Cambridge Consultants

Memorandum

To DECC
cc
Prepared by REDACTED REDACTED REDACTED

Subject: CCL Response to DECC SMETS2 Consultation

1 Introduction

This is the Cambridge Consultants response to :

- DECC Smart Metering Implementation Programme:
- Consultation on the second version of the Smart Metering Equipment Technical Specifications) URN 12D/258.
- smartmetering@decc.gsi.gov.uk

In the past few years Cambridge Consultants has provided feedback to DECC on a number of smart metering consultation documents, including :

- eSmart-M-005 v1.0, 31 July 2009.
- eSmart-M-006 v1.2, 1 December 2009.
- eSmart-M-031 v0.1, 7 April 2011.

In addition, we have issued a number of papers to DECC with suggestions on how to make GB smart metering successful, recently including :

- eSmart-M-038 v0.3, 22 Feb 2012, Design Principles for GB Smart Metering Security.
- eSmart-M-039 v1.4, 23 April 2012, All GB Smart Metering Equipment should have a LocalPort.
- eSmart-SK-051 v1.0, 14 May 2012, Secure Data Packets over Data Pipes.

We are happy to supply these papers again if needed.

In this response to the SMETS2 consultation document, we have focused on a few key technical issues which we feel may influence the long-term success of GB Smart Metering.

2 Overall Comments

2.1 It's about Energy, not Equipment

The programme should be clear about the objectives of Smart Metering in energy terms. What is the change in GB annual domestic energy consumption (in Joules or kWh) that will be achieved as a result of the smart metering rollout ? We are not aware of this being clearly published anywhere. Without these objectives how will the programme assess whether it has been a success in the years that follow the smart metering rollout?

At present the business case has been stated in GBP. This is not enough on its own. To achieve public buy-in the programme needs to agree and publish the energy objectives of the smart metering rollout. Without this the public will think that it's all about equipment and not about energy. There is a danger that this may actually reflect the atmosphere in the smart metering programme itself.

2.2 Should SMETS2 be Technically Prescriptive ?

SMETS1 (April 2012) is a functional description for smart metering equipment. It enables competing manufactures to produce smart metering equipment that offers the same functions to the user. However it is not a technical specification. It does not contain the information required for competing manufacturers to release inter-operable equipment.

The general expectation within the smart metering community has been that SMETS2 will contain sufficient technical information for competing manufacturers to produce inter-operable equipment. However, there is also the view that there are still competing views inside DECC as to whether :

- DECC should be technically prescriptive and define the interfaces needed between smart metering devices.
- DECC should not be technically prescriptive. "It's not for Government to pick winners. We should let the market decide".

Actually either way can be made to work for GB, but the uncertainty as to which one is causing great damage and delay. If DECC publically steps away from the technical definitions, someone will have to fill the void. So long as DECC appears to be about to make technical decisions, then no one else will. This uncertainty is damaging. It will help GB greatly if DECC could soon make it clear as to which of these 2 paths it intends to pursue.

2.3 The Metering HAN should have a Reserved RF Band

DECC are selecting CSPs (Comms Service Providers) for the North, Central and South regions. The regions could be won by different companies using different WAN technologies.

The device manufacturers would like to sell the same types of gas meter, electricity meter and IHD, regardless of which CSP region they are installed in. This will be possible if the same HAN is used in all 3 CSP regions.

The product lifetimes for comms hubs, gas meters, electricity meters and in-home displays are unlikely to all be the same. This means that the generation 2 devices are unlikely to all be changed at the same time in a given home. This means that there will be a need for a new comms hub to work with an old gas meter, or a new electricity meter to work with an old comms hub. This means that any changes to the Metering HAN technology will need to be backward-compatible. It will be impossible to change to a brand new incompatible HAN technology, unless all 4 devices are changed at the same time. This is very unlikely to be acceptable logistically or financially. So once we've started with a given HAN technology, we will be forced to stay with it for several generations of meter (3 gas meter generations should last for 45 years). i.e it will be like the mains power socket or standard gauge railway. Once you've started with a particular standard, it becomes impossible to move away from it.

The Metering HAN technology needs to be one that will continue to operate with good performance for several decades (4 or 5). The ideal would be a HAN technology that operates well between all 4 devices in every GB home for at least 45 years.

