



---

**Technical Document**

**Response to Smart Metering  
Prospectus for September 28th 2010**

---

<b>Project</b>	Ofgem E-Serve Smart Metering Prospectus
<b>Author</b>	[REDACTED]
<b>Document Ref.</b>	OSMP/TD000001/V1.0/rcc
<b>Date</b>	
<b>Status</b>	Release
<b>Distribution</b>	

---

## Revision History

Version	Date	Description
1	27/09/10	First release

# Contents

## Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
1.1	About Gridmerge Ltd.....	5
1.1.1	Contact details.....	5
1.2	About Robert Cragie.....	5
1.3	Involvement in USA Smart Grid activities.....	6
1.4	Gridmerge Ltd and the UK programme.....	6
1.5	Gridmerge Ltd.'s Prospectus Questions response.....	7
1.5.1	Response provided.....	7
1.5.2	No particular comment.....	7
<b>2</b>	<b>Prospectus Questions.....</b>	<b>8</b>
2.1	Question 6 response.....	8
2.2	Question 7 response.....	8
2.3	Question 17 response.....	8
2.4	Question 18 response.....	8
2.5	Question 19 response.....	8
<b>3</b>	<b>Detailed analysis of Statement of Design Requirements.....</b>	<b>9</b>
3.1	Clause and figure comments.....	9
3.1.1	Section 1.....	9
3.1.2	Section 2.....	9
3.1.3	Section 3.....	9
3.1.4	Section 4.....	10
3.1.5	Section 5.....	11
3.1.6	Catalogue: Security and Privacy Requirements.....	11
3.1.7	Catalogue: HAN Requirements.....	12
3.1.8	General and Operational Services: Diagnostics.....	13
3.1.9	Appendix A3.....	13
3.2	Questions from Statement of Design Requirements.....	13
3.2.1	Question 1.....	13
3.2.2	Question 2.....	14
3.2.3	Question 3.....	14
3.2.4	Question 4.....	15
3.2.5	Question 5.....	15
3.2.6	Question 6.....	15
3.2.7	Question 7.....	15
3.2.8	Question 8.....	15
3.2.9	Question 9.....	16
3.2.10	Question 10.....	16
<b>4</b>	<b>Prospectus general response.....</b>	<b>17</b>
4.1	Need for network communications expertise.....	17
4.2	Keep pace with the data communications.....	17
4.3	In-home display focus.....	17
4.4	Layered stack approach to interoperability.....	17
4.4.1	Layer 1.....	17
4.4.2	Layer 2.....	18

4.4.3	Layer 3.....	18
4.4.4	Layer 4.....	18
4.4.5	Layers 5 to 7.....	18
4.4.6	Recommendations.....	18
4.5	HAN design approaches.....	19
4.6	Why ZigBee?.....	19
4.6.1	History behind ZigBee Smart Energy Profile (SEP) 1.0.....	19
4.6.2	The need for ZigBee SEP 2.0 and ZigBee IP.....	20

# 1 Introduction

This document is the response by Gridmerge Ltd. to the Smart Metering Prospectus published by Ofgem E-Serve on 27th July 2010 to the questions requiring response by September 28<sup>th</sup> 2010. Gridmerge Ltd. will provide a following document for questions requiring response by October 28<sup>th</sup> 2010.

Gridmerge Ltd. provides this response as an individual.

## 1.1 About Gridmerge Ltd.

Gridmerge Ltd. is a Smart Grid Communications 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.

The Director of Gridmerge Ltd. is Robert Cragie.

### 1.1.1 Contact details

[REDACTED]

Gridmerge Ltd.  
89 Greenfield Crescent  
Grange Moor  
Wakefield  
WF4 4WA  
United Kingdom

[REDACTED]

[REDACTED]

## 1.2 About Robert Cragie

Robert has been Chair of the ZigBee Alliance Security Task Group since September 2006 and was MAC/Security Technical Editor for the IEEE 802.15.4-2006 wireless networking standard, which is widely used in sensor network and Smart Grid and Smart Metering deployments. He is currently Co-Editor-In-Chief for the upcoming ZigBee IP Specification and a Security editor for the ZigBee SEP 2.0 specification and was Security Editor for the ZigBee SEP 1.0 specification and the ZigBee PRO specification. He currently works through Gridmerge Ltd. as a consultant for the Pacific Gas and Electric company in the Standards and Security areas. Prior to that, he was a Systems Architect at Jennic Ltd. (now part of NXP Semiconductor), where he architected the first ever system-on-chip 802.15.4 device and participated in ZigBee and 802.15.4 stack design and development.

