as it enables a separation of the Metering HAN and an Appliance HAN. The occupier will normally want to own the Appliance HAN themselves. The occupier will not be able to own the Metering HAN as that would give them the right to turn it off or break it. The energy suppliers need to maintain access to their meters via the Gateway and the Metering HAN, so they cannot allow the Metering HAN to be turned off by the occupier.

### **HA.14**

See HA.12. The meters sometimes need to tunnel through the HAN and through the Gateway, to achieve end-to-end security with the HEC. Such communications do not really use a defined application profile in the HAN.

Profiles are good for enabling inter-operability of equipment inside the HAN from different suppliers. But they are not good for everything, especially some of the security requirements that require end-to-end links between devices inside and outside the HAN.

Data object standardisation is very important (especially for the use of signatures), but it must be at a level that is used across the whole smart metering system. It is not useful when the data object standardisation is only valid within one part of the system (such as the HAN).

At present ZigBee Smart Energy profile only seems to be considered for use inside ZigBee (i.e inside the HAN). This is not very useful. To be really useful, ZigBee Smart Energy data objects should be used across the whole smart metering system (i.e in the meter, the HAN, the WAN and the HEC). The same applies to DLMS OBIS code data objects. They are both definitions for application-layer data objects and should be used across the whole smart metering system. They are not that helpful when constrained to just one part of the system.

### **HA.17**

Presumably this referring to Water meters? The difficulty is that the frequencies being considered (868 MHz, 2.4 GHz) for the smart metering HAN are probably too high to be useful to water meters that are installed beneath the soil.

## Memorandum

### HA.18

This feature will be very unpopular with some customers and will make them resist smart metering installation, as they will prefer to stick with their old dumb meters. This is a perfectly reasonable position for good energy payers to take !

This feature is also a good reason why the home appliances should be connected to an Appliance HAN (that they own) and not to the Metering HAN (which they do not own). The occupier should still be able to use his home automation facilities even when an authorised personnel member has chosen to turn off the Metering HAN. The occupier can do this if his home automation functions are supported on a separate Appliance HAN that the occupier owns (so it cannot be turned off externally).

### HA.12, HA.19, HA.20

These requirements all relate to future expansion and evolution of the system. The response to IM.3 has raised the issue of a limited lifetime of the metering HAN solution and the requirement for a transition to a new technology.

The two network implementation described for SP.12 above provides the additional benefit that the customer appliance equipment (which is likely to have a faster evolving network solution) is separated from the metering equipment, allowing them to evolve at a different rates. The Smart metering devices will not need to be upgraded or replaced because the network technology for the home equipment has changed.

### HA.20

We think that the HAN backward compatibility needs to be much longer than one meter life (15 years). If there are a number of devices connected to the HAN, they are unlikely to all be upgraded at the same time. In practise some devices will be changed before others. So if the HAN has been modified, the new devices will have to function correctly with the old devices (and vice-versa). This is backward-compatibility and we think it needs to be maintained over three meter lifetimes (i.e 45 years).

### HA.21

This depends upon how you define the 'smart metering system components'.

If you define them as the boxes that are not owned by the occupier (white boxes in the diagram in section 2), then we agree that they should all be on the same HAN (the Metering HAN). We expect this to include :

- Gateway
- Electricity meter
- Gas meter
- In Home Display

If you include boxes that are owned by the occupier (green boxes in the diagram in section 2), then we do not think that all the devices should be on the same HAN. We

## **Memorandum**

think that most users would prefer their smart appliances should be on a separate Appliance HAN that they own. The Appliance HAN could be the same or different technology from the Metering HAN. Example smart appliances include :

- Smart washing machine
- Smart freezer
- Smart boiler
- TV
- PC
- Mobile phone
- Solar PV microgeneration
- Electric vehicle charging.

As we explained in HA.13, the Metering HAN must be owned by an external organisation (e.g utility or comms supplier) and cannot be owned by the occupier.

Smart Metering will not be a success unless it achieves genuine reductions of energy consumption and greenhouse gas emissions. We believe that the roll-out of smart metering alone will not achieve this (electricity consumption has continued to increase in Italy after Enel rolled out 30M smart electricity meters, that only had WAN functionality for AMR). Reductions of energy and greenhouse gas emissions will happen if it is followed by the purchase of smart appliances that make use of the information from the new smart metering systems to make more intelligent energy decisions. So it is essential that the commercial and technical interfaces created by UK smart metering, encourage the development and purchase of new products and services for smart appliances.

We think that many customers will be keen to add smart appliances to their home (maybe when replacing old appliances that have worn out) if they connect to a network that they own themselves (maybe WiFi ?). Many do not like the ‘big brother’ feeling of attaching their home equipment to a network that is owned and controlled by an external company (utility, comms supplier or other), especially if that company has the right to turn the network off !

We think that if there is only one HAN, that it cannot be owned by the occupier, and that this will significantly reduce the take-up of smart appliances after the roll-out has been completed. This will reduce (and maybe even remove) any long term energy and greenhouse gas reductions. It will also be a missed-opportunity for stimulating economic growth in the UK.

The way to address these problems is to allow the occupier to have their own Appliance HAN to connect his equipment to. The Gateway should contain an end-point to this Appliance HAN. This will be the window through which the appliances can acquire information from the smart metering system.



## **Memorandum**

### **WA.1**

It's nice if the WAN is based on an open standard, but it is not essential. So long as there is competitive supply from more than one vendor, we should be able to get low prices for WAN products and services, even if they are not to an open standard.

Europe seems to have been far more obsessed with open standards than the USA has. Sometimes it seems that we prefer bad open technology to good proprietary technology. We need to keep this in balance. As long as there is a competitive market, you can get good prices.

### **WA.4**

When will we decide who should do the independent certification of the WAN ?

### **WA.5**

The security and privacy requirements should not depend on the security of the WAN itself. The security system should be designed so that the system is secure even if the WAN link is not. This will be achieved if important comms is done in an end-to-end manner with :

- Signatures to prove the source of the information and prove that it has not been tampered.
- Encryption to prevent eavesdropping. This is important for the privacy of personal data.

Both of the above can be supported if the WAN is able to tunnel packets through. This can be used as a mechanism for end-to-end communication between the energy supplier's HEC and the meter.

So the WAN does not necessarily have to support the security and privacy requirements itself, although it may well have its own encryption and authentication scheme for the purposes of deploying and maintaining the WAN communication link itself.

### **WA.6**

This is another reason why the home appliances should not be dependent upon a network they don't own. What is the occupier supposed to do if their appliance relies upon the presence of the WAN, if the WAN has been turned off (and the occupier has no mechanism to get the WAN turned back on again).

### **WA.7**

It is important that the end-to-end security requirements (between HEC and meter) are still met. Will this be possible if a Broadcast mode is used ?

