gridmerge

Technical Document

Response to SMETS 2 consulation

Project	DECC SMIP SMETS 2 Consulation
Author	
Document Ref.	DSMP/TD000001/V1.0/rcc
Date	03/10/2012
Status	Release
Distribution	

Revision History

Version	Date	Description
1	08/10/12	First release

Contents
Table of Contents

1 Introduction

This document is the response by Gridmerge Ltd. to the consultation on the second version of the Smart Metering Equipment Technical Specification (SMETS2) published by DECC on 13th August 2012 to the questions requiring response by October 8th 2012.

Gridmerge Ltd. provides this response as an individual.

1.1 About Gridmerge Ltd.

Gridmerge Ltd. is a Smart Grid Communications and Security company. Gridmerge Ltd. was formed in August 2009 and starting trading in November 2009 offering consultancy services. Gridmerge Ltd. has two main contracts with the following clients:

- Pacific Gas and Electric Company
- Grid2Home Inc.

Gridmerge has also done some additional consulting for other clients in the area of home area networking security including development of an ECC cryptography library for a ZigBee SE 1.0 implementation.

1.1.1 Contact details

Gridmerge Ltd.

http://www.gridmerge.com

1.2 About

1.3 Involvement in USA Smart Grid activities

Pacific Gas and Electric are one of the most progressive utilities in the USA with regard to Smart Grid and Smart Metering. They have already installed 9 million Smart Meters in a programme of installing 10 million Smart Meters and are in the process of rolling out HAN devices for the consumer. They have employed experts and consultants (including Gridmerge Ltd.) in the wide ranging area of Smart Grid development in the state of California, and Gridmerge Ltd. has been specifically involved in standards development on behalf of PG&E and security testing of HAN devices for PG&E's test laboratories.

In the USA in general, the Smart Grid efforts are being led by the NIST (National Institute of Standards and Technology) SGIP (Smart Grid Interoperability Panel). This group was founded under mandate from the US Federal Government in 2009 with the specific aim to identify standards which can be used throughout the Smart Grid and also to develop guidelines for Smart Grid cyber security.

Gridmerge Ltd. has been involved heavily in the US standards groups with regard to development mainly in the HAN and cyber security areas. The standards organisations Gridmerge Ltd has or had direct involvement and has contributed significantly to are:

Group	Role
ZigBee Security Task Group	Chair
ZigBee IP Stack Task Group	Co-Editor-In-Chief
ZigBee PRO Specification	Security Editor
ZigBee Smart Energy Profile 1.0	Security Editor
ZigBee Smart Energy Profile 2.0	Security Editor
IEEE 802.15 TG4b task group	MAC/security technical editor
IETF lwig working group	Co-chair
IETF 6lowpan working group	Contributor
IETF core working group	Contributor
IETF homenet working group	Contributor
IETF roll working group	Contributor
UCAIUG OpenSG OpenHAN	Contributor
NIST SGIP Cyber Security Working Group (CSWG)	Contributor
SAE J2836 J2847 J2931 J2952 Work Group	Contributor

Group	Role
ISO/IEC 15118 Electric Vehicle Communication Standard	Contributor

1.4 Gridmerge Ltd. and the UK programme

Due to heavy and focussed involvement in the US, Gridmerge Ltd. has not had any specific involvement in the UK programme up to now. However, Gridmerge Ltd. is in a unique position to apply experience and knowledge gained in the US Smart Grid and Smart Meter industry to the developing programme in the UK being lead by DECC, especially in the Home Area Networking and cyber security areas, and would thus be able to provide key input to the SMIP and the STEG.

1.5 Gridmerge Ltd.'s consultation questions response

Gridmerge Ltd. is providing detailed response with respect to its main area of expertise, i.e.:

- Network Communication Protocols
- Application Protocols
- Cyber Security

The responses are heavily focused on the consultation questions which are most technically focused as this is where Gridmerge Ltd.'s expertise primarily exists.

1.5.1 No particular comment

Consultation questions soliciting response to which Gridmerge Ltd. has no particular comment are:

27, 28, 40 – 44, 48 – 50.

2 Gridmerge Ltd.'s position with regard to the responses

2.1 Use of IP-based solutions

Gridmerge Ltd. believes that, given the revised timescales, the Government should seriously consider looking at IP-based HAN solutions. This would give the following main benefits over non-IP based solutions:

- More straightforward to deploy a HAN with network segments using different physical layers (including 868 MHz and wired) whereby the segments are interconnected using simple routing
- Does not require tunnelling for transport of DLMS data to the electricity meter, which is already specified to be carried over IP-based networks
- Facilitates end-to-end provision of confidentiality and integrity of data in transit
- Allows seamless integration into home owners' existing networks

The solutions being developed in the ZigBee Alliance to provide:

- IP-based networking over 802.15.4
- Smart Energy application layer using XML and HTTP (SEP 2)

are well-advanced and fit into the revised timescales. Moreover, SEP 2 is also being developed in conjunction with the Wi-Fi and HomePlug Alliances as part of the CSEP (Consortium for SEP 2 interoperability) with the aim to work end-to-end across IEEE 802.15.4, 802.11 and P.1901 physical layers (as specified by the ZigBee Alliance, the Wi-Fi Alliance and the HomePlug Alliance respectively).

If the Government is committed to ZigBee SEP v1 and DLMS, then Gridmerge Ltd. recommends that the SMETS ensures that the products have the potential to be upgraded to support SPE 2 and IP-based network in the future, and that alongside, the recommendations from the PAP 18 work group in the SGIP be taken into consideration to develop and specify an application layer gateway to facilitate incorporation into home owners' existing networks.

2.2 Better use of mesh networking

Gridmerge Ltd. believes that better use of mesh networking technology through ZigBee PRO/SEP v1 or ZigBee IP/SEP v2 would mitigate some of the problems with regard to propagation in certain properties and solutions based on low cost additional routers should also be considered as a more currently available solution than specifying products based on 868 MHz radios.

3 HAN analysis

On general reading of the document, it is not entirely clear that all the issues surrounding the HAN are fully understood. Prior to specifically answering the questions posed in the consultation, some of the considerations around the HAN will be analysed and explained in this section.

3.1 Multiple HAN communication media

The consultation document clearly shows that there is no one single suitable solution with regards to the HAN communication medium for properties in the UK. Identified choices are:

- Wireless 802.15.4 at 2.4 GHz
- Wireless 802.15.4 at 868 MHz
- Wired

Of these three, the two wireless choices are governed by the choice of ZigBee SEP v1, which currently uses 802.15.4 at 2.4 GHz and could be adapted to 802.15.4 at 868 MHz in a relatively straightforward manner, although this would take time. The wired solution is not really expanded much and it is not clear whether this implies powerline based communication or, for example, twisted pair such as 1000Base-T.

The analysis also acknowledges the OSI layered model and identifies the split between essentially application layer functionality and the protocol stack and physical device below which carries networked data across a medium.

For this reason, flexible options clearly need to be considered for HAN deployments, which should allow seamless integration of network segments running on different physical layers into a HAN. Furthermore, easy integration into a home owner's existing local area network also needs to be considered.

3.2 Mesh networking

The consultation document states that wireless HAN trials have taken place and identified the 868 MHz band provide the best characteristics for a wireless HAN based on propagation and interference. It is accepted that propagation is better at 868 MHz, however there are limitations at this frequency, not least the duty cycle of 1%.

There also seems to be an assumption that the link will be point-to-point and one hop. One of the significant properties of the ZigBee PRO and ZigBee IP network layers are their ability to perform adaptive route discovery to provide mesh networking. This ensures that intermediate nodes can be used to relay information between neighbouring nodes taking advantage of coverage overlap between nodes to provide a continuous path through the nodes. Performance of 2.4 GHz networks alone can be significantly improved through the addition of one or more router nodes. These router nodes may be very low cost, simple devices which do not require any application layer functionality beyond simple configuration. Alternatively, additional nodes which perform an application layer function can act as routers and provide the necessary coverage to reach devices on the extremities of a network.

The addition of just one node can effectively double the range of communication between two devices and/or increase the reliability in a marginal network. The addition of more nodes further improves the redundancy of paths through the network and, as 802.15.4 was designed to be a low power, low cost implementation, this type of network can be readily set up in a premises for a relatively low cost.

