Ember reponses to Ofgem prospectus questions

[redacted]

28 October 2010

1. Introduction

Ember Corporation is a Promoter member of the ZigBee Alliance, a vendor of ZigBee/IEEE 802.15.4 chipsets and ZigBee networking stacks, and a technology leader in smart metering HAN communications. While ZigBee wireless mesh networking technology using Ember chipsets have been used in smart metering WANs, for example the installation in Gothenborg, Sweden, we accept that GB smart metering is going down a different path for the WAN communications, so our responses to the questions in these documents will focus on those questions that hit on HAN communications in particular.

We are not experts on gas or electric energy markets, or on the design of smart meters, except for the communications piece, so there are many questions where we simply cannot have a view based on our expertise or experience. We have not included these questions in our response.

In answering the questions posed, we thought that it might be useful to be brief in our answers and include more detailed information in appendices for readers to refer to later. Some of these are directly relevant to the questions asked, around security and positioning of IHD in the consumer's home, while others are more indirectly linked to discussions of regulatory questions.

These appendices are self-contained and we feel they are a useful reference for discussion on some of the key topics related to HAN communications. They will no doubt be discussed during HAN workshops.

Appendix A: How ZigBee deals with Security Concerns
Appendix B: ZigBee Propagation in UK homes
Appendix C: ZigBee in Europe
Appendix D: ZigBee as an Open Standard

The remainder of this paper is direct responses to those documents that required responses by 28th October 2010 (those others have already been responded to on 28th September).

(2) Consumer Protection
(3) Data Privacy and Security
(4) In-Home Display
(5) Communications Business Model
(6) Non-Domestic Sector
(7) Regulatory and Commercial Framework

2. Consumer Protection

2.1 Developing Services for Customers

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

Ember does not really have a view on this, but personally I agree that it is important to address unwelcome sales activities.

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

Whatever the consumer is comfortable with, but certainly not as a selling opportunity.

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

We agree that it is important to ensure that the IHD is not used to transmit unwelcome marketing messages, not least because it diminishes the correct use of the IHD and potentially could lead to it being disconnected by the consumer. Some messages about new products and services related to energy management may be useful to the consumer however.

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

We agree that consumers should be able to obtain consumption information free of charge by communicating with their smart meters or the smart metering WAN/HAN gateway, and that this should be secured appropriately and only available via authorised devices on the HAN.

2.2 Prepayment and Remote Disconnection

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

IF all IHDs supplied had as minimum functionality the prepayment functionality, then customers could easily be switched to prepayment remotely, without a visit. However, this functionality is not specified as a minimum functionality and it might increase the cost of a minimum spec IHD, as you may need a keypad or touch screen or a facility to swipe a card, even a USB interface could add to the cost of the IHD. So, it seems that switching to prepayment is likely to require a replacement of some in-home equipment, if not the meter, then perhaps the IHD, unless prepayment functionality is included in the minimum functionality for all IHDs. If this is included it would make it much easier to switch any customer to prepayment.

2.3 Cost Recovery and Monitoring of Costs

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

We suggest that any up front cost may be a barrier to the consumer accepting the IHD, however it may be useful to give the consumer the choice.

3. Data Privacy and Security

3.1 Data Privacy

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

We broadly agree with the approach.

Question 3: *Do you support the proposal to develop a privacy charter?*

We support this, however we question if it is necessary. What is required is to simply explain to the consumer, how he/she is protected by existing privacy legislation and how smart metering adheres to this. We are not sure that this requires a charter.

3.2 Smart Metering System Security

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

We agree with the approach.

In reference to (4.2), we would recommend you include some security specialists from low power wireless mesh networking background to advise on HAN security. Meter manufacturers have exposure to this area and most of the larger UK meter manufacturers have a heavy involvement with ZigBee, but they may not have sufficiently deep technical background in ZigBee security, and broader industry security experts may not have expertise in low power wireless mesh networking like ZigBee.

We believe that ZigBee Smart Energy is a strong candidate to be the communications standard of choice for GB smart metering HAN communications, so we would like to point out that a lot of work has already been done on security for ZigBee Smart Energy to satisfy the needs of US utilities and NIST in particular. Security is something that you have to come back to time and time again to stay ahead, so we feel that it is as important that any communications standard has good processes and a good track record for dealing with security issues. Since 2008 in particular, ZigBee security has been scrutinised by independent studies such as those at Carnegie Mellon University, as well as professional hackers and writers on the subject (e.g. Black Hat conferences). The ZigBee Alliance has learnt from this experience and has modified security features over time to close any gaps that have been exposed, while ZigBee technology vendors have also addressed implementation concerns raised that have nothing to do with the standard itself. Appendix A deals with some of the issues and concerns that GB smart metering may have in relation to HAN communications and shows how ZigBee deals with these issues.