## Memorandum

### IH.2

It is important that the occupier understands that if there is a discrepancy between the values (kWh, £ etc) shown on the IHD and on the Meter, then the values on the Meter are the ones to be believed. The Meter is MID approved. The IHD is not.

Gas meters should transmit new data values to the Gateway every 30 minutes, not every 15 minutes (i.e at the same time interval as is used for time-of-use pricing and for consumption logs). The IHD should have access to this data at any time, so the Gateway should store a 'mirror-site' database of the gas meter data.

**Question 7:** (28 Sep) Do you see any issues with the proposed approach to developing technical specifications for the smart metering system?

#### Response

To develop a new system of this size and complexity and prove the technical specification would normally involve a significant prototyping stage and incremental roll-out with iteration to the design based on trials. The timescales for deployment combined with the current state of the technical definition mean full pre-deployment trials are not possible. The programme should ensure prototyping is undertaken as soon as possible and this runs into the early stages of deployment. Programme planning should include the gathering of feedback from the early stages and subsequent changes to the technical specification for the system.

System design is a mixture of top-down requirements and bottom-up technology options. Normally this requires an iterative approach between these two directions to find the best solution to the overall problem. The specification approach being adopted for UK smart metering seems to be primarily concentrating on the top-down requirements. This is good, but in addition we need much more bottom-up testing (empirical and theoretical) of the possible technology options, to see how reliably they can work over many years, environmental conditions and use cases across the UK. ERDF in France feel that they need to test fully operational pilot schemes with 500k meters to learn enough about their system design to convince themselves that it will be able to work reliably. They say that this large trial has already taught them many issues that have been fed back in to change the system design to achieve better performance and reliability.

We are particularly concerned about the technology for the Metering HAN which we believe needs to operate in a backward-compatible manner for 45 years. We need to do much more testing of the RF systems under consideration to see if they can meet this need across the wide variety of installations that will be encountered in the UK.

It should also be made clear whether repeaters are acceptable to extend the range of a HAN or not? If they are acceptable, who should own them and pay for their power source ?

## **Memorandum**

**Question 8:** (28 Oct) Do you have any comments on the proposals that energy suppliers should be responsible for purchasing, installing and, where appropriate, maintaining all customer premises equipment?

### **Response**

Energy Suppliers should be responsible for the standard or mandatory equipment (meters, IHD and gateway/WAN module). The consumer should then be responsible and/or have the choice for any other devices.

**Question 9:** (28 Oct) Do you have any comments on the proposal that the scope of activities of the central data and communications function should be limited initially to those functions that are essential for the effective transfer of smart metering data, such as data access and scheduled data retrieval?

### **Response**

We would include some extra activities in ‘essential functions for the effective transfer...’ There are running certificate authorities, and a meter access control function (which can devolve meter access responsibility to other parties appropriately using certificates).

**Question 10:** (28 Oct) Do you have any comments on the proposal to establish DCC as a procurement and contract management entity that will procure communications and data services competitively?

### **Response**

**Question 11:** (28 Oct) Do you have any comments on the proposed approach for establishing DCC (through a licence awarded through a competitive licence application process with DCC then subject also to the new Smart Energy Code)?

### **Response**

The DCC will be subject to many risks. It is a new organisation; it will contract in many of its services; it has to interact commercially and technically with many different organisations; it has to develop new systems and take over legacy ones; and it will be responsible for many of the contracts, linking all the supply and administration organisations and consumers.

The scope, implementation plan and other arrangements for the DCC should identify and manage all the risks and mitigate them where possible with proven existing solutions.

**Question 12:** (28 Oct) Does the proposal that suppliers of smaller non-domestic customers should not be obliged to use DCC services but may elect to use them cause any substantive problems?

### **Response**

## Memorandum

**Question 13:** (28 Oct) Do you agree with the proposal for a Smart Energy Code to govern the operation of smart metering?

### Response

Prior to the DCC go-live date the smart metering system WAN and head-end services will be run by the energy suppliers. In the absence on the central DCC organisation how will the services be operated and regulated in this interim period prior to DCC go-live? Part of the rationale for having a single central DCC is that Ofgem will be able to regulate it (paragraph 2.23).

**Question 14:** (28 Oct) Have we identified all the wider impacts of smart metering on the energy sector?

### Response

**Question 15:** (28 Oct) Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?

### Response

Security must embrace and be developed and maintained for the whole system. Also it will require continued management and development throughout the systems life. The nature and sophistication of potential attacks will increase as will the corresponding protection. The system's security must be kept up-to-date and an organisation should be in place which can track potential and actual security breaches and fix them.

The Prospectus should recognise this need and state that a suitably qualified Security Authority with the appropriate mandate is set-up to take responsibility for the system's security through its entire lifetime.

Digital signatures on critical information (meter read, remote disconnect, firmware upgrade) should be mandated. Some companies do not intend to operate this way, and a large scale and public failure of their metering nodes/meters in the next 1-3 years might impact on the ability to deliver the rest of the programme.

The UK should consider whether it wishes to run a National certificate authority. If not, a dominant (monopoly) private provider will emerge, as certificate authorities are very difficult to compete against once hardware is rolled out into the field (because they have to be built into the meter as the root of trust). Novation may be required for certificate authority services.

**Question 16:** (28 Sep) Do you have any comments on the proposals for requiring suppliers to deliver the rollout of smart meters (including the use of targets and potential future obligations on local coordination)?

### Response

Relating to paragraph 3.52, the in-premise equipment should include an open standard interface (network connection) which provides all the necessary control and information to utilise the maximum capability of the smart metering system for

## Memorandum

energy saving. This will encourage and enable a wide range of suppliers to invest in and supply a wide range of energy saving products and services to consumers. This will be essential to achieve the required energy saving and use of renewables. If the system's functionality is closed then there will be a lost opportunity for innovation and investment and the natural competition between the energy providers will not maximise the intended national benefits of the system.

### **4.1.3 CHAPTER 4, Implementation and Next Steps, Questions 17-20**

**Question 17:** (28 Sep) Do you have any comments on our implementation strategy? In particular, do you have any comments on the staged approach, with rollout starting before DCC services are available?

#### **Response**

Starting meter roll-out before the DCC is in place places considerable risk that the initial roll-out equipment will not function as required when the DCC is in place. This is recognised in the prospectus. However the risk goes beyond incompatibility of early metering equipment, Major system wide requirements for security, interoperability, data privacy and other system wide capability could be irrevocably compromised.

A strong, well resourced and capable overall design authority for the overall system must be in place for now (ideally it already would be) right through to the completion of the full roll-out. In particular this authority must progress the technical specification and development of the DCC prior to its establishment and full deployment.

We would like to help with this overall design, but so far have been told by DECC and Ofgem that the detailed design groups are full (even though we requested this position 2 years ago).

There needs to be an overall design authority which is responsible for the correct design of the overall smart metering system for the UK. Who is this ? We don't think that Ofgem should both be the design authority and the regulator to check that the design has been done well. They should be two different organisations, otherwise there is a conflict of interest and responsibilities.