### 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 6.7 million Smart Meters in a programme of installing 10 million Smart Meters. They have employed experts and consultants (including Gridmerge Ltd.) in the wide ranging area of Smart Grid development in the state of California.

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 cybersecurity.

Gridmerge Ltd. has been involved heavily in the US standards groups with regard to development mainly in the HAN and cybersecurity 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 6lowpan working group	Contributor
IETF roll working group	Contributor
IETF core working group	Contributor
UCAIUG OpenSG OpenHAN	Contributor
NIST SGIP Cybersecurity Working Group (CSWG)	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 and Ofgem E-Serve, especially in the Home Area Networking and cybersecurity areas, and would thus be able to provide key input to the SMDG and the PSAG.

## 1.5 Gridmerge Ltd.'s Prospectus Questions response

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

- Network Communication Protocols
- Application Protocols
- Cybersecurity

### 1.5.1 Response provided

Prospectus questions regarding response by 28th September 2010 to which Gridmerge Ltd. will provide a response in this document are:

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

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

*Question 17: 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?*

*Question 18: 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?*

*Question 19: 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?*

### 1.5.2 No particular comment

Prospectus questions regarding response by 28th September 2010 to which Gridmerge Ltd. has no particular comment are:

*Question 3: 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)?*

*Question 16: 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)?*

*Question 20: 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?*

## 2 Prospectus Questions

### 2.1 Question 6 response

*Do you have any comments on the functional requirements for the smart metering system we have set out in the Functional Requirements Catalogue?*

Comments can be found in section 3.

### 2.2 Question 7 response

*Do you see any issues with the proposed approach to developing technical specifications for the smart metering system?*

Comments and responses can be found in section 3.

### 2.3 Question 17 response

*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?*

In general, the author has no specific comments with regard to the implementation and rollout strategy. With regard to the staged approach, the author believes it is feasible to implement a Smart Metering system before the DCC services are available providing the guidelines regarding interoperability and using open standards are given the utmost priority. This would facilitate a phased migration to the DCC and independent development of the DCC.

### 2.4 Question 18 response

*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?*

Comments can be found in section 3. In general, the author believes that existing HAN technologies can be used now, which would accelerate initial trials and rollouts, for example the use of ZigBee SEP 1.0 as specified by British Gas/Centrica in their initial rollout.

### 2.5 Question 19 response

*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?*

The author believes that there is sufficient expertise and that the technical specifications can be agreed on more quickly than the plan assumes, especially with regard to the HAN technology. This is based on the author's own experience in the Smart Grid and Smart Meter industry in the USA. The primary guiding principles which will achieve this are:

- The use of existing proven HAN technology
- The ability to upgrade the HAN technology
- The use of prolific, world wide open standards going forward



## 3 Detailed analysis of Statement of Design Requirements

A detailed analysis of Ref 94b/10 Smart Metering Implementation Programme: Statement of Design Requirements was undertaken to consider responses to this question. The responses to the questions asked in this document also answers Prospectus Question 7 to some extent.

### 3.1 Clause and figure comments

#### 3.1.1 Section 1

##### 3.1.1.1 Clause 1.5

Compliance with functional requirements and technical specifications must be performed in conjunction with a rigorous and stringent certification programme. This area can be overlooked for many reasons, the primary one being the lack of incentive for test houses, who typically bill by time and materials, to spend a large amount of time and money upfront in developing the test specifications they will ultimately use. This can be rectified by forming fully-fledged certification bodies who are responsible (and more importantly funded) to develop the test and certification programmes.

##### 3.1.1.2 Figure 1

The diagram mixes devices and networks in an unclear manner.