3.3 Typical HAN topology

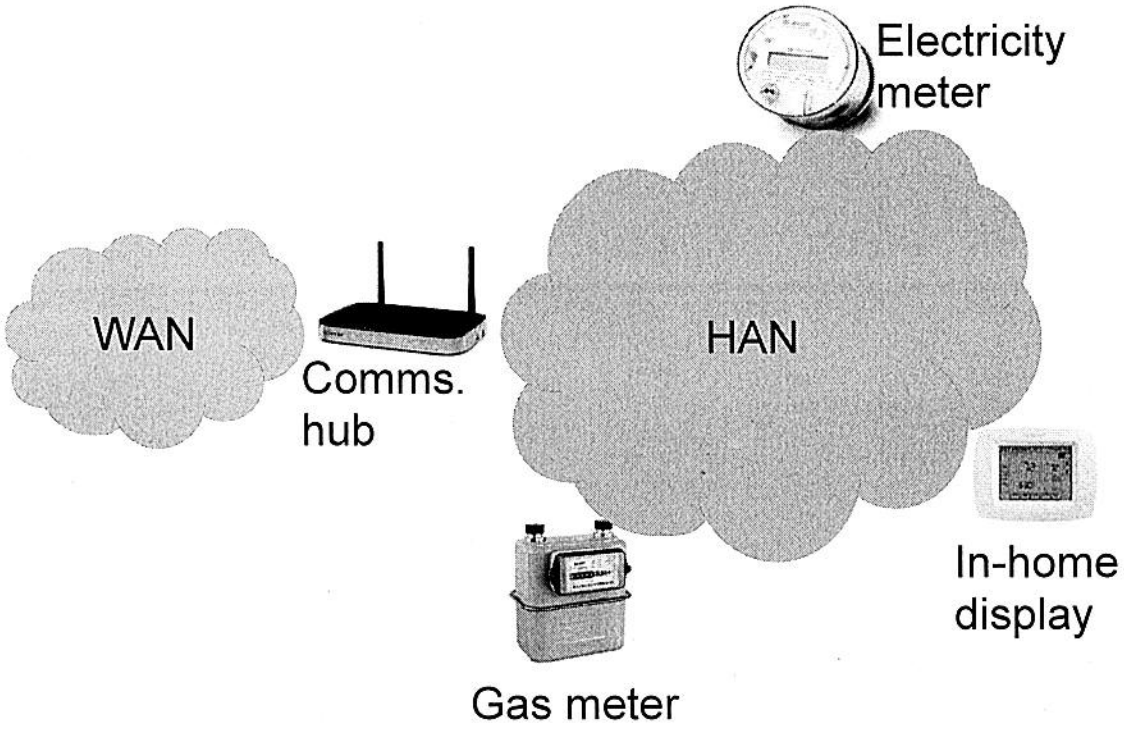


Figure 1: Typical HAN topology

A typical topology of a simple system containing all the components identified as Smart Metering Equipment, is shown in Figure 1, with the emphasis put on the HAN and the HAN devices.

3.3.1 Topology variations

The HAN is shown as a single wireless network and this is generally the proposed model for the HAN in the consultation document. However, a HAN may also be considered one or more network segments joined together to link all the Smart Metering Equipment and also the Consumer Access Devices. These network segments may use different physical layers and media, e.g.:

- Wireless PAN (802.15.4/ZigBee)
- Wireless LAN (802.11/Wi-Fi)
- Powerline
- Twisted pair

The more seamlessly these network segments can integrate, the more scalable the solution will be and the easier it will be to deploy "fit-for-purpose" installations for particular properties.

The picture for e.g. blocks of flats is much more complicated, where the meters may all be co-located in a basement room and each premises will require its own access to each meter. This will inevitably require different network segments and indeed multiple HANs securely communicating through a shared network medium (e.g. twisted pair Ethernet).

3.3.2 Bridging in existing home networks

Consider a typical home environment today, where there is a single wireless (Wi-Fi) home router. In many cases, especially in buildings with thick stone walls, the wireless range from the router is inadequate to reach all devices. Solutions have been developed to overcome this issue, which include:

- Wireless repeaters (e.g. Wi-Fi WDS)
- Plugs using HomePlug powerline communications
- Twisted pair cable to extend networks where convenient to install

These solutions are manually installed and configured and all tend to bridge (at the MAC layer) the individual network segments together to form one home local area network. From a network topology point of view, all devices effectively appear as if they are on "one piece of wire".

3.3.3 Routing between network segments and within mesh networks

Whilst convenient for all network interfaces which use Ethernet-style communications, the bridging solution does have its own issues. It is generally impractical in wireless mesh networks as nodes tend to be more mobile and thus the network may be constantly reconfiguring itself automatically. Also, not all network segments use a common Ethernet-style MAC addressing, therefore it is not always possible to bridge networks directly.

The solution is to route the network segments at the network layer using intermediate routers. This is easily achieved using the Internet Protocol (IP) version 4 (IPv4) or version 6 (IPv6) as routing protocols exist to facilitate connecting routers together, irrespective of the underlying physical medium and medium access layer. Work is being undertaken currently in the IETF in the homenet working group to identify mechanisms to simplify this for home users as it is certain that as home owners become more technology-aware, there will be an increased use of networking in the home and home owners' networks will inevitably consist of multiple network segments.

Routing allows application layer data to be carried end-to-end throughout the network segments interconnected through routers. For example, home networks predominantly use IPv4 networking, which allows home owners access to the Internet through their home router and thus end-to-end connection from e.g. a web browser in someone's home to a web server in e.g. Australia.

This also allows end-to-end securing of the data, which means that the data from the web server in Australia can travel through any number of unsecured network segments and remain confidential and integrity-protected all the way to the web browser in the home. This is the mechanism used for online banking and other secure sites (HTTP over TLS). It is also the mechanism used by mobile phone carriers (e.g. Vodafone) when providing femtocell base stations to improve signal strength in marginal areas (e.g. Vodafone Sure Signal). This uses the home owner's existing Internet connection to transport mobile phone calls to the mobile carriers switching centre and uses a secure link (VPN) to ensure the data is protected end-to-end from femtocell base station all the way to switching centre. This arrangement actually bears many similarities to the electricity meter scenario whereby a secure link can be set up through a potentially insecure network.

If the same underlying network technology were used in the HAN and WAN, it would potentially allow end-to-end security of data from suppliers' head-end equipment all the way to an electricity meter using transport layer security or IPsec (security for IP packets).

3.3.4 Application layer gateway (ALG)

The extension of IP-based networks using routers is relatively straightforward, as these routers need no knowledge of the application layer running above. However, if the network segments run different network protocols (usually at the edge of the network), it is not possible to route them. It is then necessary to terminate at the application layer within the network segment, translate and carry using a different protocol into the next network segment. This is generally performed by an application layer gateway (ALG) as opposed to a router.

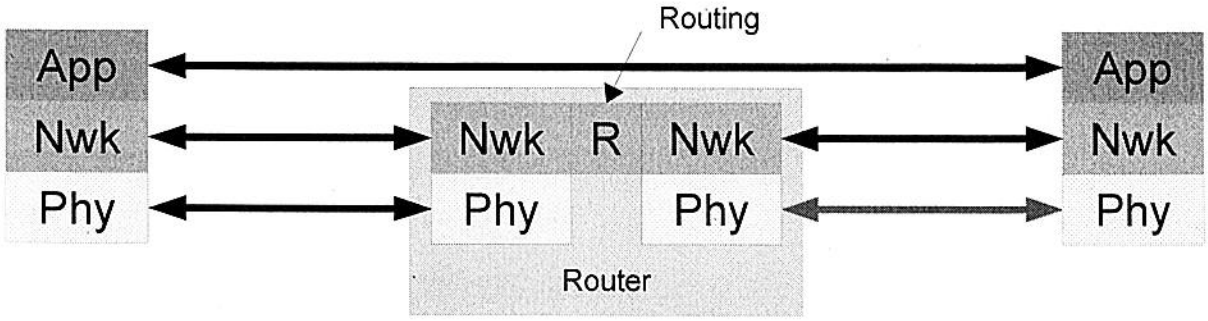
The main disadvantage of this approach is that the ALG is now performing a more complex function than a router and requires full knowledge of two or more application protocols and how to translate between them. This makes cascading of networks much harder as each node has to be aware of the different application layers and how to translate. This would make a large network of many devices impractical, although in a small network such as a home network it is possible due to the relatively limited application layer functionality.

It also makes end-to-end security harder, as there needs to be a common content format between the application layers which can be secured in the same fashion by both application layers running at either end of the connection.

3.3.5 Tunnelling

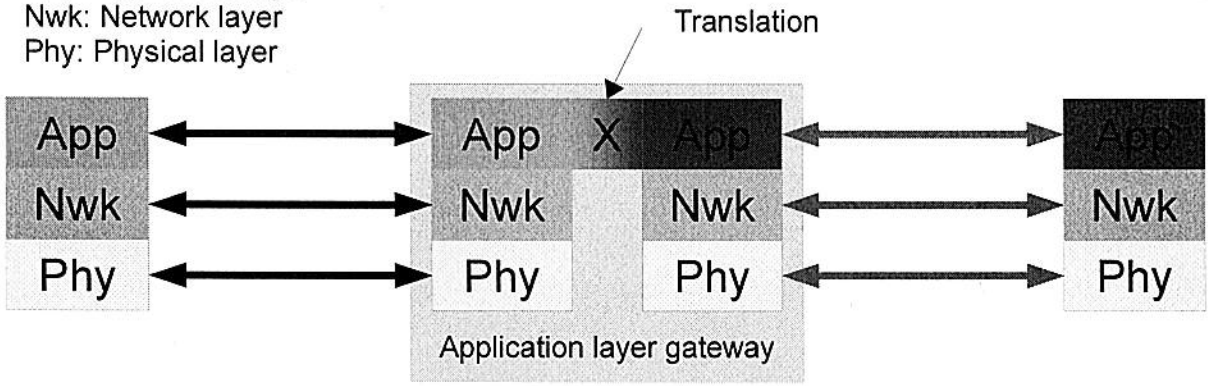
Another approach is to tunnel the application layer data. This means there is no translation taking place and the application layer is simply performing the routing function by encapsulating the original data and transporting it to the end point. This requires the application layer to provide a tunnelling mechanism. This mechanism does not scale well but is adequate for small networks.