4. In-Home Display

4.1 Functional Requirements of the IHD

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

Comments we have on the real-time nature of data displayed on the IHD are adequately covered by 2.28-2.32 in the document. We would add that constraints on the frequency of communications are typically (for ZigBee anyway) flexible, but depend on trade-offs between frequency and traffic on the network or battery life. For instance there is no technical reason why the turnaround time of a request for data from IHD to an electric meter shouldn't be less than say 100 milliseconds, however allowing an IHD to continuously poll an electric meter for real-time data every 100 milliseconds would create excessive data on the network and cause latency issues with other communications e.g. to smart appliances. The timescales indicated in the document are acceptable.

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

We have no expertise in the area of consumer behavioural change, however we do have some comments on IHD portability, in particular with regard to 2.48, positioning of the IHD and signal strength.

As the smart metering HAN grows to include other devices in the future, such as smart plugs, smart appliances, perhaps lights or security systems (e.g. occupancy sensors to advise heating systems to come on or off), ZigBee's mesh networking technology can make use of that to create a very robust network in the home and complete coverage for all homes, regardless of where the IHD is placed.

In the interim, however, we recognise that the HAN will consist of up to 3 devices located close to one another (gateway/ESI, Electric Meter and Gas Meter), and a 4th device located further away, somewhere in the home, the IHD, and that this configuration puts an emphasis on simple point-to-point or 1-hop communications.

For ALL wireless communications this is a challenge, because there are 2 barriers to good communications; range/propagation and blockages, and all short range radio frequencies can be blocked by an unfortunately placed and large enough metal object (e.g. skip, fridge, range cooker etc.). While we are aware of concerns over the 2.4GHz frequency adopted by ZigBee Smart Energy, in particular related to propagation of the signal in GB homes, we are confident that 1-hop communications from the gateway/ESI or meter to the IHD placed wherever the consumer wishes it to be located, in a high percentage of GB homes will work without a problem. We suggest that in some percentage of homes, there will always be a need in the HAN for either a repeater (which might be some useful device like a smart appliance or smart plug), or an alternative communications medium (e.g. HomePlug). This requirement exists regardless of wireless technology selected.

An independent study by University of Sheffield will be published next year and will be a useful tool for advising planners and installers on the sort of homes and configurations that will require more than single hop ZigBee communications.

Appendix B deals with this issue in more detail.

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

We think there may be some functions missing from the minimum set of functionality;
* Ability to receive secure firmware upgrades over the air via the HAN communications. This is a standard feature of ZigBee Smart Energy 1.1 devices.
* Ability to receive a short text message from the energy supplier or utility and display it (this is a standard feature supported by ZigBee Smart Energy). Perhaps this is a feature for enhanced IHDs or future basic IHDs.

Other comments;
* (2.27) Both received signal strength (RSSI) and LQI is available with ZigBee, however we recommend that some simple mechanism of red/amber/green or bars is used to indicate signal strength, something that consumers can instictively understand. This is probably a matter of innovation among manufacturers of IHDs rather than something to be specified.

4.2 Nature of the mandate on suppliers in relation to the IHD

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

We cannot see how innovation could be hampered by the set of minimum requirements outlined.

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

Whatever about role and obligations, we agree that IHDs are better coming from suppliers, as it allows them the opportunity to innovate and differentiate. We feel that a single bland low-cost IHD coming from DCC is likely to be uninspiring to the consumer, and end up in a drawer. It would be difficult to see how suppliers could continue to be responsible for IHDs in a consumers home after some time has elapsed (one year as suggested, seems reasonable), as these consumers may move to a new supplier, or may be a dual fuel customer. We think that the process of moving supplier could be a good time for the new supplier to offer a new IHD with its own branding etc., and that otherwise there could be an open market for IHDs so that consumers can purchase new ones, either from suppliers or elsewhere. In situations where the display gets more than standard use, e.g. prepayment (3.22), we agree that it may make sense for the energy supplier to maintain the IHD.

Regarding 3.11, we feel that if there is a well-designed, secure installation process, there is no reason why IHDs could not be posted to consumers who already have smart meters installed. Indeed we feel that we should plan for appropriately certified IHDs to be ultimately available to consumers from sources other than suppliers. ZigBee Smart Energy supports such a secure installation process as outlined in Appendix A, and as designed already for US deployments of displays and other devices.

5. Communications Business Model

5.1 Structure and Realisation of DCC

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

From the view of the HAN, and the DCC provsion of a WAN/HAN gateway, we suggest that the quickest and most cost-effective way to provide a HAN interface is to choose a single GB HAN standard that is already used in smart metering and has most of the functionality required for GB smart metering. For instance, choosing to allow the market to decide on HAN technologies and standards would mean that the gateway provided by the DCC would need to support multiple HAN technologies, or at least allow for expansion to support multiple HAN technologies, which will add to the cost, and will make the implementation more complex, especially with regard to end to end security and communications through the WAN and HAN. It would also make the change of supplier more difficult.