- In-home display, Smart meter electricity, Smart meter gas are all devices (physical or logical)
- Home area network and Wide Area Network are not devices but are shown connecting to devices
- It is therefore not clear what the connections represent – either application binding or network connectivity
- There is no device shown connecting to the Home area network and the Wide Area Network
- The other device have unidirectional arrows going in different directions. It is not clear what these flows represent

##### 3.1.1.3 Clause 1.10

‘Communication hub’ is mentioned but this does not figure on the Figure 1.

#### 3.1.2 Section 2

##### 3.1.2.1 Clause 2.17

The storage of data is not mutually exclusive. It is highly likely services will be offered which can aggregate data from various sources.

#### 3.1.3 Section 3

##### 3.1.3.1 Clauses 3.4 and 3.5

This limit suggests a low power communications technology would be preferred.

#### **3.1.3.2 Clause 3.19**

This suggests the technologies are independent from the HAN, however this may not necessarily be the case.

#### **3.1.3.3 Table 4**

100k bytes as an upper limit for firmware upgrade may be too low.

#### **3.1.3.4 Clause 3.20**

The author agrees with the current position that there is a requirement for the WAN hardware to be exchangeable without exchanging the meter as there is less possibility for adaptation in the neighbourhood area.

#### **3.1.3.5 Table 5**

It is not clear why a gas meter would have a higher cost for interoperability level in the HAN

### **3.1.4 Section 4**

#### **3.1.4.1 Clause 4.3**

Subjective statements by 'security specialists' need to be analysed very carefully. A holistic view of security needs be carefully undertaken, with a proper threat analysis regarding typical usage and deployment scenarios and the respective security domains. The author will submit a more comprehensive report regarding security in the next submission before the due date of 28th October

#### **3.1.4.2 Clause 4.9**

The author agrees with the need for open standards and protocols within the HAN. However it is important to understand that it is more than just naming a particular standard. Considerable effort needs to go into specifying how the standard is actually used with regard to configuring the often large number of operational parameters in a manner which ensures interoperability. It is also important to ensure that communications stacks with different underlying layer 2 technology can also interoperate at an appropriate level, whether it is as a layer 3 router or a layer 7 application gateway. It is this task which is being undertaken by, for example, the ZigBee Alliance with regard to development of the ZigBee IP stack.

#### **3.1.4.3 Clause 4.10**

Significant innovation is underway with respect to establishing a truly open standards-based system by groups like the ZigBee Alliance and the WiFi Alliance. The author strongly recommends that solutions which use the most prolific standards worldwide are considered first and that there should not be any attempt at islanding technology based on geographic origin.

#### **3.1.4.4 Clause 4.11**

The author does agree that the certification programme for some of these devices has been lacking thus leading to poor performance in the field. However the author disagrees fundamentally that this implies that all of the HAN technology options are at a low technology readiness level. The author considers the technology readiness level of ZigBee SEP 1.0, for example, to be very high and the poor performance is an indictment on the performance of the conformance test houses, not the technology itself.

#### **3.1.4.5 Clause 4.12**

The author disagrees with the statement that there is no 'one size fits all' solution. The author does agree that certain installations may have different requirements on the medium used for communication and therefore recommends that a HAN solution which has flexibility with regard to the physical medium should be selected. There may be scenarios where it is better to use two HAN technologies. This could be accommodated by low-cost bridging devices. In this case, it must be clear through a certification policy which devices would reside on which type of HAN and testing must be rigorous with regard to interoperability.

#### **3.1.4.6 Clause 4.16**

The author strongly recommends the ultimate adoption of a communications standard based on the Internet Protocol for both the WAN and the HAN. As stated, the availability of tried and tested solutions is the primary driver for adoption, most critically in the cybersecurity area. The downside stated (bandwidth) is insignificant compared to the benefits. If mobile carrier networks are being considered, these are already carrying Internet Protocol traffic for, e.g. smartphones.

#### **3.1.4.7 Clause 4.24**

It is possible to augment authentication and security by use of public key cryptography and device certificates. These also serve to give a level of security to devices which are unable to have any form of user input.