Figure 2 illustrates the difference between routing, translation and tunnelling.

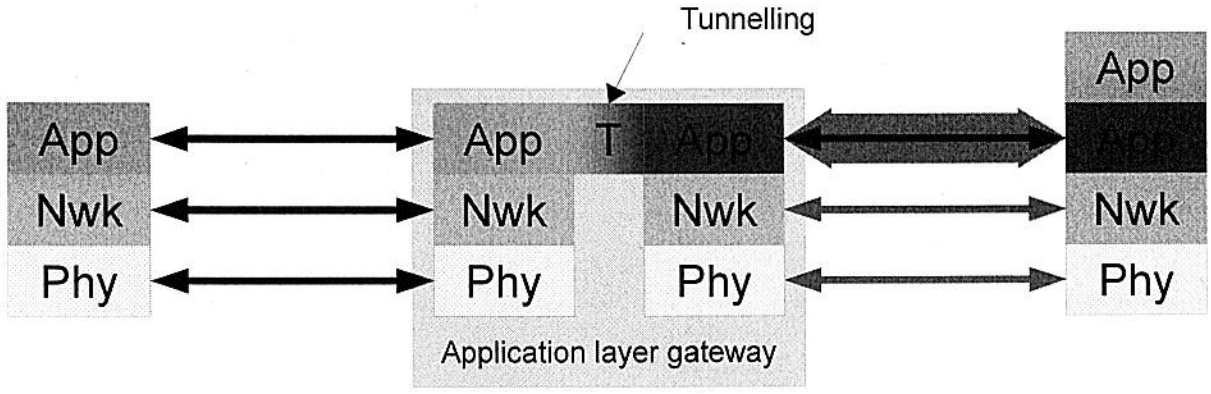


Routing showing end-to end application layer connectivity

App: Application layer
Nwk: Network layer
Phy: Physical layer



Application layer gateway showing application layer translation



Application layer gateway showing tunelling

Figure 2: Difference between routing, translation and tunnelling

3.3.6 Integration of energy management functions

Energy management and monitoring lends itself very well to being integrated into home owners' existing networks and it is more likely to have an impact if it can be seamlessly integrated.

Therefore it is very important to consider how the HAN being specified for Smart Metering equipment will integrate with home owners' existing networks.

Most home owners' existing networks will be based on IPv4 connectivity. IPv6, the next generation of the Internet Protocol, is rapidly gaining momentum and most consumer devices (e.g. notebook computer, tablet, smartphone) used for accessing the Internet, support IPv6. The Internet Service Providers and the home routers generally do not support IPv6 at the moment but this situation is changing rapidly.

Therefore, it would be useful if consumers can easily access energy usage data and devices which will perform this function have been described as Consumer Access Devices (CAD) in the consultation document. These devices can also include home management systems, which may need to combine energy management functions with other typical home management functions, e.g. security. For example, security systems exist today based on IP networking which allows a home owner to look at the images from a CCTV camera installed at the premises over the Internet using a web browser (webcam).

If the HAN were based on IP, CADs could (with appropriate authorisation) access meters and other smart metering equipment directly using an application layer protocol such as ZigBee SEP v2.

If the HAN were based on ZigBee PRO/SEP v1, then an ALG would be needed. It is likely in this case that the ALG would translate and present the data to CADs in a different format to that used by ZigBee, for example, using a web server. One potential issue here is one of interoperability of CAD devices. In many cases, these ALGs are designed to have a common standard interface to one network but often have proprietary application layers on the other network or at least proprietary rendering of the information and treatment of the information. This may not be a particular detraction but it would be useful to have some common format and consistency with the data.

The Green Button initiative in the USA was an attempt to standardise ways of consumers accessing their data over the Internet from the suppliers. It is recommended that the UK government consider a similar approach for both consumers accessing data locally and from their supplier.

4 Consultation Questions

4.1 Chapter 4 – SMETS 2 Development

4.1.1 Home Area Network Solution

1. Do you have any comments on the criteria used in the evaluation of the application layer standards?

The three criteria as stated are important to the selection. With regard to maturity, it is also important to consider how ubiquitous the solution is with respect not necessarily to the whole implementation but to the component parts of the implementation, e.g. stack, hardware etc.

The choices mentioned cover different areas of the protocol stack model; some are more concerned with the physical layers, others are more purely application layer and some vertically cover the whole stack (e.g. ZigBee).

With regard to clause 33, the OSI model is rarely used in real implementations and is more of a conceptual model. The OSI model is also primarily concerned with abstraction, not decoupling. It is also difficult to talk specifically about "endpoints" in any layered stack model as endpoints will differ from layer to layer. The distinction between application layer and physical layer is also not 100% clear but is sufficient for the remainder of the document. The concept of network layer is also important when considering segmentation of the HAN and when considering supporting multiple physical layers.

2. Do you agree with the proposal to adopt ZigBee SEP / DLMS as the HAN application layer standards for GB?

Gridmerge Ltd. agrees to the use of DLMS for electricity meters but does not completely agree with the use of ZigBee SEP v1 for the other devices in the HAN for the reasons given in section 3.3 and to comply with the vision outlined in clause 28.

The use of DLMS and ZigBee SEP (v1 or v2) is complementary to a large extent with little overlap therefore it makes sense to combine them as a choice. However it would be important to clearly understand and specify how the two respective entities present in an electricity meter would communicate internally.

With regard to clause 44, it is also important to consider how DLMS will be tunnelled over SEP v1 to the electricity meter from the communications hub as this will require the electricity meter to have effectively two virtual devices in it, one for communication with the rest of the HAN through normal transactions and one with the Communications Hub tunnelling the DLMS data. The electricity meter will also need to translate between the two protocols internally and serve its internal data to both interfaces so the IHD can read it as well as the Communications Hub. Also the addressing of the electricity meter over the tunnel will effectively have to be handled by the Communications Hub acting as proxy for the electricity meter (see Section 3.3.4)

Gridmerge Ltd. believes that the decision to disregard ZigBee SEP v2 at this stage is unwise. Contrary to the immaturity mentioned in clause 43, the specification for ZigBee SEP v2 is virtually complete, interoperability testing has been taking place for almost a year and it fundamentally supports many different physical layer communications. It is also based on the standards of XML, HTTP, TLS and TCP, which are probably the most widely used protocols existing due to their use in the Internet and the World Wide Web. The ZigBee Alliance has also developed ZigBee IP, which is a specification calling out publicly available and widely-used IETF standards such as TCP, UDP and IPv6, which can be used to transport the SEP v2 application

layer transactions using 802.15.4 radios. This is also complete, with 7 platform suppliers having been involved in interoperability testing for over two years.

The use of IP networking would provide the ability to do real end-to-end security as it is likely data over the WAN would be carried using IP datagrams using a transport protocol such as TCP, which can use transport layer security (TLS). This would not be easy if translation occurs and an application protocol acceptable to both ends with cryptographic protection at a high layer would need to be developed independently.

3. Do you agree that equipment should be required to comply with SMETS and a GB Companion specification for ZigBee SEP / DLMS?

For good interoperability, it is extremely important for equipment to comply to a standard. Both ZigBee and DLMS provide comprehensive conformance programmes and it is important that all the equipment which must interoperate is covered by appropriate conformance plus any additional conformance such as the GB Companion Specification. It may also be necessary to provide additional device conformance as well as the conformance for DLMS and ZigBee address the communications protocols but do not address device functionality; for a truly interoperable and successful roll-out, devices must also perform and function in a consistent manner.

4.1.2 HAN Physical Layer

4. Do you agree with the overall approach proposed in relation to the HAN physical layer? If not, please provide a rationale and evidence for your position.

There seems to be an overriding assumption made that the HAN has to be one physical layer and whilst the position of having both 2.4.GHz and 868 MHz devices in the network has been considered, the options seem limiting. With different approaches, this could be achieved in many different ways. The consideration for wired networks is very vague at this stage and it is impossible to see how the proposed solution could scale for complex deployments such as blocks of flats etc.

5. Do you have any comments on the criteria used in the evaluation of the physical layer of the HAN?

Sufficient bandwidth needs to be considered alongside the actual "goodput" of a technology, i.e. the actual rate of data which can be achieved at the application layer, end-to-end. The latency of the data communication should also be taken into consideration. Gridmerge Ltd. agrees with the choice of 868 MHz and 2.4 GHz for the wireless network to give acceptable bandwidth and goodput, although the 1% duty cycle consideration for 868 MHz is not mentioned.