We suggest that ZigBee Smart Energy is the best available fit for the GB HAN, because it is already designed with most of the current and future features required by GB smart metering (with the rest being worked on by primarily UK-based ZigBee Alliance members) and is specified for the HAN in a number of countries including US and Australia. Appendix C deals with the popularity of ZigBee in Europe in particular.

6. Non-Domestic Sector

6.1 Use of DCC to communicate with meters in the smaller non-domestic sector

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

The question of interoperability is posed here with regard to the WAN communications only, so on that basis we have no view.

6.2 Other issues related to non-domestic customers

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

In the case of non-domestic customers, IHD may not be necessary, and provision of e.g. USB dongle to give access to smart meters from a PC may deliver what the customer requires. In the non-domestic sector other devices in the smart metering HAN may make a lot more sense in the short term than in domestic cases, e.g. smart plugs or similar to identify and manage the high usage appliances in a workshop.

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

Yes.

7. Regulatory and Commercial Framework

7.1 Smart metering regulatory regime

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

The list appears to be complete, assuming technical interoperability includes the HAN and any certification required for HAN devices.

7.2 Roles and responsibilities at customer premises

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

It is unclear if the ability to display a message from the utility should be a minimum requirement for the display, but it is worth discussing.

For functionality accessible from a computer (4.14) we suggest that the device connected to the computer (probably a USB stick with a HAN communications module built in) should act like an in-home display in terms of security, authorisation on the HAN and functionality and information available.

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

We consider that shared infrastructure makes most sense, especially when one or other supplier is switched later by the consumer.

7.3 Other regulatory and commercial issues

Question 9: *What is needed to help ensure commercial interoperability?*

With regard to the HAN, commercial interoperability requires first technical interoperability, that requires not just that the same HAN communications are used, but that the same application messages and security mechanisms are used by all suppliers, OR that the HAN can support multiple HAN communications technologies (which would be much more expensive, especially for the WAN/HAN gateway).

We recommend that a single HAN communications standard and technology is selected for GB smart metering and recommend that ZigBee Smart Energy is the best fit for the requirements of GB smart metering.

7.4 Impact on wider industry process

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

We anticipate the introduction to the market of numerous home products such as smart appliances and LED lighting with ZigBee communications built in, to communicate with ZigBee Smart Energy HANs, and make use of features like demand response and TOU tariffs. Primarily because of the US market's adoption of ZigBee Smart Energy, we expect to see products from several top manufacturers on the market in the next couple of years. We suggest that it is important for the HAN communications standard chosen by GB smart metering to be capable of connection to these future products, and it is important to point out that many proprietary and even standard technologies currently used for smart metering in Europe are unlikely to ever be commercially interesting to appliance and other home automation manufacturers in the way that ZigBee is already. We refer to the recent study by the Association of Home Appliance Manufacturers (AHAM) (http://www.mwjournal.com/News/article.asp?HH_ID=AR_9842) which looks at various technologies and scores ZigBee very highly.

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

With regard to HAN communications, ZigBee already has a strong, proven certification process in place for ZigBee Smart Energy products to ensure interoperability of devices. This process includes 3 test organisations capable of testing ZigBee products, including one located in the UK, Trac Global in Hull. This mature process could be adopted in full by GB smart metering for HAN products, including the appointment of more UK-based test houses, or incorporated into a larger GB smart metering certification process managed by e.g. Ofgem.

Appendix A: How ZigBee deals with security concerns

There are two types of concerns that could be raised about ZigBee or any other communications solutions in smart metering;

a) Concerns about the protocol and specifications
b) Concerns around specific implementations by particular platform vendors, e.g. random number generation mechanisms that are nothing to do with the ZigBee specification itself.

These concerns are applicable to either ZigBee Smart Energy 1.1 or ZigBee Smart Energy 2.0.

ZigBee had an independent security audit by Carnegie Mellon University in 2008, which was generally positive and revealed "no major security vulnerabilities in the high-level construction of the SE protocol". In broad terms the main points were;

- There were some questions around the use of install codes.
- The use of ECC in security was taken to be strong

ZigBee has used this audit as a planning tool and has been working on the issues raised. It is important to be realistic when reviewing security issues, as it is always possible to find issues; the main thing is to strive for excellence and be flexible and open to change and to making improvements.

The whole security question is a combination of the strength of the encryption and authentication process as well as the implementation process. In general if you put a device in a home, you have to assume that it will be broken into; you can make it more difficult for a hacker, but the device can always be physically opened and hacked. The real issue is to make sure that in breaking into one device the hacker cannot do any harm to the network or system.

Key Areas for discussion

a. Security of OTA firmware upgrades
b. Poor implementation of random number generator
c. Device authentication on the network.
d. Installation process and the number of organisations that need to know keys
e. Two way communications with In-home display
f. Multiple ESI
g. Proprietary vs Standard Security Mechanisms

(a) Security of Over-the-air firmware upgrade

In 2009 at the BlackHat security conference Mike Davis from IOActive published a paper on exploiting meter networks by injecting malware or unintended software to take control of the meter (see http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html#MDavis). He demonstrated using the meters own bootloader for upgrading software to upgraded this unintended software. Their review indicated similar weaknesses existing with many of the meter suppliers. (Note that this was presented without naming specific meter vendors and was a warning to improve our processes and protocols.)