**Question 18:** (28 Sep) Do you have any other suggestions on how the rollout could be brought forward? If so, do you have any evidence on how such measures would impact on the time, cost and risk associated with the programme?

#### **Response**

The inclusion of a single common open modular solution in the metering system, particularly for the WAN modules, but also for the HAN, will reduce risk by providing flexibility and future proofing. Also it will save time and effort as hardware and software development can be reused and redeployed (there will only be one solution to develop).

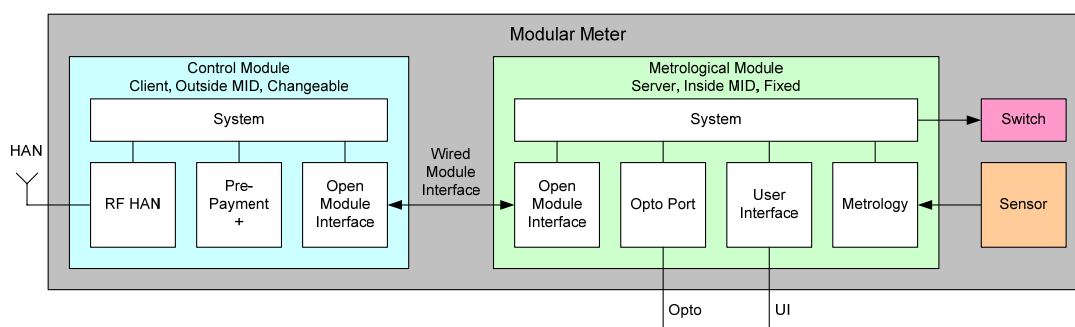
## Memorandum

A sensible separation of functions in smart meter is :

- **Metrological module.** Everything in this is inside the metrological seal and is MID-approved. The functionality does not change fast. Indeed it may even be possible to develop a module that does not need to support remote software upgrade. The module acts as a Server to an external Control module. The metrological module measures the flow of energy and creates the consumption log. It keeps performing this function all the time, whether a Client asks it for information or not. There shouldn't ever be a need to change the hardware in this module. If a hardware change really was needed it would require the whole meter to be changed. This is unlikely to happen because the functional requirements of this module are so stable and well understood.
- **Control module.** Everything in this is outside the metrological seal. It contains functions that can change fast (pre-payment, tariff schemes, HAN comms, security, ...). Consequently it must support remote software upgrade. It is a Client and reads and writes data from/to the Metrological module which is its Server. The function flow for a particular metering installation is controlled from the Control module. Requirements for this module will change. The changes could be quite fast and unpredictable. Hopefully most of these can be absorbed with remote software upgrades. But there may be an occasion when there is no alternative to a hardware change, but the pain of this will be reduced because it will be possible to change one Control module for another one. This could even include a change from one HAN RF standard to another. This does require a house visit. This would be unacceptably expensive if it was done one house at a time in an ad-hoc manner. But such a hardware problem will require a mass module change which can be done a street at a time. This will be much cheaper and quicker than replacing the whole meter.

Such a strategy for a modular meter requires the interface between these two modules to be fully defined. It is best if this is an open interface and not proprietary. UMI (Universal Metering Interface) is such an interface definition. The specifications and licence to use UMI are available free. This modular approach can be applied to meters, gateways, IHDs and Appliances. The philosophy works best for meters as there is a formal certification (MID) of part of the product.

Developing smart metering equipment in this modular manner will de-risk the project, as there are cheaper escape routes available in the future if problems are found after installation. Please see the earlier section on UMI in this document.



## Memorandum

This modular approach could also be used to install smart-ready meters now instead of dumb meters (we are already replacing over 1M G-meters and 1M E-meters per year). The smart-ready meters contain everything in the diagram above, apart from the Control module. This can be fitted in the field later when the requirements are known. It's useful to be aware of this approach as an option, but it is still quite difficult to coordinate. Most of the issues still to be decided in UK smart metering are in the Control Module only. But there are still a few that affect the Metrological Module (e.g security and software upgrade).

**Question 19:** (28 Sep) The proposed timeline set out for agreement of the technical specifications is very dependent on industry expertise. Do you think that the technical specifications can be agreed more quickly than the plan currently assumes and, if so, how?

### Response

The plan information in the Prospectus does not provide sufficient information to assess this. Cambridge Consultants would be pleased to help assess and achieve this by working for the Programme on an Expert Group or otherwise.

UK needs to set up a team to design the security strategy and system as soon as possible. This is likely to be the critical path. You cannot retrofit security after the meters have been installed. Certain fundamental design decisions must be taken before roll-out is started. The DCC, energy suppliers and other organisations should expect to set up their own certificate authorities to support the security scheme. They should start planning this now.

The roll-out time is likely to be limited by the number of installation engineers available. Any techniques that enable the home installation time (of all 4 boxes and commissioning) to be reduced will be very valuable. Tools should be created to enable this to be a very streamlined process.

**Question 20:** (28 Sep) Do you have any comments on our proposed governance and management principles or on how they can best be delivered in the context of this programme?

### Response

An overall Technical Authority should be established which is in place until roll out is completed and possibly for the lifetime of the system - See response to Question 17 above. This should not be Ofgem. Ofgem should continue to act as the referee, not as a player.

## Memorandum

### 4.2 94a/10, Consumer Protection - 28 October

All questions require responses by the 28 October.

#### 4.2.1 CHAPTER 2, *Developing services for consumers*, Questions 1-5

**Question 1:** (28 Oct) Do you have any views on our proposed approach for addressing potential tariff confusion? What specific steps can be taken to safeguard the consumer from tariff confusion while maintaining the benefit of tariff choices?

**Question 2:** (28 Oct) Do you agree with our proposed approach for addressing unwelcome sales activities during visits for meter installation?

**Question 3:** (28 Oct) What do you consider as acceptable and unacceptable uses of the installation visit and why?

**Question 4:** (28 Oct) Do you agree with our proposed approach to ensuring that the IHD is not used to transmit unwelcome marketing messages?

**Question 5:** (28 Oct) Do you agree that consumers should be able to obtain consumption information free of charge at a useful level of detail and format? How could this be achieved in practice?

#### 4.2.2 CHAPTER 3, *Prepayment and remote disconnection*, Questions 6-15

**Question 6:** (28 Oct) Do you consider that existing protections in the licence are sufficient to ensure that consumers are not remotely switched to prepayment mode inappropriately?

##### Response

The license should be arranged such that digital signatures have to be applied to 'switch' commands, to prevent inappropriate switching (not initiated by the supplier).

**Question 7:** (28 Oct) Could provision of an appropriate IHD help overcome meter accessibility issues to facilitate prepayment usage?

**Question 8:** (28 Oct) What notification should suppliers be required to provide before switching a customer to prepayment mode?