The radio frequency propagation trial, whilst useful, does not seem to take into consideration the use of mesh networks which are provided through technologies such as ZigBee PRO (as used with SEP v1) and ZigBee IP (as used with SEP v2). Section 3.2 explains how this can simply and cheaply extend the range of a HAN. So whilst 868 MHz may seem an obvious choice, that is based solely on point-to-point one hop radio range.

Interference can manifest itself at any channel and many of the radio modulation schemes in place now have redundancy built in to extend the link budget and to improve reliability. Reliability schemes at higher layers also help to guarantee delivery of data so perceived levels of interference may not manifest themselves as greatly as considered. Whilst it is not a scientific study, it has been noted by many ZigBee manufacturers that their (2.4 GHz) products "just work" in quite challenging environments (for example, trade shows). Standards developed under the IEEE (e.g. 802.15.4 and 802.11) have to go through stringent coexistence evaluation to ensure

that they will not cause undue interference to other IEEE protocols at least and therefore are able to coexist. The use of Wi-Fi at 2.4 GHz has grown immensely over the last few years and whilst there are some interference issues, it generally does work acceptably in environments where there are many coexisting Wi-Fi networks, e.g. in cities.

Development time is an important consideration and a lot of emphasis has been put on developing 868 MHz solutions as opposed to considering mitigation approaches using more intelligent HAN topologies using either mesh networking or multiple sub-networks. Even with the development of an 868 MHz solution, the integration into existing HANs needs to be carefully considered.

6. What are your views on the compatibility of the reserved spectrum 870-876MHz with 868 MHz and the value of considering the use of this band?

It depends on the radio standard used. It is recommended that IEEE 802.15.4g-2012 is specified for the MAC and PHY layers for 868 MHz solutions as it is likely that if the MR-FSK modem specified in 802.15.4g-2012 is used, the hardware will be capable of changing channel easily whilst using the same modulation scheme. There are existing solutions using 802.15.4-2006 radios (O-QPSK) at 868 MHz but these are not compatible with 802.15.4g-2012 solutions.

7. Do you consider that additional measures should be taken to encourage the development of an 868 MHz solution?

The development of an 868 MHz solution is predicated on the fact that communication must be one-hop point-to-point between the devices. There are alternative solutions using just 2.4 GHz radios, for example, mesh networking, which could be proven through further testing. The level of interference may not prove to be as problematic as perceived and in exceptional cases a tight mesh network is likely to provide just as effective a solution as a longer range point-to-point solution based on 868 MHz.

The additional use of IP networking could provide a variety of options for MAC and PHY which could provide a large portfolio of solutions based on commonly-used systems already widely in use in existing home networks, e.g. HomePlug powerline communications or simply Ethernet over twisted pair,

8. Do you agree with the approach to allow the market to determine the balance between 2.4 GHz and 868 MHz? If not, please provide rationale and evidence.

Gridmerge Ltd. does agree with the approach to let the market decide and would also promote consideration of alternative approaches as well, especially those based on IP networking.

9. What are your views on the costs and benefits of the three options identified for deploying wireless solutions (i.e. 2.4 GHz as the default; dual-band communications hubs; or market led)?

For the foundation phase, it is recommended that 2.4 GHz alone is considered. It is likely this would be the market choice as well in this stage. It seems unnecessary to have to develop 868 MHz solutions at this stage and alternative solutions such as low cost repeaters/routers should be considered for exceptional cases where communication is challenging due to propagation issues.

Beyond the foundation phase, Gridmerge Ltd. believes that the most scalable solution exists in IP-based networks. The Government should consider looking into IP-based networks going forward and that equipment being developed now should be able to support moving to IP-based networks. This would facilitate a market-led approach as a variety of underlying physical layers could be developed which would work with a common application layer, instead of trying to adapt a vertically-sliced stack such as ZigBee to many different physical layers. Note also that this does not just limit the choice to another radio, i.e. 868 MHz. Note that work done in the USA

considered this of sufficiently high importance to warrant the formation of a Priority Action Plan (PAP 18) by the Smart Grid Interoperability Panel (SGIP).

10. Do you agree with the proposal for a 'fit for purpose' installation obligation on suppliers?

Gridmerge Ltd. agrees with the proposal and believes that the fit-for-purpose installation obligation would be greatly facilitated where suppliers have a wide choice of equipment to choose from. This position would be greatly facilitated by the use of IP-based networking.

4.1.3 Wired HAN

11. Do you have any views on the proposed approach to developing a wired HAN solution?

The fact there is one short section and one single question in this section suggests it has not been considered in anything like the depth that complex deployment scenarios such as high-rise flats warrant or indeed provision in a standard domestic premises.

It is clear that existing deployments for local area networking in buildings are common place and these are almost universally based on IP networking. Whilst a separate IP-based local area network can be used in a "backbone" fashion to carry data from other non-IP network segments, it makes more sense to have all segments of the network to all the end devices based on IP for the reasons stated in Section 3.3.3 as this simplifies the intermediate devices and provided a highly scalable solution. Alternatively, application layer gateways will need to be deployed at the edge network segments.

The complexity of building the types of network which require multiple segments with distinct security domains should not be underestimated and needs to be considered in conjunction with the development of smart metering equipment specifications for simpler network topologies.

4.1.4 Communications Hub – Introduction

12. Do you agree with the proposed scope of functional requirements for a communications hub? Are there any other functions that should be included and what would be your rationale for including those functions (including estimated costs and benefits)?

It is not clear from clause 64 how the various communications would occur as it states that "the communications hub should support smart metering devices... and consumer access devices (CADs)". It then states that CADs access data from smart metering devices, so it is not therefore clear if the CADs (or even the IHD for that matter) are able to access e.g. the electricity meter directly, or whether all HAN communications would occur through the communications hub. Figures 3 and 4 illustrate the different scenarios (without showing a CAD).

The preference would be to limit the functionality of the communications hub to that solely confined to communications. For this reason, it may be better to consider the gas meter mirror functionality existing within the electricity meter, especially as the two are often located close to each other. This would also suit the CSP-led model better.