### **3.1.5 Section 5**

#### **3.1.5.1 Clause 5.12**

Option 2 is more likely to succeed. This is the approach taken by the US Federal Government, whereby NIST does not create any standards but facilitates the choice of appropriate standards and encourages development by recognised industry bodies and SDOs

#### **3.1.5.2 Clause 5.18**

The author agrees with the choice of Option 2

#### **3.1.5.3 Clause 5.19**

The author recommends that existing developments internationally are considered first

#### **3.1.5.4 Clause 5.20**

The approach taken in the US has been very much driven by the utilities, although the regulation framework is considerably different in some states (e.g. California) than it is to the UK. This has met with some early criticism from potential third party service providers, which has led to modifications to the service provision model specified by various industry alliances.

### **3.1.6 Catalogue: Security and Privacy Requirements**

#### **3.1.6.1 Requirement SP.2**

Data at rest also needs to be considered with regard to confidentiality and integrity. Keys are mentioned later, but other data may need to be securely stored as well

#### **3.1.6.2 Requirement SP.5**

The certificate itself is not confidential, only the private key associated with it.

### **3.1.6.3 Requirement SP.10**

Rigorous independent testing – does this refer to penetration testing? If so, penetration testing is deliberately all but rigorous. It may be possible to introduce a ‘white hat’ programme for testing but in some respects the less this is managed, the better. Otherwise, the notion of rigorous testing for conformance is of course required

### **3.1.6.4 Requirement SP.11**

How is access control managed? If it can be managed remotely, a separate statement on the security of access control management needs to be in place

### **3.1.6.5 Requirement SP.12**

Whilst this refers to authorised devices connecting to the Smart Meter, it is also important to consider what those authorised devices may also be connected to. There is a strong requirement generally for third party service provision and it is possible that a single device could register with two Service Providers. In this case, a statement about appropriate authorisation within the device needs to be made

### **3.1.6.6 Requirement SP.13**

The narrative seems to be arbitrarily specific in solution. Network segmentation is but one way to achieve the requirement.

## **3.1.7 Catalogue: HAN Requirements**

### **3.1.7.1 Requirement HA.1**

Whilst it is important to consider European standards, the most prolific standards worldwide should be considered first, e.g. TCP/IP.

### **3.1.7.2 Requirement HA.2**

There may be a case for allowing public information to unauthorised devices on the HAN. Therefore the HAN should segregate security policy into network access and service provider registration.

### **3.1.7.3 Requirement HA.4**

The network topology is independent of network coordinator functionality. A mesh network will typically require some central coordination, especially when authentication is required.

### **3.1.7.4 Requirement HA.9**

It may make sense to extend the list to include bridges (i.e. across heterogeneous media), which may be an appropriate way to extend a HAN.

### **3.1.7.5 Requirement HA.10**

It may be necessary to consider non-repudiation for critical events, at least to the extent where a secure acknowledgement, along with local secure logging is performed.

### **3.1.7.6 Requirement HA.13**

The simplicity of the statement underlies the complexity this requirement introduces, especially with regard to multiple service provision. This should be highlighted.

### **3.1.7.7 Requirement HA.20**

Backwards compatibility can be achieved by a number of means, primarily:

1. Retirement
2. Upgrade
3. Proxy

Retirement may be appropriate for early generation IHDs based on the turnaround of consumer electronic goods in general (e.g. mobile phones).

Upgrade is essential and is clearly specified in the requirements.

Proxying is often overlooked as a method to provide backwards compatibility. It is a means where a simple device can proxy for one or more older devices and relay the functionality through translation. It is far from a perfect solution but is a solution nevertheless in cases where it is impossible to retire or upgrade an existing device.

### **3.1.7.8 Requirement HA.21**

It is not clear what is meant by 'multiple HANs'. The development should support a model whereby multiple networks can exist in the home and where it is possible for a device on one network to communicate at an application level with another device residing on a different network in the home. Limiting it to one HAN, i.e. physical network, is unnecessarily restrictive

### **3.1.7.9 Requirement HA.22**

It may be necessary for devices to work in conjunction with existing consumer networks. A consumer may not want to have to manage more than one network in the house.

### **3.1.7.10 General**

The HAN requirements do not go into much detail on bandwidth and latency requirements. It provides minima but these do not address potential future requirements.

## **3.1.8 General and Operational Services: Diagnostics**

It may be necessary to offload diagnostics more frequently than suggested to prevent overflow of diagnostic buffers in relatively resource constrained devices.