## Memorandum

**Question 9:** (28 Oct) Do you believe that suppliers should be required to provide emergency credit and „friendly credit“ periods to prepayment customers or whether, as now, this can be left to suppliers?

**Question 10:** (28 Oct) Do you consider that an obligation similar to Prepayment Meter Infrastructure Provision (PPMIP) may be required?

**Question 11:** (28 Oct) Is the obligation which Ofgem is proposing to introduce on suppliers to take all reasonable steps to check whether the customer is vulnerable ahead of disconnection sufficient? If not, what else is needed?

**Question 12:** (28 Oct) What notification should suppliers be required to provide before disconnecting a customer?

**Question 13:** (28 Oct) Do you have any views on the acceptability of new approaches to partial disconnection and how they might be used as an incentive to pay bills?

**Question 14:** (28 Oct) Do you agree with our approach for addressing issues related to remote disconnection and switching to prepayment?

### Response

Digital signatures should be applied to critical commands; a candidate requirement would be :

- Bodies authorised to issue Remote Disconnect commands to in home devices shall apply a Qualified Signature (1999/93/EC) to remote disconnect commands before they leave their secure premises.

**Question 15:** (28 Oct) Have we identified the full range of consumer protection issues associated with the capability to conduct remote disconnection or switching from credit to prepayment terms? If not, please identify any additional such issues?

### **4.2.3 CHAPTER 4, Vulnerable consumers and fuel poverty, Question 16**

**Question 16:** (28 Oct) What information, advice and support might be provided for vulnerable consumers (e.g. a dedicated help scheme)? Who should it be provided to?

### **4.2.4 CHAPTER: 5 Cost recovery and monitoring of costs, Question 17**

**Question 17:** (28 Oct) Do you have any comments on our proposals to prevent upfront charging for the basic model of smart meters and IHDs?

## Memorandum

### 4.3 94b/10, Statement of Design Requirements - 28 September

All questions require responses by the 28 September.

#### **4.3.1 CHAPTER 3, Overview of the Smart Metering System Functional Requirements Catalogue, Questions 1-6**

**Question 1:** (28 Sep) Should the HAN hardware be exchangeable without the need to exchange the meter?

##### **Response**

While there is no explicit or currently known requirement or reason for HAN modularity (The WAN modularity is required because of the later establishment of the DCC) there is considerable risk if it is not modular. See the response to IM.3 from the catalogue of functional requirements given above. Also see the response to question 18 in the Prospectus. In summary the HAN could require major upgrade/replacement (which would benefit from modularity) due to:

- Obsolescence of technology and/or key components
- Subsequent RF interference making the system unusable – this is a particular risk if it is in an unlicensed band
- Replacement of meters and addition of new meters (e.g. water) at different times resulting in the potential deployment of the system to 30 to 45 years (2 or 3 meter lives) . All equipment will not be due for replacement at the same time.
- Severe failings in Security or Data Privacy that can not be resolved with a firmware upgrade,

**Question 2:** (28 Sep) Are suitable HAN technologies available that meet the functional requirements?

##### **Response**

Yes, but it is a concern that all the HANs being considered operate in unlicensed RF bands (868MHz and 2.4GHz). Thorough analysis (empirical and theoretical) is needed to see what effect the worst case legal interference would have on the smart metering system. It would give us more peace of mind if there was a suitable HAN available that operated in a licensed band. This would give us a bit more confidence that the HAN would continue to function successfully for more years into the future.

**Question 3:** (28 Sep) How can the costs of switching between different mobile networks be minimised particularly in relation to the use of SIM cards and avoiding the need change out SIMs?

## **Memorandum**

### **Response**

Multi network SIMs are available. Technically this is possible. Any barriers will be due to commercial agreement.

**Question 4:** (28 Sep) Do you believe that the Catalogue is complete and at the required level of detail to develop the technical specification?

### **Response**

Our response feedback on the Catalogue is given above. The Catalogue is complete enough to progress to the Technical Specification but this activity and other parts of the overall Programme will raise issue that will require changes to the Catalogue. It must be a living document regularly updated and reviewed.

There is still a lot of work to be done to create a Technical Specification for UK Smart Metering that can be used by equipment manufacturers as input to their product development cycles.

**Question 5:** (28 Sep) Do you agree that the additional functionalities beyond the high-level list of functional requirements are justified on a cost benefit basis?

### **Response**

**Question 6:** (28 Sep) Is there additional or new evidence that should cause those functional requirements that have been included or omitted to be further considered?

### **Response**

Security is not raised as a top level Function (Tamper Proof is). Achieving robust security will add cost to the meter system and this should be made visible through the Functional definition and associated cost modelling. Improved security adds cost in terms of hardware (for example an HSM (Hardware Security Module) device/chip. It also adds more software and processing and more development and test time and system proving.

Recent experience and security weaknesses in some systems deployed in the US indicate this should be an item which is budgeted for in the meter specification.

## **4.3.2 CHAPTER 5, Achieving Technical Interoperability, Questions 7-10**

**Question 7:** (28 Sep) Do you agree that the proposed approach to developing technical specifications will deliver the necessary technical certainty and interoperability?

### **Response**

Interoperability can not be achieved by specification alone. Equipment and systems must be tested with each other and implemented reference standards to show

## Memorandum

compliance with the specification and interoperability. This approvals testing must be part of the overall Programme's technical governance and management.

Interoperability does require that the Technical specifications do identify physical interfaces that should be used for the Metering HAN and for the WAN. We will not be able to develop interoperable systems that can be sold installed anywhere across the UK, if Ofgem does not select a physical interface, preferring to leave it to the market to decide. This will lead to many different interfaces being used, resulting in lower interoperability and lower economies of scale. We can continue to change software (even for RF HAN stacks) after the devices have been installed in the field. But we do need to have compatible comms hardware in the devices before they are installed.

**Question 8:** (28 Sep) Do you agree it is necessary for the programme to facilitate and provide leadership through the specification development process? Is there a need for an obligation on suppliers to co-operate with this process?

### Response

Yes, a single overall control, ownership and responsibility is essential.

**Question 9:** (28 Sep) Are there any particular technical issues (e.g. associated with the HAN) that could add delay to the timescales?

### Response

There is a need for trialling the HAN technology (and associated networking software) in a representative configuration in a representative (worst case) deployment environment. Factors such as connection point density, data transfer loading or interference with other systems could all reduce or stop the operation of the metering system.

We need to run tests on :

- Old buildings with thick stone walls and external meters.
- Blocks of flats where the meters are remote from the flats (e.g in the basement).

**Question 10:** (28 Sep) Are there steps that could be taken which would enable the functional requirements and technical specifications to be agreed more quickly than the plan currently assumes?

### Response

Put together the right technical design team quickly. Make sure that there are some strong technical designers in the team. Don't let the design team get lost in 'design by committee' loops. Make sure that the design team has a good mix of people who understand :

- Top-down system requirements.
- Bottom-up technical constraints.