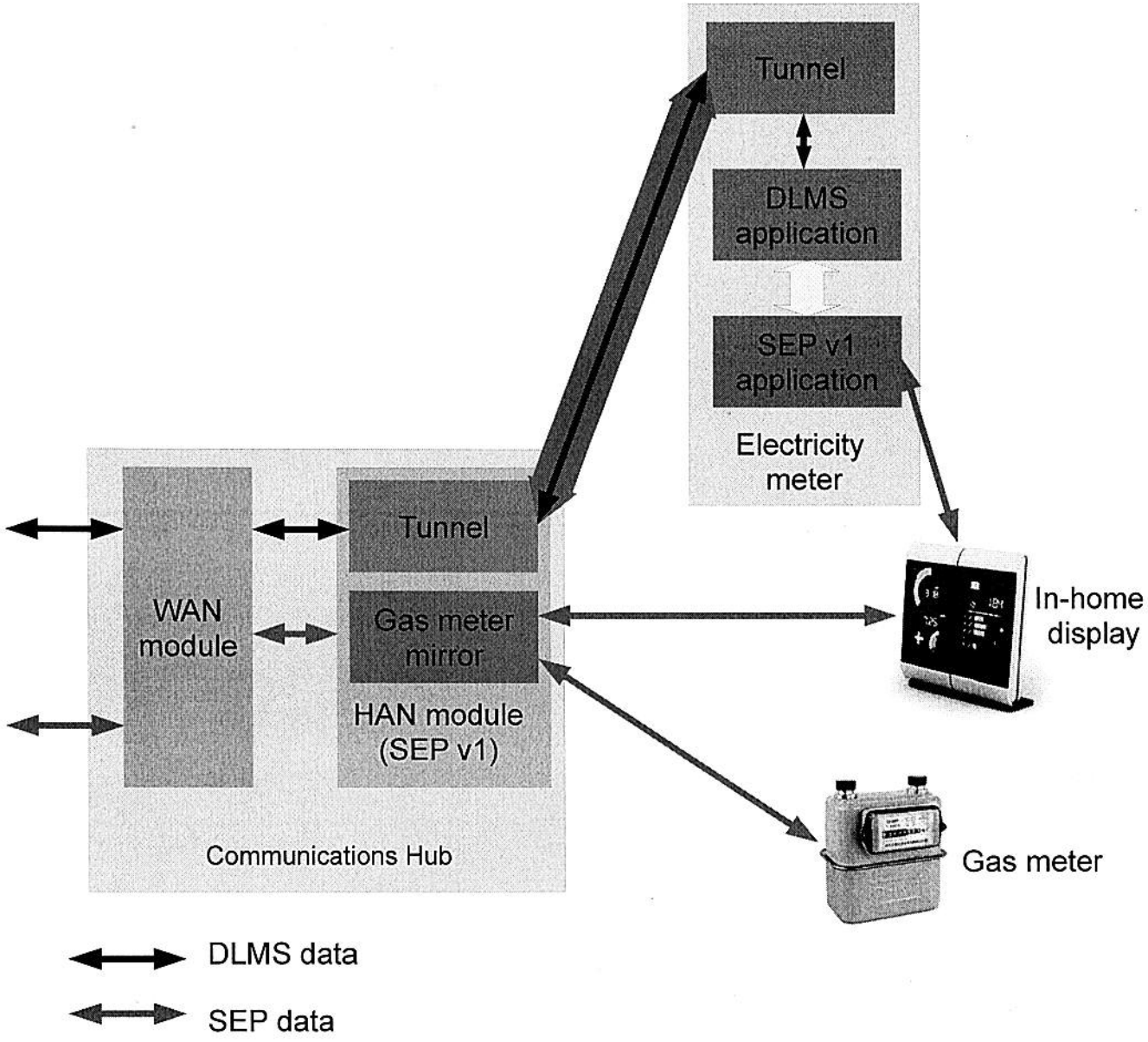


Figure 3: Direct access to electricity meter

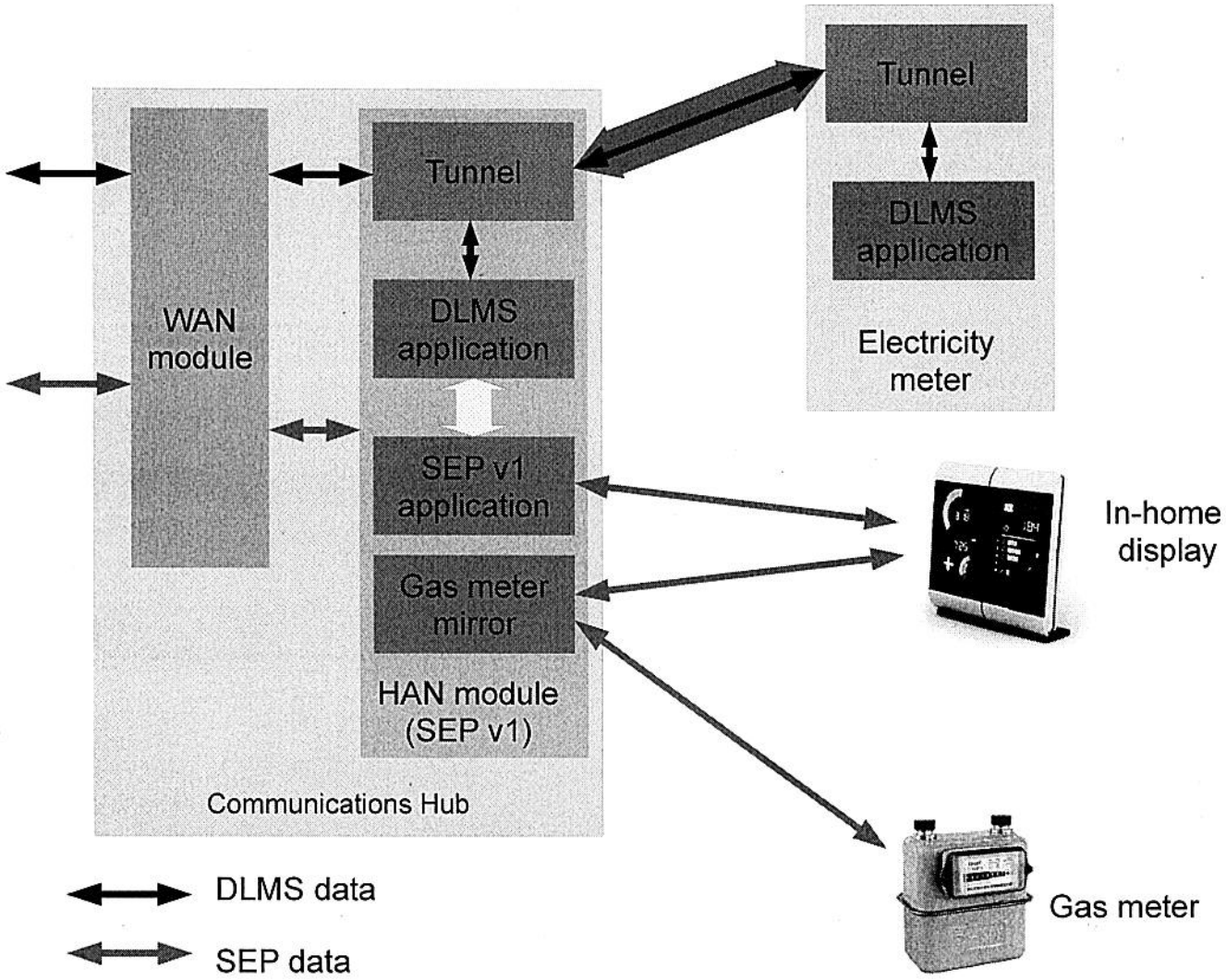


Figure 4: Access to electricity meter through communications hub

13. Do you have views on the specification for an 'intimate' interface between electricity meters and communications hubs?

Regarding clause 65; it would seem unless the communications hub is co-located with the electricity meter, it will be difficult to provide an unmetered mains supply to it. Therefore, if the communications hub and the electricity meter are co-located, it would be sensible to connect the two as expediently as possible using a simple interface, i.e. an "intimate" interface. However, this link still needs to be secure and be able to transport DLMS data to the electricity meter. The use of an intimate interface could eliminate the need for a SEP v1 tunnel if these two devices are no longer required to communicate over SEP v1. In this case, the communications hub would have to represent all the information from the electricity meter which is available to other smart metering equipment and CADs.

4.1.5 Communications Hub – Responsibilities

14. Do you agree with the Government's marginal preference for the CSP-led model for communications hub responsibilities, or do you prefer the supplier-led model? Please provide clear rationale for the advantages and risks associated with your preferred option.

If the communications hub is strictly concerned with providing communications from the WAN to the HAN and there does not have to be any functionality associated with metering, the preference for a CSP-led model is greater, as the role becomes one more associated with communications only.

If the communications hub contains clear metering functionality, whether as a gas meter mirror or proxy for an electricity meter, then it becomes less clear what the preference would be. It is still likely that a CSP-led model would be better as even in this case, the functionality is more of an application layer "relay" of data for the purposes of other smart metering equipment and CADs in the HAN. Therefore the communications hub would have no requirement for conformance testing for e.g. meter accuracy.

It would become clearer if the communications model is clearly established.

A potential issue with the CSP-led model whereby the communications hub is developed entirely independently is if there is an "intimate" interface; this would clearly have to be carefully specified to avoid any interoperability issues. For this reason, it may be more expedient to consider the communications hub and the electricity meter as completely independent from a networking aspect. In this case, IP-based network would also facilitate this, as it gives more flexibility on the physical connection between the two.

4.1.6 Communications Hub – Opted out non-domestic consumers

15. Do you agree with the proposal that a CHTS-compliant communications hub should not be mandated for opted out non-domestic sites and that suppliers should be free to use whatever type of communications equipment best supports their processes and WAN service?

Gridmerge Ltd. generally agrees that a CHTS-compliant communications hub should not be mandated for opted out non-domestic sites. However, if the communications hub is solely for the purpose of communications and does not have to represent metered data, then it is likely that the functionality of a CHTS-compliant and non CHTS-compliant communications hub would be very similar, if not the same. The only clear difference may be the type of WAN used. If IP-based networking is specified, it is likely the same basic equipment could be used with only the WAN module perhaps needing to change. This would mean fewer changes if a premises did decide to opt in or opt out. It is also likely that supplier and CSPs would be more aligned regarding the specification of the communications hub.

16. Do you agree that the gaining supplier should bear the costs of installing an appropriate communications hub if they decide to switch between opted in and opted out?

Gridmerge Ltd. agrees that the gaining supplier should bear the costs of installing an appropriate communications hub. However, every effort should be made to make the specification of the communications hub as generic as possible to facilitate the reuse of equipment as much as possible.

4.1.7 SMETS Additional Capabilities

4.1.7.1 Additional DNO functions

4.1.7.1.1 Outage Management

17. Do you agree that the design and implementation of outage reporting functionality should be assigned to CSPs, documented in the communications hub technical specification?

Gridmerge Ltd. agrees that outage reporting should be assigned to CSPs on the basis that a CSP-led model for the communications hub is preferable and that the communications hub is powered from the unmetered supply which feeds the premises. This would require the communications hub to have a simple power monitoring function which would send an alarm should the power fail.

18. Do you agree that it would be inappropriate to require meters operated outside DCC to be required to implement outage reporting? Please provide rationale to support your views.

Gridmerge Ltd. agrees that it would be inappropriate to require meters operated outside the DCC to be required to implement outage reporting on the basis that an equivalent opted out communications hub would also likely be powered in a similar fashion and would therefore be able to detect the power outage. The only situation where this may be different is if there is any aggregation of multiple reads of meters using a special form of communications hub. Even then, in this case, it does not seem necessary to require the meters to provide signalling to such a communications hub.