It is highly unlikely that such performance will be achievable with a HAN technology based on an unlicensed RF band. Whether it's 2.4 GHz or 868MHz, the performance will degrade over the years as more and more interference sources compete (legally) for the same RF bandwidth. It will be very costly (and embarrassing) if in years to come the smart metering communications systems stop working and start to cause customer complaints.

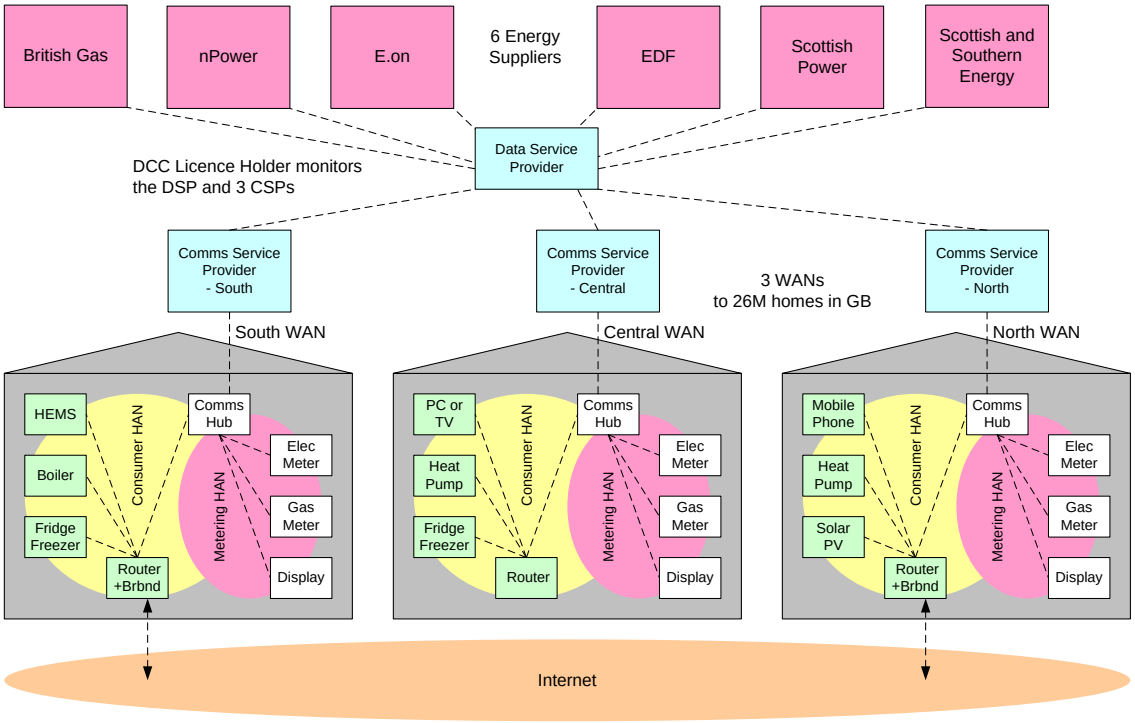
A possible solution is for the Metering HAN to be based on a reserved RF band. DECC should identify an RF band that will operate between the 4 smart metering devices in most GB homes and then apply to Ofcom to reserve this band to be used only for Smart Metering. Ofcom's main concern about reserved bands is that they end up not being used. This will not be the case for the GB smart metering HAN, so Ofcom should have no objection.

Over the past few years the smart metering community has drifted into a view that 2.4GHz ZigBee could be used as the Metering HAN in all GB homes. The radio trials this year (which could and should have been run much earlier) have indicated that 2.4GHz ZigBee will only operate well enough between all 4 devices in 70% of GB homes. As a result, people are now considering 868MHz ZigBee or other technologies. But as another unlicensed band this is still likely to suffer from performance degradation over the years.

We should learn from our mistakes and now select the RF HAN properly. We must agree on the operational life required of the Metering HAN. In our opinion this should be 3 meter lives (45 years). We believe a reserved RF band will be needed to achieve this lifetime.

2.4 Consumer Appliances should have Direct access to Smart Metering information

We feel that the long-term energy-reductions enabled by smart metering will be greater from smart appliances (automatic decisions) than from in-home-displays (manual decisions). So it is important that the smart-metering architecture stimulates the maximum uptake of smart appliances after the rollout.



Smart Appliances will make more intelligent energy decisions by using the information available from smart metering via a consumer interface. We think that the uptake of smart appliances will be much higher if there is not a ‘standards war’ over this consumer interface :

- Consumers are more likely to buy smart appliances if they all use the same consumer interface. Most consumers will not buy equipment if there is a standards war and they cannot yet tell which standard is the winner.
- Manufacturers will not want to release smart equipment if they are not sure which consumer interface standard will win. This all kills the market.