## **3.1.9 Appendix A3**

The impact of PEVs (plug-in electric vehicles) seems to be underestimated both in the respect on increase in demand on local grids and the use of their inherent storage for load balancing. This aspect is considered much more seriously in, e.g. California.

The US analysis of Smart Grid considers the interdependence of Smart Grid and Smart Metering is to be much closer than that suggested in this appendix.

## **3.2 Questions from Statement of Design Requirements**

### **3.2.1 Question 1**

*Should the HAN hardware be exchangeable without the need to exchange the meter?*

The author agrees with the current position that there is no requirement for the HAN hardware to be exchangeable without exchanging the meter. There are a number of concerns with this approach:

1. The additional bill of materials cost to add a connector and develop a separate HAN network interface controller (NIC)
2. The cost of having to actually physically change the HAN NIC in all the meters as this is an operation which cannot be undertaken by the consumer.

If the choice of underlying NIC is based on a well-known and well-established layer 2 standard for wireless and/or powerline (the two technologies most appropriate), then it should be possible to use additional converter devices within the premises should the information need to be relayed to alternative networks and devices in the premises. If a standard layer 3 technology is also used, this then becomes a relatively trivial routing function.

#### **3.2.1.1 Recommendations**

1. Use well-known MAC/PHY for layer 2 interface, e.g. 802.15.4
2. Use a well-known and standardised layer 3 technology, e.g. IPv6 (Internet Protocol v6)

### **3.2.2 Question 2**

*Are suitable HAN technologies available that meet the functional requirements?*

The author considers that there is a HAN technology available now which meets the functional requirements, i.e. ZigBee SEP 1.0 in conjunction with the ZigBee PRO stack. The author also recommends that the HAN technology be upgradeable to ZigBee SEP 2.0 in conjunction with the ZigBee IP stack when available.

#### **3.2.2.1 Recommendations**

1. Use ZigBee SEP 1.0/ZigBee PRO as initial technology for the first wave of rollouts
2. Upgrade to ZigBee SEP 2.0/ZigBee IP when available

### **3.2.3 Question 3**

*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?*

There is an assumption here that the WAN will be based on existing mobile carrier technology. Whilst the networks are well-established in the UK, they may not always be the most appropriate choice for WAN technology. Other technologies could be used which do not require the use of SIMs. It may be possible to consider a single network operator for the DCC or to set up some arrangement between service providers. There may indeed be a case for selecting the service provider with the most appropriate network in terms of performance for the vicinity. The increasing use of femtocells may also be appropriate in certain cases in areas where mobile carrier coverage is weak

#### **3.2.3.1 Recommendations**

None

### 3.2.4 Question 4

*Do you believe that the Catalogue is complete and at the required level of detail to develop the technical specification?*

The author believes the Catalogue is generally complete. It is lacking in certain areas such as privacy and security and HAN; these have been identified in 3.1.6 and 3.1.7. It is also likely to need to be extended as more use case studies are undertaken. The author bases these assumptions on similar activity in the US Smart Metering industry groups.

#### 3.2.4.1 Recommendations

1. Undertake more comprehensive use case analysis of consumer scenarios and meter/operator scenarios
2. Review security and privacy scenarios in more detail

### 3.2.5 Question 5

*Do you agree that the additional functionalities beyond the high-level list of functional requirements are justified on a cost benefit basis?*

The author agrees that the functional requirements in the Acceptable category (3.37) are justified and that the functional requirements in the Rejected category(3.38) are not justified.

#### 3.2.5.1 Recommendations

1. There needs to be firm guidelines on data collection and storage functionality to ensure devices are not required to have a large amount of local storage

### 3.2.6 Question 6

*Is there additional or new evidence that should cause those functional requirements that have been included or omitted to be further considered?*

The author is not aware of any such evidence.

#### 3.2.6.1 Recommendations

None

### 3.2.7 Question 7

*Do you agree that the proposed approach to developing technical specifications will deliver the necessary technical certainty and interoperability?*

The author agrees with the choice of Option 2 as the best way to facilitate development of interoperable technical specifications

#### 3.2.7.1 Recommendations

None

### 3.2.8 Question 8

*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?*

The author believes it is necessary to provide guidance and leadership. This must be completely impartial and not seen to be leading in any particular direction (for example, in the USA, there is some criticism of NIST not being totally impartial in their leadership). The suppliers will need to cooperate in the development of the DCC, which will be critical to the success of the programme.