## Memorandum

### 4.4 94c/10, In-Home Display - 28 October

All questions require responses by the 28 October.

#### 4.4.1 CHAPTER 2, *Functional Requirements of the IHD, Questions 1-6*

**Question 1:** (28 Oct) We welcome views on the level of accuracy which can be achieved and which customers would expect, in particular in relation to consumption in pounds and pence.

##### Response

All the information necessary to calculate the accurate consumption in monetary terms can be made available in the meter and the result sent to and shown on the IHD. Where relevant information is available retrospectively e.g. the calorific value for gas or short notice pricing changes these can be sent down to the meter from the energy supplier. An alternative scheme would be for the accurate cost to be calculated in the head end and sent to the IHD as a message directly.

There will be some delay in calculating the accurate cost and probably some WAN data transfers to make with the head-end. Consequently it may be appropriate to only have an accurate reconciled cost updated on the IHD once a day.

**Question 2:** (28 Oct) We welcome evidence on whether information on carbon dioxide emissions is a useful indicator in encouraging behaviour change, and if so, how it might be best represented to consumers.

##### Response

Consumers have limited understanding of the kWh unit and even less so of what a kg of CO<sub>2</sub> means. A better approach may be to introduce “green” tariffs where there is a special rate or even control switch to mark the start and end of periods where low carbon electricity is available. These could then be shown on the display with graphics and consumers would be motivated by the amount of “green” energy they used compare to standard energy.

**Question 3:** (28 Oct) We welcome views on the issues with establishing the settings for ambient feedback.

##### Response

Paragraph 2.29 indicate 15 minute updates from the gas meter to the IHD. The generally accepted requirements is 30 minute updates. This is what is stated in the Catalogue of Requirements Requirement reference HA.11.

**Question 4:** (28 Oct) Do you think that there is a case for a supply licence obligation around the need for appropriately designed IHDs to be provided to customers with

## Memorandum

special requirements, and/or for best practice to be identified and shared once suppliers start to roll out IHDs?

### Response

This response relates to customers with special requirements but not necessarily the IHD. The smart metering system will have useful information for careers and those responsible for the less able. Subject to the necessary safeguards this could be made available to the responsible adult/career either via the internet or possibly mirroring the dependents IHD. (This would have data traffic requirements but the overall requirement would be small as the number of cases would be small).

As well as managing the financial aspects of a dependents energy supply this may enable others to advise on energy saving or simply provide reassurance that the dependent is doing OK by looking at their energy use profile.

**Question 5:** (28 Oct) We welcome evidence on whether portability of IHDs has a significant impact on consumer behavioural change.

### Response

**Question 6:** (28 Oct) Do you agree with the proposed minimum functional requirements for the IHD?

### Response

The IHD will include a processor and firmware as part of the HAN connection and the manage data on the display. The firmware in the IHD should be upgradeable over the air so that in the future when there is additional useful information to display this can be added. Also as new ways of displaying information are developed than the display can be upgraded.

There is evidence that consumer's loose interest in the IHD and energy saving after a short time. An upgrade to the IHD giving it a new look and feel may re-engage the consumer.

## **4.4.2 CHAPTER 3, Nature of the Mandate on Suppliers in relation to the IHD, Questions 7-8**

**Question 7:** (28 Oct) Do you have any views or evidence relating to whether innovation could be hampered by requiring all displays to be capable of displaying the minimum information set for both fuels?

### Response

This will not hamper innovation. The requirement to support both fuels can easily be included on an IHD from the most basic model to the most sophisticated.

**Question 8:** (28 Oct) Do you agree with the proposals covering the roles of and obligations on suppliers in relation to the IHD?

## Memorandum

### 4.5 94d/10, Communications Business Model - 28 October

All questions require responses by the 28 October.

#### 4.5.1 CHAPTER 2, *The Scope of DCC, Questions 1-4*

**Question 1:** (28 Oct) Do you agree that access control to secure centrally-coordinated communications, translation services and scheduled data retrieval are essential as part of the initial scope of DCC?

#### **Response**

##### Security

Yes we agree and reinforce the DCC's key role in the system's security. Secure transfer of data with the meter requires data objects to be signed at source and then only un-signed/extracted at their final destination. Resigning and re-encryption at some stage in the intervening communications is a security weakness.

The DCC can provide a suitable end point. Data will still be transferred on to suppliers and network companies but this is between a small number of end-points and can be done using existing secure IT solutions like SSL.

However, in many cases it will be cheaper to run a DCC that acts as a conduit and pass on secured data (data with digital signatures) to and from the supplier. In particular if the supplier is to be held responsible for issuing remote disconnect commands, the DCC may wish to pass a signed message from the supplier straight through, rather than take on combined responsibility for the command by resigning it before it goes to the meter. With a certificate authority infrastructure, the DCC is at liberty to devolve or resume responsibility for particular actions to key parties over time by issuing and revoking certificates.

Associated with the DCCs security responsibility its scope should include key storage and management and also a Certificate Authority.

##### Common Format (translation service)

The translation service in the DCC would convert the data into a common format. This common format must be carefully defined and a system put in place to maintain and develop it. The type of information that the DCC will handle will evolve in time and this development must not be constrained by a fixed data interface.

Many meters have proprietary data and some meter data may be specific to certain suppliers. A common format will need to address how proprietary of supplier/meter specific data types are handled. It would also include signature formats.

## **Memorandum**

**Question 2:** (28 Oct) Do you agree that meter registration should be included within DCC's scope and, if so, when?

### **Response**

Yes we agree. Meter registration data is used by a number of organisations and as the central system the DCC is the logical place for it. The DCC must be a robust and very secure system and hence will have the technical capability to hold the meter registration. Also it will improve security as less data will need to be transferred between systems.

It would be logical to include meter registration from the start so that all new meter installations are registered with the DCC. This should be subject to it being practically achievable and balanced against the downside of any potential delay to the DCC being in place.

The practical implementation of meter registration within the DCC may require a communications interface with the existing meter registration so the systems can run in parallel and data can be transferred and cross checked during a transitional period.

**Question 3:** (28 Oct) Should data processing, aggregation and storage be included in DCC's scope and, if so, when?

### **Response**

Logically if the same processing is performed on the data in different systems then it would be better performed in a single central system but this is an incremental improvement and must be traded off against the timescale to get the DCC up and running.

**Question 4:** (28 Oct) Do any measures need to be put in place to facilitate rollout in the period before DCC service availability and the transition to provision of services by DCC, for example requiring DCC to take on communications contracts meeting certain pre-defined criteria?

### **Response**

The WAN interface has been specified as a module to allow it to be replaced without replacing a meter. Paragraph 2.64 states that there should not be further visits to change the communications module on meters installed before the DCC is up and running.