The root of this issue was an over the air upgrade mechanism that did not have proper security mechanisms or review. The bootloader in process was a vendor proprietary mechanism and not standards based. ZigBee was in the process of developing a standards based upgrading mechanism that would include industry recommended security protocols.

ZigBee followed the normal specification development process which included approval of a Marketing Requirements Document to define the use cases and requirements for the feature. From this a Technical Requirements Document was developed and ultimately an over the air bootloader specification. As of October 2010 this bootloader mechanism has been interoperability tested among a number of ZigBee companies and is ready for certification. This bootloader includes a number of security features to prevent the loading of unintended code on devices that were recommended from the utility industry and security consultants, as well as mechanisms used for protecting code updates in other industries. These include:

- Using digitally signed images for software updates and only when the signature of the image is validated can the new code then be installed.
- Using Application Level Encryption to ensure the integrity of the upgrading process.
- Using manufacturers certificates to sign software images so devices in the field can validate that a new image came from a trusted source.
- An external review of the over the air bootloading mechanism is being completed now by the ZigBee Alliance.

This development of the new standards based bootloader is an example of how the ZigBee Alliance takes feedback from industry and members and responds with updates to the specification. This feedback and correction mechanism is critically important in an area such as security where ongoing threat analysis and attacks result in newly discovered weaknesses. Only by being vigilant to these new threats and developing new defenses can modern systems be protected.

(b) Poor Implementation of Random Number Generator

Also in 2009, security researcher Travis Goodspeed published a report on a particular weakness of a ZigBee implementation due to a weakness of the random number generator on the platform (see http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html#Goodspeed). Because there was not sufficient randomness, only a small subset of possible keys were being used, making the system much easier to attack.

When this was published, the ZigBee Smart Energy team investigated the problem and developed a plan of action to address improvements. These include the following:

- The implementation in question was patched by the supplier with a software fix resulting in proper operation.
- The ZigBee stack test procedures were revised to include a test of the random number generator to find implementation problems such as this during certification of the product.
- Other ZigBee suppliers were asked to verify their implementation of this function.
- ZigBee suppliers have also addressed other issues raised by this paper, and these were not related directly to the ZigBee specifications.

This is another example of where the ZigBee Alliance can react to identify the problem and not only implement an upgrade for the particular implementation but new tests can be instituted to ensure other devices do not have the same problem.

(c) Authentication of devices on the network

There have been question as to the behavior and vulnerabilities of the ZigBee network during the joining process. The joining process is a multi-step process that involves the following:

- The gateway device for the HAN must be notified that a device will be joining and the specific identification of the expected device is provided to the gateway. This is done in an out of band mechanism where this information is provided through a web portal, on the phone or through the store where the device was purchased.
- The gateway turns on permit joining for the network for a defined time period to allow devices to join the network.
- The new device joins the network and is only provisionally authorized. The device is not allowed to send messages into the network except for security messages required for authorization.
- The device then completed a certificate based key exchange mechanism to validate its identify and security credentials. Once this is completed the device can now participate in the network.

This process is similar to what is done with cable-modems and similar systems. The adjacent device can police messages from a newly joined device and not allow messages to other devices – the only thing allowed at this stage is security exchange protocol. It is not possible to attack the network with a repeated join, a simple RF interferer would be much more effective.

(d) Vulnerability of keys due to number of organisations that need to know them

In the UK metering infrastructure, a number organisations might need to know the keys to be used in the smart metering HAN;

- meter operators
- suppliers
- manufacturers
- DCC

And they also need to know how certified modules need to be installed.

In ZigBee Smart Energy, each device has a certificate that is tied to its MAC address. Manufacturers will have a set of certificates. The actual person installing the meter or the IHD (In Home Display) does not need to know what the certificate is – it is buried in the memory of the device. The Certification Authority knows the certificate, but it is trusted. Any given device can be cracked, but it cannot do harm to the rest of the system.

A lot depends on the infrastructure the utility (or DCC) puts in place. Someone needs to tell the hub/gateway (in ZigBee terms the ESI, Energy Services Interface) which device will be joining the network – usually through the backhaul network of the utility (/DCC). Certificates can be checked and controlled at the time of joining.

When an IHD goes to negotiate with the ESI (in the US this functionality is in the electric meter), US utilities say someone needs to tell them, what that device is before they allow it to connect. You expect ‘this’ device to join – then that device is allowed on. In US, you can log in to the portal, maybe even in the store (enrollment), so ultimately the meter knows that device is coming to join it.

(e) Vulnerability resulting from two-way communications with the IHD

It might be claimed that as the IHD uses 2-way comms with the ESI (in the US, this is the electric meter), this may make the network vulnerable given you could buy IHD from anywhere.