#### **3.2.8.1 Recommendations**

None

#### **3.2.9 Question 9**

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

Having worked in this area for some considerable time, the author believes that there is a HAN solution implementable now which would be suitable for initial deployment and which is suitable for upgrade in the future as new requirements and functionality appear; see 3.2.2.

#### **3.2.9.1 Recommendations**

See 3.2.2.

#### **3.2.10 Question 10**

*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?*

Assuming basic technology and resource requirements for devices are specified, it is possible to phase the deployment based on existing technology solutions with the mandatory requirement that such a solution can be remotely upgraded. An existing technology solution (ZigBee SEP 1.0/ZigBee PRO stack) can be deployed now, based on widespread deployment in the US and can be upgraded in the future to an IP-based HAN (ZigBee SEP 2.0/ZigBee IP stack) to support true end-to-end connectivity using IP and enhanced service provision. ZigBee SEP 2.0 is an extension to ZigBee SEP 1.0 based on established standards used throughout the Internet (HTTP/XML).

#### **3.2.10.1 Recommendations**

See 3.2.2.



## 4 Prospectus general response

This section provides general opinions from the author in matters related to the Prospectus.

### 4.1 Need for network communications expertise

Metering companies have a long history of expertise in metrology but not necessarily in data communications. This is why SSN and GE have succeeded well in the US; SSN as comms. experts and GE as metrology experts. It is critically important to have the communications networking technical specifications developed by network communications experts.

It seems clear up to now the dominant contributors to this exercise are those involved primarily in the utility industry and their vendors.

### 4.2 Keep pace with the data communications

The data communications model is changing rapidly. Cloud computing and Web 2.0 may be buzzwords but they reflect the underlying trend in data communications, i.e. using the Internet to distribute data and provide access and management mechanisms to enable such distribution. Web services and APIs underpin all dynamism and interactive user experience provided by Google's applications such as Google Maps, Gmail etc. Similarly Amazon Web Services (AWS) provides such an infrastructure to enable cloud computing.

### 4.3 In-home display focus

Development must not be focussed around the IHD itself. The IHD should be considered as specific low cost device aimed at supplying information to households who have no other means to obtain the information. It is likely that households would opt to obtain the information through different mechanisms, e.g. smart phone app. or through an option on the television or by simply visiting a web site using a PC. Services are converging these days and the services offered by a television will soon be almost the same as the services offered by a smart phone and a PC. Each type of device will have its own specialisation still, e.g. PC as productivity tool, Smartphone as mobile communicator and television as passive entertainment system but all three overlap in terms of information delivery.

### 4.4 Layered stack approach to interoperability

The Smart Metering Design Group must place emphasis on a protocol stack analysis with regard to network and application interoperability.

#### 4.4.1 Layer 1

Layer 1 is the physical layer (PHY). In this respect, it refers to the medium the devices are going to communicate over. There are three logical choices for the medium:

- Wireless
- Powerline
- Wired

### 4.4.2 Layer 2

Layer 2 is the MAC (medium access control) layer. The MAC layer is often tied to the physical layer as the medium places requirements on how the MAC layer should work. The IEEE (Institute of Electrical and Electronic Engineers) has specified many standards in this area which are widely adopted, for example:

- Wireless: 802.15.4, 802.11
- Powerline: P1901.1
- Wired: 802.3

### 4.4.3 Layer 3

Layer 3 is the network layer. At this point, the communications stack becomes independent of the underlying layer 2/1 technologies, and this is referred to as an interface. The network layer is responsible for getting data from one network node to another, potentially via other network nodes through different interfaces. This is best known by the term 'routing'. By far the most prolific network layer is the Internet Protocol. One issue with the Internet Protocol as it stands is that the number of addresses it uses is now rapidly running out. To enable true end-to-end connectivity between all possible devices in the whole world, a new version called Internet Protocol v6 (IPv6) was developed with a much larger address space which would be inexhaustible.