The Prospectus should provide clarification on:

- When it is acceptable to change the communications module?
- When the specification for the WAN communications module will be available?
- What happens to smart meters installed before the WAN module is specified which are not compatible with the DCC WAN just by firmware upgrade?



## Memorandum

- Whether the meter or the WAN node will be authenticated by the head end(s) for the purposes of meter readings (end to end security would define this as the meter. This approach also helps with a secure gradual roll-out of WAN infrastructure after meters have been deployed)

### 4.5.2 CHAPTER 3, *The Structure and Realisation of DCC, Questions 5-8*

**Question 5:** (28 Oct) Do you agree that the licensable activity for DCC should cover procurement and management of contracts for the provision of central services for the communication and management of smart metering data?

#### Response

The DCC will be operating with a new licence; have to define and procure services to create and run a new system; have to transition existing systems into its scope including the early mover and pre DCC smart meters and manage the introduction of new technology while working with multiple new suppliers. The risks to the timely and successful establishment of the central communications and data management services are numerous and complex.

The choice of organisational and licensing structures and the details of how they will operate and be monitored should consider and mitigate these risks at every stage.

The success of the DCC will depend heavily on the co-operation and support of the existing organisations that will form part of the smart metering system and in particular the energy suppliers. The DCC and associated licences should include arrangements to encourage and incentives all relevant organisations that form part of the smart metering system to make the DCC's activity a success.

**Question 6:** (28 Oct) Do you consider that DCC should be an independent company from energy suppliers and/or other users of its services and, if so, how should this be defined?

#### Response

Independence is important because of the central and very influential position the DCC will have in the smart metering system.

However, mutual co-operation as stated in the response to the previous question is also essential.

**Question 7:** (28 Oct) Do you have any comments on the steps DCC would need to take to be in a position to provide its services and the likely timescales involved?

#### Response

**Question 8:** (28 Oct) Do you have any comments on the proposed approach to cost recovery and incentivisation for DCC?

## Memorandum

### Response

The central communications and data management functions will have substantial development and set-up costs whose uncertainty, timing and rate of spend is very different from the day to day running of the system when it is established.

Consideration should be given to this in any contracts and incentivisation agreements. Should the DCC and its service providers amortise the up front cost over the licence period or is it better audited, managed and incentivised if the set-up and operational costs are separated.?

## Memorandum

### 4.6 94e/10, Data Privacy and Security - 28 October

All questions require responses by the 28 October.

#### 4.6.1 CHAPTER 3, Data Privacy, Questions 1-4

**Question 1:** (28 Oct) Do you have any comments on our overall approach to data privacy?

##### Response

Many objectives of the data privacy charter would be enabled by securely identifying the parties involved (authentication) using digital signatures. The current proposals which involve translation at key areas prevent this happening.

It should be considered whether it is a key requirement for the meter (or the meter operator) to be able to uniquely identify individual companies and even individual technicians who take actions that affect the meter, as this drives the design requirements for the deployed meters.

Some example requirements for identifying personnel are in the NIST “Security Profile for Advanced Metering Infrastructure 2.0 June 22 2010” document (DHS 2.15.3 p72 and 2.15.4 p73). Note that these types of requirement may be deployed at less cost with a public key infrastructure (enabling end to end security) than the symmetric key approach favoured by the US until recently.

**Question 2:** (28 Oct) We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

##### Response

**Question 3:** (28 Oct) Do you support the proposal to develop a privacy charter?

##### Response

**Question 4:** (28 Oct) What issues should be covered in a privacy charter?

##### Response

#### 4.6.2 CHAPTER 4, Smart Metering System Security, Question 5

**Question 5:** (28 Oct) Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

## Memorandum

### Response

In addition to unauthorised access to personal data and unauthorized remote disconnection, access for fraud should be a key risk (paragraph 4.8).

In the measures to address risk (paragraph 4.10) the provision of secure Certificate Authorities should be included.

The Prospectus documents use the term 'end-to-end' system when discussing security but it is not clear what is meant by this. The smart metering system should have 'end-to-end security' where messages are signed (and can be encrypted) at one end (for example inside the meter) and verified and decrypted at the other end (for example at the energy suppliers head-end). In end-to-end security, messages are not re-signed at any point in their transfer as this would create a security weak point. End-to-end security can be difficult to achieve in a complex system which has multiple intermediate networks and communications and data standards.

A significant advantage of end-to-end security is that all intermediate communications and systems do not need to have as high a level of security with its associated cost.

We present more detailed information and possible solutions for the smart metering system security in the 28 September 2010 deadline response to the Statement of Design Requirements given earlier in this document (section 4.1.2, Question 6, SP.1-12).

## Memorandum

### 4.7 94f/10, Implementation Strategy - 28 September

All questions require responses by the 28 September.

#### 4.7.1 CHAPTER 2, Programme management and governance, Question 1

**Question 1:** (28 Sep) Do you have any comments on our proposed governance and management principles or on how they can best be delivered in the context of this programme?

##### Response

Correct governance of the technical aspects of the programme is essential and an overall responsible authority should be in place which oversees and directs the development and deployment phases of the Programme through all 4 phases. This is particularly necessary because of:

- The fast development and roll-out of the system. There is not time for the coordination and consultation to make decisions across different groups. The specific groups proposed must report into a central authority.
- The many stakeholders need coordination and their remits defining.
- The establishment of the DCC after meter deployment has started requires a complete consistent design to be in place from the start. This will be very difficult to achieve. The DCC is likely to push back on certain assumptions once it is formed.

#### 4.7.2 CHAPTER 3, Programme activities, Question 2

**Question 2:** (28 Sep) Are there other cross-cutting activities that the programme should undertake and, if so, why?

##### Response

Interoperability must be considered across the whole system not just within the home and HANs (Metering and Appliance). Interoperability must ensure

- Equipment from different sources must be fully compatible in the home.
- Consumers must be able to swap suppliers and still operate the Smart energy equipment they have purchased to work with the smart metering system.
- Homes which get their electricity from one supplier and their gas from another must operate just as well as homes which get both from the same supplier. The user should not experience any reduction of convenience or performance.
- Consumers must be able to use the smart energy equipment in their new home when they move house.

## Memorandum

The benefit of the smart metering system will only be realised when there are a range of Smart energy devices installed in the home. This will include Domestic Appliances, Home Energy Management Systems, Displays and interfaces to other user interaction equipment like TVs and PCs and in the future electric vehicles. There will also be fixed equipment such as room and water heating and local renewable energy (PV solar, thermal solar, wind and ground source)

Manufactures must have the assurance that there is a large market for their standard products and consumers must have the confidence to buy them. Much of this will be a long term investment. Lack of interoperability will block the market for Smart Energy equipment and the required benefits of Smart Metering will not be realised.

### **4.7.3 CHAPTER 5, *Proposals requiring changes to the regulatory framework, Questions 3-8***

**Question 3:** (28 Sep) Do you agree with our proposal for a staged approach to implementation, with the mandated rollout of smart meters starting before the mandated use of DCC for the domestic sector?