But;
- The IHD has limited comms with ESI/meter, it is not a pass-through communication – it does not get to the backhaul network.
- There is a carefully defined set of messages for the IHD, e.g. demand response and rogue messages would be ignored by the ESI.
- The ESI is effectively a firewall between the HAN and the backhaul network.
- There is process of enrollment of the device in the network.
- Only certain controlled messages are passed through.

(f) Managing multiple ESI (gateways)

There might be a concern that the use of multiple ESI or gateways into the network will present security vulnerability.

In the US systems it is expected that multi-ESI systems will be a common configuration. The normal expected configuration is an electric meter with the utility communications system and a broadband connection using the homeowners network systems.

Under such a system it may be that devices register with the meter for utility specific information such as retailer pricing or demand response messages and registers with the broadband connection for software upgrades or more complex home energy management services. It may also be that utility messages on demand response travel through both connection points but the Event ID is used by the local device to recognize it has received two requests for the same event.

In any of these scenarios, the devices involved on the network must have completed the security authorization process and are limited in the messages they can send and receive based on their authorizations. So, for example, an in home display may be authorized to read consumption data from the meter and respond to demand response events. However, it does not have authorization to reset consumption data on the meter, nor can it send demand response events to other devices (since it is a receiver of these events and not a creator of the event).

The ESI's themselves will likely have little communication with each other under these scenarios. Their data and information is based on their own communications backhaul system and they typically are not using the other ESI as a backup communication path.

Which ESI is the trust center?

Under a multi-ESI system, it is necessary to determine which of the ESI's acts as the trust center to provide security credentials for the network. It is a requirement that there be such a device and that the device be unique within the network for controlling access.

This is resolved in SE 1.x because the trust center must be started when the network is initiated and that device communicates to other devices as they join and conduct the authorization process. So each new joining device queries a parent that allows it to join, and it initiates authorization for the device with the trust center. In this manner, each new device learns the address of the trust center in the network. This trust center can be replaced as part of Smart Energy 1.1 but then the new trust center contacts each device and reestablished security credentials to validate that it is the new trust center. A new ESI joining a network would therefore use the existing trust center in the network and not initiate a new trust center.

(g) Proprietary versus Standard Security Methods

There have been reviews and attacks on the ZigBee security methodology and some suggest that proprietary solutions are more secure.

However, we need to consider the reasons for security attacks and the best means to thwart such attacks. In general, security attacks become problematic when there is a large enough target and when there is some real incentive (for example economic) for attacks to be replicated by a large group. So one example would be early satellite cable TV services. A virtual cottage industry grew up around finding, exploiting and selling hacks to these systems to allow people to get premium channels without paying the subscription. The early systems were simple to break, and an escalating set of improvements by the suppliers and new tricks by the hackers played out over several years (see http://www.usatoday.com/news/acovmon.htm for a discussion on some of this).

What a standards based security system provides is assurance that best practices have been used, reviewed, tested and validated. A standards-based process also provides mechanisms to collect, analyze and resolve security weaknesses as they are uncovered allowing the system to improve over time. While a dedicated sophisticated attack may succeed, the resources and time required make it impractical or not cost effective for the average person. If the cost of thwarting the security is more than the potential savings, such widespread attacks become less common.

Many of the mechanisms used by standards based security solutions can be used by proprietary systems. However, too often, proprietary systems have chosen security through obscurity and assumed that private methods would be suitable because hackers would not know what they are. In reality, these solutions do not typically have the rigorous peer and industry review needed to ensure robust protection.

Any widespread rollout of devices in the UK would clearly represent a large target of devices to be attacked and the most robust and defensible security mechanisms should be put in place.

Appendix B: ZigBee Propagation in UK homes

In Europe, one of the most frequent criticisms heard about ZigBee is that its primary target frequency (the only one with standard products and widespread deployments) is 2.4GHz, and that this poses a problem for coexistence with WiFi and propagation in buildings, with many recommending 868MHz instead. A report by Schneider Electric (2008, available at: http://www.zigbee.org/LearnMore/WhitePapers.aspx) helped to successfully dispel the issue of WiFi coexistence, however there is not a comprehensive study of propagation in homes for Europe.

In the US, tests conducted by Southern California Edison (2008, available from: http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=15571) showed that 94% of their customers' homes could be covered by a ZigBee 2.4GHz signal. These tests are not relevant in Europe for 2 reasons;

- The size of homes and building materials used in the US is very different from Europe, and the UK in particular; and
- Most importantly, the permitted maximum transmit power for IEEE 802.15.4 2.4GHz radios according to FCC in the US is 100mW (+20dBm), while the permitted maximum in Europe according to ETSI EN 300 328 is 10mW (+10dBm), a difference that could represent 3x-4x the range in free space.

Why 2.4GHz?