4.1.7.1.2 Maximum Demand Recording

19. Do you agree that maximum demand registers should be included in SMETS? Please provide evidence to support your position and provide evidence on the cost implications of delivering this functionality via back office systems or via the meter.

Gridmerge Ltd. agrees that maximum demand registers should be included in SMETS. The main reason for this is to limit the amount of communication required over the WAN for bandwidth and availability reasons. If this information can be recorded as required in the meter then queried as required, it will optimise the communication over the WAN. Given the increase in functionality and complexity required by smart metering anyway, it is unlikely that the addition of three extra registers would have a significant cost impact.

4.1.7.1.3 Additional Voltage Alerts

20. Do you agree with the proposal not to include the capability to generate additional voltage alerts based on counter thresholds in SMETS 2? Do you have any evidence that could justify including this functionality in SMETS 2?

Gridmerge Ltd. does not entirely agree with the proposal not include the capability to generate additional voltage alerts. The main reason for disagreement is on a similar basis to question 19, i.e. that given the increase in functionality and complexity required by smart metering anyway, it

is unlikely that the addition of this capability would have a significant cost impact. On the other hand, it may require more sophisticated metering capabilities on the meter. Gridmerge Ltd. would defer the judgement to meter manufacturers.

4.1.7.1.4 Access to remote disablement by multiple parties

21. If DNOs were permitted to access remote disablement functions, should control logic be built into DCC systems or meters? If the logic should be built into meters, should the logic be specified in SMETS 2? Please provide rationale to support your position including estimates of the cost of delivering this functionality under the different options being considered and any evidence relating to safety issues associated with each option.

It would seem that it is only really possible to build control into the DCC given the current smart metering equipment technical specifications and on the basis that the WAN communications goes solely to the DCC. It may be feasible to consider sharing of the WAN between DCC and Smart Grid operations. Even then delivery to the meter should be the same, however the meter would need arbitration logic to sure disablement functions originating from different sources do not conflict. The cost of arbitration logic is negligible in that it is simply code in the meter.

Gridmerge Ltd. believes arbitration logic should be built into the meters in any case to enable future proofing. Arbitration logic could also act as a fail-safe within the meter itself in case of WAN failure causing apparent conflicting request. However, alternative communications paths into the meter do not need to be considered at this stage.

4.1.7.1.5 Electricity Meter Variants

22. Do you agree that variant smart electricity meters should be specified in SMETS 2 and that the cost uplift for variant smart meters is similar to that for variant traditional meters? Please provide evidence of costs to support your views on cost uplifts.

Gridmerge Ltd. agrees that variant smart electricity meters should be specified in SMETS 2. The cost uplift is similar because the additional cost is down to communications ability This communications ability is fundamentally the same in a traditional and variant meter.

4.1.7.1.6 Randomisation of auxiliary load control switches

23. Do you agree that randomisation offset capability should be included for auxiliary load control switches and registers as described above? Do you have views on the proposed range of the randomisation offset (i.e. 0 – 1799 seconds)? Please provide evidence on the cost of introducing this functionality.

Gridmerge Ltd. agrees that randomisation offset capability should be included for auxiliary load control switches on the basis that this facility is normally included in the application protocols for load switching (i.e. ZigBee SEP v1/SEP v2). The range of 0 to 1799 seconds seems appropriate.

4.1.7.2 Interface Requirements

4.1.7.2.1 Consumer Access Devices

24. Do you support Option 1 or Option 2 for 'pairing' a CAD to the HAN? Please present the rationale for your choice and your views on the implications that these options have for the technical design of the solution.

Gridmerge Ltd. considers that the two options presented are too simplistic and there are numerous possibilities for pairing.

Most importantly, there are two aspects to "pairing" which should be considered separately:

- Network Access authentication and authorisation
- Application layer authentication and authorisation

In some cases the two operations may be merged but there are many cases where they should be treated independently.

Network access depends on how the CAD is introduced into the network and how the network is combined with respect to its segments. If the CAD is an application layer gateway (ALG), it would need to be paired using the mechanism broadly described in Option 2. The ALG would have appropriate credentials to enable it to be authenticated as a genuine SEP HAN device and subsequently authorised to perform smart metering functionality. However, the ALG may then also access the home owner's existing LAN, in which case it would typically use WPS (Wi-Fi Protected Setup) or WPA-PSK where the home owner uses the passphrase configured in the home router to join the home owner's LAN. Thus, if an ALG is used, two independent application layer authentication and authorisation procedures may be needed:

- Between ALG and communications hub
- Between other device(s) and ALG

Unless tunnelling is taking place, the ALG is then responsible for marshalling and translating transactions between the application layer entities.

If the CAD is a simple router, it could gain network access in the same way as an ALG on both of its interfaces but the application layer entities would be able to authenticate end-to-end through the network segments. This would require the same application layer protocol to be running on the CH as the other CADs behind the CAD router but this would be desirable from an interoperability point of view anyway.

This is illustrated in Figures 5 and 6.