#### **Response**

We think it is very risky to start meter roll-out before the DCC is operating. The risk can be reduced a bit by installing modular meters. The functional requirements of the Metrological module will be known well before the requirements are known for the Control module. It will be possible to start developing the Metrological parts of meters before the DCC is in operation. There are still many decisions that need to be taken even for the Metrological modules in such smart meters.

**Question 4:** (28 Sep) Do you have any comments on the risks we have identified for staged implementation and our proposals on how these could best be managed?

#### **Response**

To mitigate the risk of equipment not being interoperable, an extensive programme of interoperability trials, compliance testing and approvals should be put in place. The existing practice in mobile communications and PC systems which ensures interoperability provides a good working example of how this can be done.

**Question 5:** (28 Sep) Do you have any other suggestions as to how the rollout could be brought forward, including the work to define technical specifications, which relies on industry input?

#### **Response**

The inclusion of a single common open modular solution in the metering system, particularly for the WAN modules, but also for the HAN, will reduce risk by providing flexibility and future proofing. Also it will save time and effort as hardware and software development can be reused and redeployed (there will only be one solution to develop).

## Memorandum

Further savings can be made by adopting an existing open standard which meets the systems requirements. UMI – Universal Metering Interface is proposed for this. See the section on UMI, earlier in this document)

**Question 6:** (28 Sep) Do you agree with our planning assumption that a period of six months will be needed between the date when supply licence obligations mandating rollout are implemented and the date when they take effect?

### Response

Detailed visibility with frequent updates to the Technical Specifications and other Regulatory requirements will be required so that suppliers can be prepared and undertake the major part of the equipment design and testing before these key documents are finalised. Six months is the order of time required to ramp up production.

**Question 7:** (28 Sep) Do you have any comments on the activities, assumptions, timings and dependencies presented in the high-level implementation plan?

### Response

**Question 8:** (28 Sep) Do you have any comments on the outputs identified for each of the phases of the programme?

### Response

## Memorandum

### 4.8 94g/10, Rollout Strategy - 28 September

All questions require responses by the 28 September.

#### 4.8.1 CHAPTER 2, *Approaches for Rollout, Questions 1-3*

**Question 1:** (28 Sep) Do you believe that the proposed approach provides the right balance between supplier certainty and flexibility to ensure the successful rollout of smart meters? If not, how should this balance be addressed?

##### Response

**Question 2:** (28 Sep) Would the same approach be appropriate for the non-domestic sector as for the domestic sector?

##### Response

**Question 3:** (28 Sep) Is there a case for special arrangements for smaller suppliers?

##### Response

#### 4.8.2 CHAPTER 3, *Mechanisms for General Consumer Engagement, Questions 4-5*

**Question 4:** (28 Sep) What is the best way to promote consumer engagement in smart metering? As part of broader efforts, do you believe that a national awareness campaign should be established for smart metering? If so, what do you believe should be its scope and what would be the best way to deliver it?

##### Response

A significant group of consumers, particularly earlier adopters will be motivated and engaged with the smart metering system if they can access the information in their own way, typically onto a PC. They also want to install their own energy saving equipment to work with the Smart metering system.

The Smart metering system should include a standard interface (physical and application) to enable this.

Looking to later adopters this will also increase uptake. Many customers are more likely to engage with a product or service if they have a choice in what they take, and have no contract or ongoing costs. This was demonstrated by pay-as-you go mobile services which made a large number of non-mobile users adopt the technology.



## Memorandum

**Question 5:** (28 Sep) How should a code of practice on providing customer information and support be developed and what mechanisms should be in place for updating it over time?

**Response**

### **4.8.3 CHAPTER 4, *Obligations on Suppliers to Complete the Rollout, Questions 6-9***

**Question 6:** (28 Sep) Do you agree with the proposed obligation on suppliers to take all reasonable steps to install smart meters for their customers? How should a completed installation be defined?

**Response**

**Question 7:** (28 Sep) Do you think that there is a need for interim targets and, if so, at what frequency should they be set?

**Response**

**Question 8:** (28 Sep) Do you have any views on the form these targets should take and whether they should apply to all suppliers?

**Response**

**Question 9:** (28 Sep) What rate of installation of smart meters is achievable and what implications would this have?

**Response**

### **4.8.4 CHAPTER 5, *Prioritisation of Specific Consumer Groups, Question 10***

**Question 10:** (28 Sep) Do you have any evidence to show that there are benefits or challenges in prioritising particular consumer groups or meter types?

**Response**

### **4.8.5 CHAPTER 6, *Reporting Arrangements, Question 11***

**Question 11:** (28 Sep) Do you agree with our proposed approach to requiring suppliers to report on progress with the smart meter rollout? What information should suppliers be obliged to report and how frequently?

## **Memorandum**

### **Response**

#### **4.8.6 CHAPTER 7, Consumer Issues, Questions 12-13**

**Question 12:** (28 Sep) Do you agree that there is already adequate protection in place dealing with onsite security or are there specific aspects that are not adequately addressed?

### **Response**

**Question 13:** (28 Sep) Do you agree with our proposal to require suppliers to develop a code of practice around the installation process? Are there any other aspects that should be included in this code of practice?

### **Response**

Yes, we agree.

**Subject:** Response to the Ofgem Smart Metering Implementation Programme  
Prospectus July 2010

## **4.9 94h/10, Regulatory and Commercial Framework - 28 October**

All questions require responses by the 28 October.

### **4.9.1 CHAPTER 2, Smart Metering Regulatory Regime, Question 1**

**Question 1:** (28 Oct) Have we identified all of the key elements that you would expect to see as part of the Smart Metering Regulatory Regime?

**Response**

### **4.9.2 CHAPTER 3, Smart Energy Code, Questions 2-4**

**Question 2:** (28 Oct) Do you agree with the proposal to establish a Smart Energy Code?

**Response**

**Question 3:** (28 Oct) Do you have any comments on the indicative table of contents for the Smart Energy Code as set out in Appendix 3?

**Response**

**Question 4:** (28 Oct) Do you have any comments on the most appropriate governance arrangements for the Smart Energy Code?

**Response**

### **4.9.3 CHAPTER 4, Roles and responsibilities at customer premises, Questions 5-7**

**Question 5:** (28 Oct) Do you agree with the proposals concerning the roles and obligations of suppliers in relation to the WAN communications module?

**Response**

Yes having one organisation that installs, maintains and operates the in-premises equipment is the overriding reason for the proposed responsibilities.

For the WAN, consideration should be given to the communications standards used and availability of technology, components and modules that would implement it. Solutions for widely adopted standard like GPRS can be obtained from multiple

**Subject:** Response to the Ofgem Smart Metering Implementation Programme Prospectus July 2010

sources at reasonable cost. More specialised or proprietary solutions may not have the low cost sourcing that comes from a large total market and multiple suppliers.