IEEE 802.15.4 actually includes 3 different frequencies;
- 868–868.6 MHz (e.g., Europe),
- 902–928 MHz (e.g., North America) or
- 2400–2483.5 MHz (worldwide)

All of these bands are licence free, which means that they can be used by any applications. There are a few reasons why ZigBee, and in particular ZigBee Smart Energy has not typically been implemented at 868MHz;

- **Global:** 868MHz is not used in the US or many parts of Asia, which is not necessarily an issue for strict smart metering programmes, but it does matter if you want to also attract white goods manufacturers to make products, or lighting manufacturers, because they will want a global market to address. 2.4GHz is available globally.
- **Bandwidth:** The raw data rate for ZigBee/IEEE 802.15.4 at 2.4GHz is 250kbps (kilo bits per second), while the raw data rate at 868MHz is only 20kbps, 12.5 times less bandwidth. This is accentuated when you realise that the best real data throughput that can be achieved with ZigBee is about 50kbps (because of headers, acknowledgements, retransmissions etc.), which means the best you can do at 868MHz is about 4kbps real data throughput. Even if the actual data transfer requirements of the application are low, this means that adding security mechanisms causes problems, over-the-air upgrades are 12 times slower, networks cannot easily scale, etc.
- **Interference avoidance:** While much is said about interference at 2.4GHz, actually the greater risk is arguably at 868MHz, where there is only one channel operating and available, compared to 16 channels available at 2.4GHz. So, while it is arguable that there are more potential interferers at 2.4GHz, if you have an interferer and it impacts network performance you just move to another channel, whereas at 868MHz there is no other channel to go to.

So, the ONLY possible concern with 2.4GHz is point-to-point range, which will never be quite as good as 868MHz indoors, but everything else points to 2.4GHz, so as long as the propagation of 2.4GHz is acceptable, it should be used.

ZigBee and mesh networking

It is important to understand that ZigBee is not a simple point-to-point radio protocol, so it does not rely entirely on the ability of 2 nodes to communicate directly with one another; rather they can communicate by hopping messages through a mesh network of ZigBee nodes. In fact, in a ZigBee mesh network, the more nodes you have in the network the stronger and more robust the communications is. This is a key reason why ZigBee is deployed in such a variety of applications and networks, from Raymarine LifeTag devices to raise an alarm when someone on a boat goes overboard, to home automation, industrial control, smart metering HANs and even smart metering NAN/WAN like Gotheborg.

Nonetheless it is accepted that in early smart metering HAN deployments, the number of devices in a network will be low, so the opportunity to make use of relaying of messages is limited, so an understanding of point-to-point range or propagation is important.

OnStream / E.ON propagation tests

The only published UK report that I am aware of on ZigBee propagation is "ZigBee Carrier Frequency Tests for UK Smart Metering Infrastructure", a report produced as input to the ERA SRSM Local Communications Forum by Eric Beattie, OnStream and Kevin Clayton, E.ON in March 2008. This report is available on the SRSM local commss blog site at: http://srsmlocalcomms.wetpaint.com/page/UK+Field+Test+for+Frequency+Comparison.

This report indicated that 868MHz radios performed better than 2.4GHz radios in all cases in UK homes, and that in 10 out of 30 use cases tested (different home types/locations), communications was not successful at 2.4GHz. These tests showed that in 3 out of 6 of the building types (stone cottage, semi-detached house and first floor flat), a 2.4GHz signal could be obtained from the meter to all 5 rooms tested (kitchen, lounge 1, lounge 2, hallway, bedroom), and that 2.4GHz did not work at all in tests in a detached 2-storey house with extension.

Location	Kitchen		Lounge 1		Lounge 2		Hallway		Bedroom	
	2.4G	868M	2.4G	868M	2.4G	868M	2.4G	868M	2.4G	868M
Stone cottage	35	125	85	155	70	150	50	140	50	140
Semi-detached	85	110	16	110	80	110	90	200	25	150
Detached Bungalow .	0	75	40	170	55	115	115	190	35	160
Detached two story	0	20	0	50	0	50	0	30	15	80
Detached two story with extension	0	45	0	60	0	50	0	60	0	25
First floor flat	25	150	35	155	45	115	35	135	35	155

(Beattie & Clayton, 2008) – 0-255 indicates strength of signal, 0 = no signal

The report conceded that;

> *"It is possible to add a power amp to the 2.4GHz radio and increase its output power to 10mW. This would increase the range of 2.4GHz radio to about the same as the 868MHz radio, but would use more energy, affect battery life, and may cause interference."*
>
> (Beattie & Clayton, 2008)

At the time of the report's publication to the SRSM Local Comms Forum, I criticised some of the assumptions and test conditions of the report, especially;

- Not transmitting at the legally permitted limit for IEEE 802.15.4 2.4GHz radios unfairly skewed the tests; and
- Not using leading ZigBee radios in the tests, preferring 'older technology' platform, also skewed the tests, as the leading radios have much better receive sensitivity, which improves propagation also.