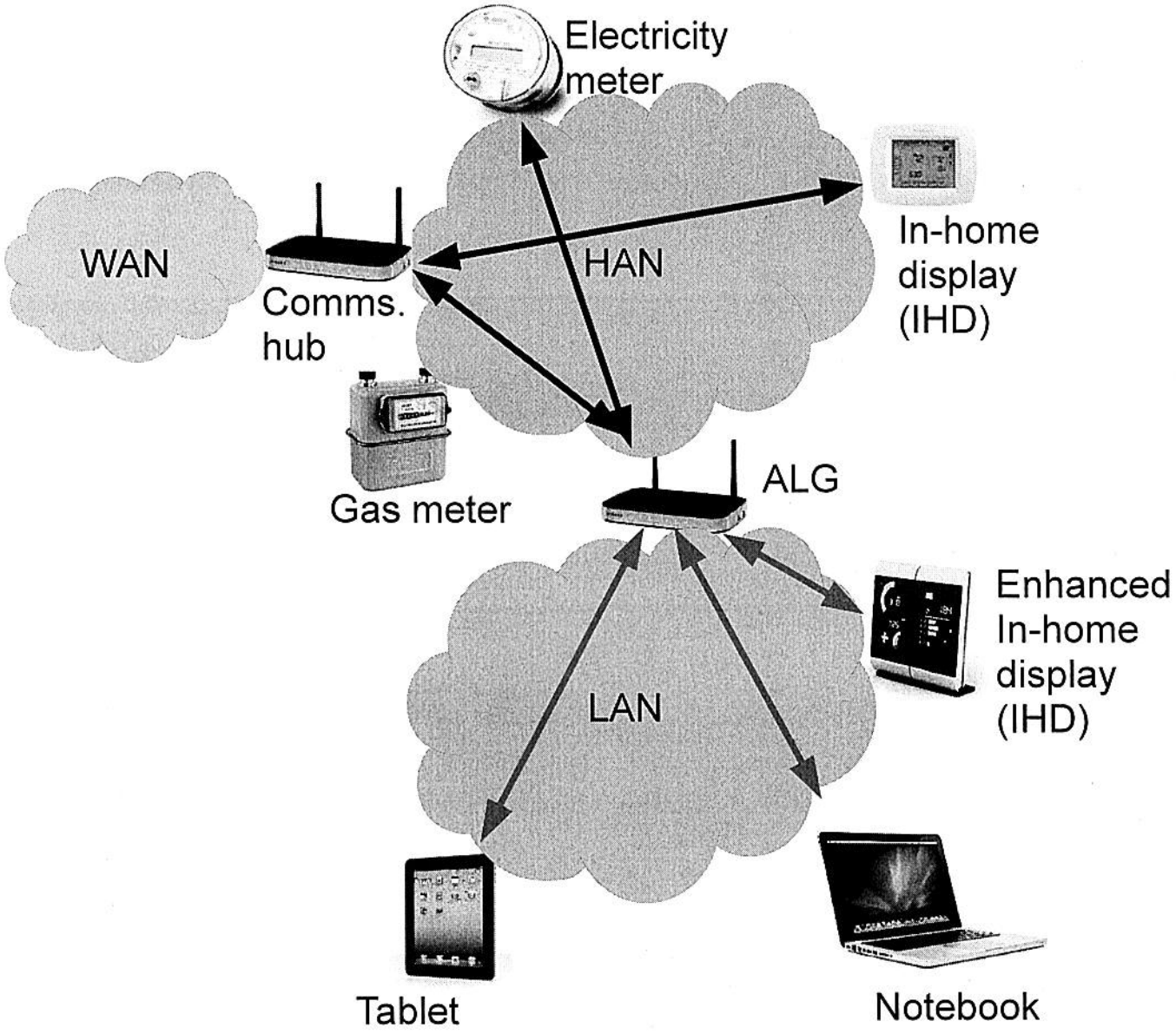


Figure 5: Application layer gateway between network segments

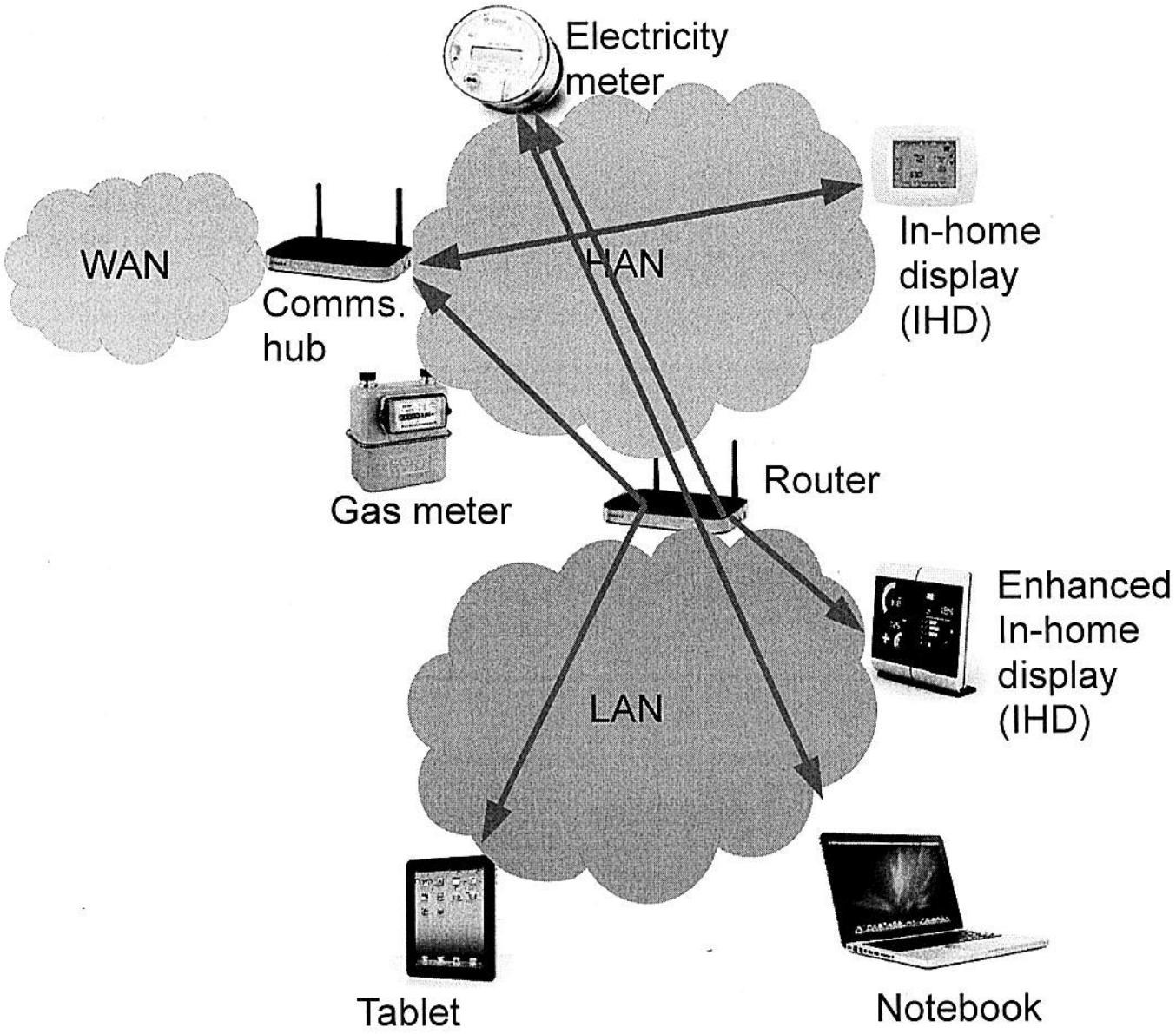


Figure 6: Router between network segments

Clause 130 suggests these devices would also be connected to the Internet, thus clearly hinting at the need for an ALG or HAN-LAN router as depicted in the Figures above. Clause 131 also suggests that a CAD could also be a LAN connected device. If IP-based networking is used then there is no particular distinction; the HAN and the LAN effectively merge into one.

Clause 134 states that there will be restricted access from CAD devices. This can be achieved using access controls or by "air gapping" if an ALG is used. Access control uses authentication and configuration to determine if the device is authorised to access data. This configuration has some similarities to how a firewall tends to work and indeed firewalling can also be provided as well as application layer access control. "Air gapping" uses the fact that translation has to occur to provide some isolation between the data access by the ALG and then relayed to the CAD.

It is not clear in clause 136 what issues having shared physical spaces has for privacy with regard to the HAN. The use of a HAN may allow removal of external displays but it is extremely unlikely this will happen as a fundamental reading needs to be easily available.

Considering the two options proposed for pairing:

Option 1: The passkey should not be confidential information and the use of a shared secret for pairing is strongly discouraged. It is suggested that a device ID based on a certificate fingerprint is used. This is not confidential but when the certificates are validated it can be confirmed that the actual device performing the handshake is associated with the passkey/device ID). Some visual feedback is also suggested to confirm both devices have paired successfully.

Option 2. It is recommended that shared secrets are not used either and that it is preferable to use a device ID. On the other hand, it is useful to have a PIN on the joining device to be presented securely on joining to ensure the joining device has steered to the correct network. This PIN may be fixed in case of devices with no UI, or can be configured by the user in other cases.

25. If Option 2 were adopted, do you agree that obligations should be placed on energy suppliers to support this process by submitting 'pairing requests' to the DCC on request from their consumers?

Gridmerge Ltd. agrees that obligations should be placed on energy suppliers to support this process by submitting 'pairing requests' to the DCC on request from their consumers on the basis that this mechanism has been used successfully in Texas, which has similarities in its deregulated market.

26. Do you consider that other CAD installation options should be pursued? If yes, please explain the approach you favour and your reasons.

Gridmerge Ltd. believes that it is difficult to specify basic pairing operations as it depends very much in the capabilities of the devices. As mentioned above, the concept of network access and application layer authentication also needs to be distinguished.

4.1.7.2.2 Microgeneration meters

29. Do you agree with the proposal that the communications hub should be specified such that it can support multiple smart electricity meters? How many smart electricity meters should be supported by each communications hub?

Gridmerge Ltd. agrees with the proposal that the communications hub should be specified such that it can support multiple smart electricity meters on the basis that it is essential that the system is future-proofed given the proposed lifetime. It is not clear whether these would be DLMS-capable meters but the assumption is that they would be. It may not be important to support them in the foundation stage but the communications hub should have capacity to

support upgrades to enable assimilation of further electricity meters in the future. This is also important for sub-metering for plug-in electric vehicles and could be combined with allowing multiple service providers for energy. On this basis, it is suggested a minimum of two additional electricity meters should be supported for a domestic premises to account for solar microgeneration and electric vehicle submetering.

4.1.7.2.3 Hand-held Terminals

30. Do you agree that a specification for a HHT interface to the HAN should be defined? If yes, please identify the functions that this interface would need to support and the scenarios in which such functionality could be required.

Gridmerge Ltd. mostly agrees with the proposal that a specification for a HHT interface to the HAN should be defined.

The most important general functions for a HHT are:

- System configuration
- Diagnostics

With regard to system configuration, the HHT could be used to configure any device already connected to the HAN and to assist commissioning of new devices on the network. Generally speaking, the interface would need to support modification of attributes in the devices which in turn would change the data and state of the device in its operation within the system. Specific attributes would need to be identified and very strong access control would need to be in place to ensure only an authorised HHT would be able to access these attributes.

With regard to diagnostics, a HHT can be used to assist fault finding. In this case, the interface would need to support reading of device logs and potentially other attributes associated with diagnostic functions. Again, similar strong access control would be needed and more importantly in this case, authentication of the HHT must be able to take place without any access to the WAN. This provides a particular challenge as the use of pre-shared secrets is known to be flawed in this case as revelation of the secret can compromise all communications with the device and leave it particularly vulnerable to attack.

Therefore, the most important issue to consider with the use of the HHT is security. It is essential that strong authentication is used so it is not possible for an attacker to easily recreate a HHT and use it to access a system, either as an insider (with an aim to gain financially, for example) or as an outsider with malicious intent. This has many challenges for the situation where the device under diagnosis may have no external means to securely identify and authenticate the HHT.

Gridmerge Ltd. has a proposal for securely authenticating HHTs for supplier-owned devices which requires a one-off pre-configuration of the device and subsequent identity assignment to a HHT to provide it with a time-limited secure token which can be used to the supplier-owned device. This would prevent any unauthorised access to supplier-owned devices. Gridmerge Ltd. would be willing to supply more details on its proposal to interested parties.

4.2 Chapter 5 – Governance and Assurance of Security and Interoperability

4.2.1 Governance of Security Requirements

31. Do you agree with the proposed approach to the governance of security requirements? If you propose alternative arrangements please provide evidence to support your views.

Risk assessment and modification of requirements in light of the outcome of the assessment. This needs to be a continuous programme with the ability to collect reports of security breaches and vulnerabilities and to produce mitigating responses in a timely manner.