The current DECC plan is that the CAP (Consumer Access Portal) is only a logical port to the metering HAN. It is likely to be implemented as various different bridge devices. Sadly this is likely to lead to the very standards war that we are trying to avoid.

It would be better if the CAP could be a real physical port with a published interface. This would make it easy for the appliance manufacturers to develop smart appliances

that complied. They could even carry a 'GB-Smart-Ready' sticker if they complied with the published CAP interface.

Maybe the CAP could actually be based on a network that 70% of GB homes already have – WiFi. This could be implemented as an endpoint in the Comms Hub. This could act as a firewall so that the consumer devices do not need to be security approved. In addition to enabling various smart appliances, WiFi would also add a real WOW factor for the users when their smart metering equipment is first installed, as the information would be immediately available on their computers, smart phones and smart TVs.

2.5 We need an agreed Application Packet Format for End2End Security

The smart metering system consists of many nodes (meters, comms hubs, displays, computers, head ends, etc) sending messages to each other. The security of these messages can be achieved with :

- Endpoint security. Application layer packets are signed and encrypted by the source node, then tunnelled through various channels to be checked by the destination node.
- Channel security. Nodes cannot use a channel until they are authenticated. Thereafter the channel operation can be encrypted.

We believe the smart metering programme should concentrate on endpoint security. For a national communications network it will be impossible to ensure that all the channels are secure. It is safer to secure the packets at application layer, so that the system does not rely on the channels to be secure. This is the method used for most internet security.

This means that all the nodes need to agree on a single set of security rules for application packets. These Secure Data Packets can then be generated by any source node and checked by any destination node.

If all the nodes were IPv6 then we could adopt a defined subset of IPsec (IP security) as the security format to be used for the application packets sent between all nodes. However this is not the case in the current GB smart metering design (IPv6 may be used from the DCC to the Comms Hubs, but not over the Metering HAN to the meters and IHD).

So we need to adopt a format for a secure data packet that can tunnel through IP and non-IP parts of the network. Cambridge Consultants has a design for such an application-layer Secure Data Packet. We are happy to share this with DECC if it is of interest.

3 Comments on Specific SMETS2 Questions

3.1 Consultation Question 2

A system containing two application layers (SEP and DLMS) will be complex and will have security issues. Example: how does the IHD interact with the e-meter? Does the CH translate between DLMS and SEP? This may result in effectively two security domains - one associated with SEP and one associated with DLMS - with translations required (re-encryption, re-signing) for messages traversing the two domains.

Is the HHT required to act as a ZigBee device and a DLMS client? Or does the CH provide a translation so that the HHT only implements one protocol?

3.2 Consultation Question 3

A detailed companion specification will be necessary. Thought should also be given to the method of assessing compliance with the companion specification - eg, third-party type approval, golden units, publication of standard test sequences for self-assessment.

3.3 Consultation Question 5

What traffic model was used when estimating the volume of data (in for example kByte per day) on the HAN?

Devices operating in licence-frees bands will remain at risk from interference from other devices in the same band. This risk is perpetual and is outside the control of DECC or the DCC. There is the possibility that what works on the day of installation may not work at a later time. This is the nature of RF communication.

3.4 Consultation Question 11

A wired HAN is a shared media system, just a ISM-band wireless HANs are. The same issues over interference might apply. As with the wireless equivalent, adopting a wired HAN in a reserved band (CENELEC A) will help.

3.5 Consultation Question 13

It's not clear whether, in an intimate e-meter, the CH and e-meter are separable (by installer or service man). If they are inseparable, then an e-meter exchange would also result in a CH exchange. If it's easy for a CH to find its set of HAN devices and rejoin the WAN then this is probably OK. But if the process of a CH rejoining its networks is slow and/or unreliable, then it may best to avoid the 'intimate' option.

Also, is it the installer who inserts the correct (PLC v 868 MHz v 2.4 GHz) HAN module into the intimate CH/e-meter, or are the CH/e-meters delivered with their HAN module pre-installed?

3.6 Consultation Question 14

Paragraph 78 states in relation to the supplier-led model, "It places responsibility for delivering an effective HAN with one party". This is only the case in dual-fuel households. In non-dual-fuel households, which supplier has the responsibility for the HAN?