Technology selection may have impacted the link budget in these tests by as much as 10-13dBm, which can mean 3-4 times the range in free space (less predictable in a building).

Furthermore, some of the assumptions about transmitting at higher power should also be challenged. Some ZigBee radios (e.g. Ember EM357) can transmit at close to the legal limit without the use of an external power amplifier therefore with almost no impact on energy consumption, so battery life is not an issue, and certainly no impact on cost.

Anecdotal evidence

A number of leading companies have conducted their own tests of ZigBee propagation at 2.4GHz and have concluded that it was acceptable for their home automation products; Philips, Schneider Electric and LeGrand for example. Typically tests carried out by commercial companies do not get published, however LeGrand in its Arteor documentation suggests that a distance of 15m through 1 reinforced concrete wall is possible between its ZigBee devices (which are not operating at maximum transmit power).

In the UK, Alertme reported to the SRSM Local Comms Forum that in 80% of houses they installed their ZigBee security system in, a repeater was not necessary, and they do not make use of the maximum legal transmit power.

University of Sheffield study – work in progress

The Communications Group within the University of Sheffield, under Professor Richard Langley, is currently carrying out a study and set of tests using ZigBee at 2.4GHz in multiple building types, and we expect that this report will be completed and published in the next year. The radios involved are Ember EM357, which represent the leading ZigBee chip used in UK meter designs today, and can transmit up to 8.5dBm. This is at a very early stage of defining the tests and making initial measurements without any special antennae or tuning, just a simple ceramic PCB antenna, however so far it appears that communications through one floor and 2 rooms works consistently.

Facing up to the reality of wireless propagation

Different radio frequencies have properties that are dictated by the laws of physics and cannot be denied, and 868MHz (all sub-1GHz frequencies) will propagate better in buildings than 2.4GHz. However, all radio signals can be blocked by certain materials in walls or fixtures, e.g. by metal cookers or fridges, so no matter what radio frequency chosen for communications in a HAN, it can fail.

The issue of propagation with ZigBee is one of percentages – what percentage of the housing stock requires either a ZigBee repeater or some other communications solution?

According to the 2001 census of England and Wales, the breakdown of house type is as follows;

- Semi-detached house: 31.57%
- Terraced house: 25.84%
- Detached house: 22.51%
- Various types of flats: 19.66%

(Office for National Statistics, available for download at: http://neighbourhood.statistics.gov.uk/dissemination/filesetSelection.do?step=5&datasetFamilyId=49&instanceSelection=125&filesetIndex=8&Next.x=9&Next.y=4&rightPaneBoxHeight=501&JSAllowed=true&browserHeight=691&browserWidth=1440&%24ph=60_61_64&CurrentPageId=64)

The University of Sheffield report should help advise on which building types are vulnerable and which installation cases require a special installation. The OnStream/E.ON report from 2008, flawed as it is, indicates that a worst-case scenario is that homes that will not work with point-to-point 2.4GHz ZigBee could be somewhere between 17% (1 in 6 homes) and 33% (10 in 30 use cases). Assuming the tests done by Beattie & Clayton (2008) were representative (we are fairly sure that the sample was not representative), we could conclude that detached houses being the biggest problem, and cross-referencing with the 2001 census, this could be up to 22.51% failures. We know it will be better than that if we use better radios at higher transmit power, and that different building materials within house categories will also have an impact. Ultimately the University of Sheffield study will help the planning process here.

Summary

It is clear that regardless of what wireless technology is used in the smart metering HAN, some percentage of GB homes will require repeaters to propagate a point-to-point message from a smart meter to an in-home display placed somewhere in the home. This percentage is impacted not just by the radio frequency used for the HAN, but also by building materials, mix of house types, positioning of meters and gateway/hub and where consumers will place the in home display. An ongoing study at University of Sheffield will inform a calculation of this percentage for ZigBee at 2.4GHz, however it is likely that the difference between different radio frequencies is perhaps the difference between 80% success and 90% success without repeaters, not the difference between the overall success or failure of ZigBee Smart Energy at 2.4GHz. In any case, there is always a requirement for an alternative solution where a direct signal is not possible between a hub, gateway or meter, and an in-home display.

As the smart metering HAN evolves into more than just an in-home display however, the ZigBee mesh network strengthens, and the addition of heating boilers, home appliances, smart plugs, security systems, lights etc., can make the network more and more robust, depending on some ownership and architectural choices to be made by consumers/Ofgem/suppliers.

Appendix C: ZigBee in Europe

ZigBee popularity in the market

ZigBee is an emerging standard, and as such it is disruptive to the market. Other wireless and wired technologies have promised to revolutionise sensor networks and expand the Internet of Things, but so far have failed. Many of them have either been proprietary in nature, and therefore never gained momentum, or have been open but too academic to be truly usable in the market. ZigBee is an open standard that is grounded in real business values and a pragmatic approach, and it has a chance.