With the WAN specified by the DCC and its service companies and purchased by the energy suppliers, the solution specified may not be optimised for a low module cost.

**Question 6:** (28 Oct) We welcome views as to which other additional data items should be included in the mandated HAN data set beyond the list for the IHD.

### Response

Home energy management will develop over then next decade and beyond. The information made available from the HAN should be flexible and evolve.

Our suggestions are:

The data set made available is allowed to evolve and expand in a backward compatible manner. The mandated data set should be reviewed from time to time in consultation with stakeholders and extended where there is benefit in doing so. There will be other aspects of the smart metering system that will also need reviewing with a view to extending the specification. The system will have firmware upgrade capability to implement this.

Data items which should be made available include:

- Historic, Current and Future (if available) pricing (ToU) to a fine granularity. This will allow customers to assess how shifting/changing their existing usage could save them money. Also it will allow any “controllers” they have (manual or automatic) to optimise the running of their home energy consumption.

Note: There could be commercial sensitivity from the energy suppliers in making this pricing data available outside the protected meter system. The regulator should give guidance and/or set rules on making this information available.

- Any demand response, peak pricing events or other events which do not follow the regular ToU tariff cycle.

**Question 7:** (28 Oct) Do you agree with the proposal that the WAN and the HAN in customer premises should be shared infrastructure, with the installing supplier retaining responsibility for ongoing maintenance? If not, would you prefer to have an arrangement by which if the gas supplier is the first to install, responsibilities for the common equipment is transferred to the electricity supplier when the electricity smart meter is installed?

### Response

Should an option be considered where the all the in-premises equipment is installed, operated and maintained by one organisation which is independent from the energy suppliers and provides a service to them. This would avoid the disadvantages that the

**Subject:** Response to the Ofgem Smart Metering Implementation Programme  
Prospectus July 2010

three options proposed raise and make customer switching of suppliers simpler as there is no change in ownership of the meter(s) only change in access to the meters which will be handled by the DCC.

From a customer's perspective the energy supplier would still be responsible for the meter and be their point of contact. The energy supplier would instruct the meter company in response to customer requirements.

#### **4.9.4 CHAPTER 5, Other regulatory and commercial issues, Questions 8-11**

**Question 8:** (28 Oct) Are there additional measures that should be put in place to reduce the risks to the programme generated by early movers?

##### **Response**

Is there a requirement for smart meters rolled out before the technical specification is confirmed to subsequently comply with the technical specification? If this is not a requirement how can the interoperability of the early mover smart meters with the post technical specification meters be ensured? As well as interoperability in the HAN there may be other areas of non compliance in the early mover meters – for example information on the IHD.

Upgrading early mover meters to comply with the technical specifications may not be possible just with firmware updates and require a home visit to modify or replace the meter. Would this be acceptable to consumers?

**Question 9:** (28 Oct) What is needed to help ensure commercial interoperability?

##### **Response**

Adding to our response to Question 7 should an arrangement be considered where the meters are not owned and operated by the energy supplier? The DCC will be a part of the smart metering system and is not owned by the energy suppliers who will share in its use – could the same apply to the in-premises equipment?

If “commercial interoperability” is required as described in the prospectus then the need to first have technical interoperability is correctly identified (paragraph 5.12).

There are considerable technical risk in achieving technical interoperability which are reduced with extensive trials and compatibility testing. We have described this above in Section 3.4 under “Risks”.

**Question 10:** (28 Oct) Can current arrangements for delivering technical assurance be developed to gain cost effective technical assurance for the smart metering system? If so, how would these procedures be developed and governed?

##### **Response**

**Subject:** Response to the Ofgem Smart Metering Implementation Programme  
Prospectus July 2010

**Question 11:** (28 Oct) Are there any other regulatory and commercial issues that the programme should be addressing?

**Response**

#### **4.9.5 CHAPTER 6, *Impact on wider industry processes, Questions 12-15***

**Question 12:** (28 Oct) What evolution do you expect in the development of innovative time-of-use tariffs? Are there any barriers to their introduction that need to be addressed?

**Response**

**Question 13:** (28 Oct) Are there changes to settlement arrangements in the electricity or gas sectors that are needed to realise the benefits of smart metering?

**Response**

**Question 14:** (28 Oct) What arrangements would need to be put in place to ensure that customers located on independent networks have access to the same benefits of smart metering as all other customers?

**Response**

**Question 15:** (28 Oct) Are there any other industry processes that will be affected by smart metering and which the programme needs to take into account?

**Response**

**Subject:** Response to the Ofgem Smart Metering Implementation Programme  
Prospectus July 2010

#### **4.10 94i/10, Non-Domestic Sector 28 October**

All questions require responses by the 28 October.

##### **4.10.1 CHAPTER 3, *Flexibility for installations of advanced and smart meters, Questions 1-3***

**Question 1:** (28 Oct) Are there any technical circumstances where only advanced rather than smart metering would be technically feasible? How many smaller non-domestic customers have U16 or CT meters and what scope is there for full smart meter functionality to be added in these cases?

**Question 2:** (28 Oct) Do you agree with our proposed approach to exceptions in the smaller non-domestic sector?

**Question 3:** (28 Oct) Are there technical circumstances that we have not considered that would justify further flexibility around installation of either smart or advanced meters?

##### **4.10.2 CHAPTER 4, *Use of DCC to communicate with meters in the smaller non-domestic sector, Questions 4-8***

**Question 4:** (28 Oct) Do you agree with the proposed approach that use of DCC should be optional for non-domestic participants in the sector?

**Question 5:** (28 Oct) If use of DCC is not mandated for non-domestic customers, do you agree with the proposed approach as to how it offers its services and the controls around such offers?

**Question 6** (28 Oct) To what extent does our proposed approach to the use of DCC for non-domestic customers present any significant potential limitations for smart grids?

**Question 7:** (28 Oct) Is a specific licence condition required to ensure that metering data for non-domestic customers can be provided to network operators or DCC, and should any provision be made for charging network operators for the costs of delivering such data?

**Subject:** Response to the Ofgem Smart Metering Implementation Programme  
Prospectus July 2010

**Question 8:** (28 Oct) How can interoperability best be secured in the smaller non-domestic sector?

**4.10.3 CHAPTER 5, *Other issues related to non-domestic customers,*  
Questions 9-11**

**Question 9:** (28 Oct) What steps are needed to ensure that customers can access their data, and should the level of data provision and the means through which it is provided to individual customers or premises be a matter for contract between the customer and the supplier or should minimum requirements be put in place?

**Question 10:** (28 Oct) Do you agree with our approach to data privacy and security for non-domestic customers?

**Question 11:** (28 Oct) Is the proposed approach to rollout (for example in terms of targets and a requirement for an installation code of practice) appropriate for the non-domestic sector?