### 4.4.4 Layer 4

Layer 4 is the transport layer and is concerned with delivery of data from one node to another, either reliably or unreliably, depending on what is required by the application. Again, by far the most prolific transport layers used are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), which offer reliable and unreliable transport respectively. These are used exclusively in conjunction with the Internet Protocol thus TCP/IP and UDP/IP are commonly used to describe these pairings.

### 4.4.5 Layers 5 to 7

Layers 5 to 7 are often combined generally to be the application layer, as the top of layer 4 is essentially where the communications stack ends. However, there are certain application technologies which are very prolific and are thus worth of a mention, for example, HTTP (HyperText Transfer Protocol) is the basis of the World Wide Web and SMTP (Simple Mail Transfer Protocol) is used widely for e-mail.

Therefore, technology choices for layers 1 to 4 are important.

### 4.4.6 Recommendations

The following protocols are recommended at the relevant layers

- Application
  - ZigBee SE 1.0 (initial deployment)
  - ZigBee SE 2.0 (upgraded deployment)
- Transport
  - ZigBee APS (initial deployment)

- TCP/UDP (upgraded deployment)
- Network
  - ZigBee NWK (initial deployment)
  - IPv6 (upgraded deployment)
- MAC/PHY
  - Powerline
    - Homeplug
  - Wireless
    - 802.15.4
    - 802.11n
  - Wired
    - Ethernet

## 4.5 HAN design approaches

There are generally two approaches to the HAN:

1. Consider it a closed system which can interface to other systems via a gateway
2. Enable end-to-end connectivity to any device on the HAN

Both approaches have their advantages and disadvantages. In general, it would be desirable to have (2), however this offers considerable challenges, most notably in the area of cybersecurity. The advantage of (1) is that a HAN can be tailored specifically to service the type of devices expected on it. Thus if they are low power, low data rate devices, it is easier to design a bespoke communications stack to deliver the required communications infrastructure. This was the approach taken for ZigBee SE 1.0

## 4.6 Why ZigBee?

This has been developed extensively by vendors and utilities in the US. Some of the utilities involved operate in a deregulated market similar to the UK, e.g. Texas has a deregulated energy market.

### 4.6.1 History behind ZigBee Smart Energy Profile (SEP) 1.0

The ZigBee Alliance spent some time developing a bespoke communications stack all the way to the application layer but based on standard layer 2/1 technology (i.e. 802.15.4). This was initially targeted at home automation devices but also aimed at commercial buildings and subsequently medical and telecommunications applications. The stack was fully layered according to the ISO model up to layer 4. The primary reason for this approach was the resource constraints present in first and second generation devices which supported an 802.15.4 radio. Some of these devices also have a general purpose microcontroller built into them, thus offering the possibility of a very cheap but sophisticated device. However, these devices have very limited space for code and data.

Nevertheless, the sophistication and price point proved very interesting to a number of utilities and meter manufacturers in the USA, who invested a lot of time and effort to develop and application layer appropriate to their needs based on the ZigBee PRO communications stack. This led to the development of the ZigBee SEP 1.0 standard in a very short time frame and subsequent development and deployment by utilities and vendors in many states in the USA, most notably California, Florida and Texas.

#### **4.6.2 The need for ZigBee SEP 2.0 and ZigBee IP**

The Smart Grid market started to rapidly develop towards the end of 2008 and it became clear that much of the work done in ZigBee SEP 1.0 would be applicable going forward as the metering systems extended their roles into the Smart Grid, especially in areas like renewable energy and electric vehicle integration. However, the considerations for the communication network now expanded well beyond the HAN and thus there was a rethink on what would be appropriate. One of the main perceived issues with the ZigBee communications stack is that it was too proprietary, having been developed by a relatively small group in a membership-based Alliance, although it was still considered an open standard in the respect that there were no barriers to access. For this reason, it became important to consider the most prolific technologies which would transcend the networks being considered in the Smart Grid. That technology was fundamentally IPv6.

ZigBee still had a clear market leadership, so the aim was to develop the next generation of ZigBee based on open standards managed in true SDOs like the IEEE, the IETF or W3C. This is currently being undertaken in both the communication stack and the application protocol and interoperability testing is taking place now in conjunction with the development. It is hoped that the specification will be complete in early 2011, with products following closely behind