It is not clear which body would actually manage this programme. Whilst it is clear the DSP and CSP would have their own programmes for the DCC systems, it is not entirely clear who would run the programme regarding security of the connected devices. The conformance testing groups could be contracted to perform such a function as their members typically comprise the product manufacturers, therefore this would be an appropriate forum. However, product manufacturers also are understandably reluctant to admit breaches of security in their equipment so the organisation may need to be an independent organisation with a high degree of confidentiality with regard to publicising events to ensure they can be fixed before they can be widely exploited. Therefore, Gridmerge Ltd. approves of the proposal of a SEC technical sub-committee to perform this function.

4.2.2 Assurance of Security Requirements

4.2.2.1 Independent assurance of DCC and DCC Users

32. Do you agree with the proposal to establish independent assurance procedures for DCC and DCC users? Please explain your views and provide evidence, including cost estimates where applicable, to support your position. Comments would also be welcome in relation to the impacts and benefits of the proposed approach with regard to small suppliers.

The risk-based approach is somewhat flawed in that there has to be a subjective assessment to rank DCC users in order of risk. This assessment in itself has risk. Therefore Gridmerge Ltd. agrees that the role-based approach should be taken on the basis that roles can be objectively identified.

Gridmerge Ltd. also agrees that the assessment should be done by an independent body for the reason stated in the consultation, i.e. that it is more consistent, thorough and that appropriately skilled people will be undertaking the certification/accreditation process. It is however important to ensure that the certification bodies themselves are subject to audit and it is proposed a SEC panel is in charge of this.

33. Do you agree with the proposal that re-testing should occur at least at set intervals and more frequently when significant changes to systems or security requirements are introduced? Please explain your views.

Gridmerge Ltd. agrees with the proposal that re-testing should occur at least at set intervals and more frequently when significant changes to systems or security requirements are introduced on the basis that a continuous improvement programme needs to be in place to continually assess the security of the system. This can be achieved by a parallel programme of re-testing which can in itself augment and enhance the testing programme, making it more mature, robust and rigorous as the programme proceeds. One of the inputs to this programme needs to be changes to the functional specification of the system as any change could have a potential impact on

security. Each functional change should have security considerations associated with it and those security considerations may require additional changes beyond simply those required to comply with the functional requirement.

4.2.2.2 Independent assurance of smart metering equipment

34. Do you agree with the proposal to establish an independent security certification scheme for smart metering equipment? Do you have any views on the proposed approach to establishing a certification scheme or evidence of the costs or timelines for setting up such a scheme or submitting products for certification?

With regard to smart metering equipment, it is important that whoever undertakes the independent security certification has a full and thorough understanding of smart metering and smart grid device security, which inevitably shares many characteristics with information security but has additional considerations which are often overlooked. The risks are different to those associated with information technology systems and risks associated with control systems and power engineering must also be considered. For example, the US government commissioned the development of the NISTIT 7628 Guidelines for Smart Grid Cyber Security. Therefore, it is recommend that the technical experts are drawn from those with the most real world experience.

It is also important to categorise devices appropriately and not to impose highly stringent security constraints on consumer products which may not be able to bear a high cost of certification, for example, in home displays. In these cases, it may be sufficient to accept certification carried out in accordance with associated standards, e.g. ZigBee Alliance or Wi-Fi Alliance.

4.2.3 Non-compliance with security requirements

35. Do you agree that sanctions for non-compliance with security requirements should be included in the SEC? Do you have views on the nature of the sanctions that might be imposed?

The criteria for non-compliance are not set out in the document, therefore it is difficult to make a judgement. If the security requirements and associated conformance testing are set out to be rigorous, non-compliance should only result from continuing testing and vulnerability discovery. It is more important in this case to have a continuous improvement programme which can incorporate such discoveries back into the testing and certification process to ensure the security requirements and associated conformance testing continue to mature and have rigour.

4.2.4 Security for smart meters not enrolled in the DCC

36. Do you agree with the proposal to, in effect, extend the arrangements already proposed for SMETS installations prior to DCC operation, to all installations being operated outside DCC? Please provide evidence of the costs that might be incurred and the impact of this approach on small suppliers.

Gridmerge Ltd. agrees with the proposal to, in effect, extend the arrangements already proposed for SMETS installations prior to DCC operation, to all installations being operated outside DCC on the basis that it may promote a level of standardisation and interoperability which may not otherwise occur.

4.2.5 Assurance of Equipment

4.2.5.1 Assurance of Smart Metering Equipment

37. Do you agree that interoperability is central to the development of a successful smart metering solution and that activities related to the assurance of SMETS equipment should be governed by SEC? Please provide views on the governance arrangements that would be appropriate for assuring interoperability of smart metering equipment.

Gridmerge Ltd. strongly agrees that interoperability is central to the development of a successful smart metering solution and that activities related to the assurance of SMETS equipment should be governed by SEC. Existing organisations (e.g. the ZigBee Alliance) can provide a large amount of the certification required for interoperability and in some cases, it may be necessary to provide additional certification for particular device types and products to ensure a consistent behaviour and functionality. The SEC should oversee the formation of such additional certification organisations.

38. Do you agree with the creation of an 'approved products' list and the requirement on suppliers and CSPs to obtain, retain and provide evidence of appropriate certification should apply regardless of whether they intend to enrol the equipment in DCC?

Gridmerge Ltd. agrees with the creation of an 'approved products' list and appropriate certification. This is in line with the programmes already offered by existing certification organisations such as the ZigBee Alliance. Regarding clause 197, any evidence of requirement for increase rigour should be fed to the certification body in question to ensure they improve their test specifications as part of a programme of continuous improvement. Regarding clause 199, Gridmerge Ltd. believes that approval by a sub-committee of the SEC panel is appropriate but only as a superordinate certification body, i.e. it should attempt to use already-existing certification as much as possible and engage with those organisations to ensure their processes are fit for purpose for ultimate product certification.

39. Do you agree that protocol certification (against a GB Companion Specification) should provide adequate assurance that a product will meet interoperability requirements? Please explain your views and identify any additional assurance testing that you consider to be necessary and the rationale for including such testing.

Gridmerge Ltd. agrees that protocol certification (against a GB Companion Specification) should provide adequate assurance that a product will meet interoperability requirements but that the GB Companion Specification should be developed in conjunction with the appropriate certification body. This will ensure the right parties with the appropriate experts are developing the specification. However, one function of the SEC should be to audit the processes of the certification bodies to ensure they are satisfactory and to insist on remedial action to improve rigour should it be required.

Regarding clause 203, Gridmerge Ltd. disagrees with the assertion that customers will switch to another standard. This raises a number of important points:

- Should this situation arise, the existing attempt to standardise would be considered an unmitigated and embarrassing failure
- Steps must be taken early on in the process to ensure this cannot happen
- Speaking from experience, incentivisation is not sufficient to guarantee rigour in the testing and certification process.

- The Government should insist that the certification bodies provide ample evidence of rigour in the testing and certification process and that the certification bodies themselves should agree to a rigorous assessment of their testing and certification process.

Regarding clause 207, Gridmerge Ltd. believes that certification should be product focused and the consumer may get confused if there is more than one certificate for each product. It would be clearer if the is a superordinate certification programme for each product which amalgamates all the subordinate certification required for the product into one certificate. This certificate can be issued in conjunction with a secure credential which testifies it has been certified to a certain level and thus can be used as part of the authentication and subsequent authorisation of devices to function as approved smart metering equipment.

4.3 Chapter 7 – Next Steps

4.3.1 Regulatory framework

45. Do you agree with the proposed changes to the smart metering regulatory framework to reflect the CSP-led model for communications hub responsibilities? Are any other changes necessary?

Regarding clause 232, Gridmerge Ltd. believes it would be prudent not to defer consideration of a wired HAN solution until later as it is likely that a seamless and interoperable implementation will be compromised with this approach. Gridmerge Ltd. is concerned that the existing stakeholders may not understand the intricate details of HAN communications technology sufficiently and strongly recommends that the Government engages experts in this field.

Gridmerge Ltd. agrees with the statement regarding the communications hub specification and the development of a CHTS in conjunction with the SMETS 2.

46. Do you agree that the equipment development and availability timelines are realistic? Please give evidence.

Gridmerge Ltd. agrees that the equipment development and availability timelines are realistic based on significant experience in developing such products and the maturity of devices in the market place. However, effort needs to be put in to developing the GB Companion Specification as soon as possible and to develop the conformance testing programme.

47. Do you agree that SMETS 2 should only be designated when the Government has confidence that equipment to satisfy the new requirements is available at scale? Should a further period of notice be applied to ensure suppliers can manage their transition from SMETS 1 to SMETS 2 meters?

Gridmerge Ltd. believes that SMETS 2 should be designated now and that transition encouraged immediately. It is not clear how SMETS 1 meters can even have been developed considering there was no HAN standard specified. If SMETS 1 meters have been introduced with no HAN capability, it is likely they will be upgradable by the installation of a HAN module and, if they have a WAN module, it may be possible to consider a SMETS 2 meter with communications hub capabilities as well.