Even as an emerging standard that has had its initial successes mainly in the USA, ZigBee has already been adopted strongly around Europe by some very large electronics manufacturers and also by some smart metering projects outside of the UK;

Sweden:
ZigBee PRO is used in 270k electric meters in Gothenburg, Sweden, and is used currently as the last piece of the meter to head-end communications, sometimes referred to as the NAN (Neighbourhood Area Network). ***Goteborg Energi*** is now looking to build a a ZigBee HAN and to expand the range of services delivered through its ZigBee PRO network.

Finland:
Helen Electricity Network has announced a contract with Landis+Gyr for 200k ZigBee-enabled smart meters over the next 2 years.

Netherlands:
Philips has selected ZigBee as its wireless platform and has recently launched its LivingColors LED lighting product with ZigBee PRO-based remote controls.

France:
LeGrand has selected ZigBee as its wireless platform and its Arteor range of lighting, heating control and general home automation products.
Schneider Electric has selected ZigBee as its wireless platform.

Italy:
Telecom Italia and ***Enel*** are working together with ***Indesit*** and ***Electrolux*** on the Energy@Home project using ZigBee PRO networks.

Many more product announcements (details currently under NDA) by large European companies are expected in the next 6-12 months, in such areas as lighting, smart metering and home automation. We also expect to see ZigBee used in smart metering projects in at least 3-4 European countries other than the UK in the next 2 years.

Ember estimates that 3-5 million ZigBee PRO nodes will be sold in Europe in 2011.

ZigBee and European Standards

ZigBee and the ZigBee Alliance meets many (if not all) of the criteria for an open standard (see Appendix D), however the ZigBee Alliance, as a standards organisation, is always looking at ways to make adoption of its standard more acceptable and available generally. The ZigBee Alliance is also keen to support European utilities and manufacturers who would like to make use of ZigBee standards in smart metering programmes, and recognise that to do that effectively it is necessary to have ZigBee accepted within European Standards.

The approach to this has been on a number of fronts. The smart metering HAN contains a number of different devices such as electric meters, gas meters and in-home displays, the communications for which fall under the remit of multiple technical committees, particularly CEN TC 294, CENELEC TC 13 and CENELEC TC 205, as well as ETSI M2M. Mandate 441 seeks to bring together the work of these different committees. There are also numerous groups that are important within smart metering circles, such as ESMIG and DLMS User Association.

Liaison Agreements

To begin with, the ZigBee Alliance has opened up discussion and successfully formed liaison agreements with;

- ESMIG
- DLMS User Association
- CENELEC TC 13
- CEN TC 294

Further liaison opportunities are being pursued.

To facilitate the potential use of DLMS COSEM with ZigBee, ZigBee Smart Energy 1.1 contains tunnelling clusters to enable tunnelling of DLMS messages over ZigBee Smart Energy.

Ultimately, however, the goal of the ZigBee Alliance is to have ZigBee become a European Standard. The ZigBee Alliance has hired a representative and opened an office in the UK to support this effort.

ZigBee Smart Energy 2.0

ZigBee Smart Energy 2.0, which will be released in 2011, includes an IP stack and represents a step change in how the ZigBee Alliance operates as a standards organisation, because the entire ZigBee SE 2.0 solution will be formed of Internationally recognised standards; IEEE 802.15.4, IETF RFCs (6LoWPAN, RPL, TLS, TCP, UDP etc.) and IEC CIM (the application profile). ZigBee member companies are (and have been for > 1 year) actively involved within IETF to further develop the standards necessary for these networks and contribute the lessons learned from ZigBee development and deployment. ZigBee is also working to develop a certification process for SE 2.0 similar to the SE 1.0 process to validate interoperability for devices using these standards. With ZigBee Smart Energy 2.0, there is no argument about defacto standards etc., as these are all internationally recognised standards.

ZigBee Smart Energy 1.1 and European Standards

However, some European smart metering programmes wish to start with ZigBee Smart Energy 1.1 and ZigBee PRO networking and may or may not migrate to ZigBee SE 2.0 at some point in the future, so the ZigBee Alliance recognises the need to promote and support the use of existing ZigBee specifications.

To support mandate 441, the ZigBee Alliance believes that going forward there will have to be new European working groups and methods of working to encompass standards that spread themselves over multiple EU technical committees (TC) and do not neatly fit into the already defined pigeon holes within European standards institutions CEN and CENELEC. With the support of the ZigBee Alliance, the BSi, through its PEL/894 committee is proposing a new work item to be handled by way of a joint working group, with a convener from CEN/TC 294 and drawing expert representation from CEN/TC 294, CENELEC/TC 13, and CENELEC/TC 205. This idea already has support from UK experts and Mirror Committees for all TCs.

The HAN is an area that is not effectively addressed by current European Standards and will not be adequately addressed with current EU work packages in place within a timely manner. The UK market is progressing rapidly towards a smart meter roll out in 2012 with government aspirations to accelerate this rollout. Ofgem EServe in the UK has already indicated a smart metering functional specification incorporating HAN communications, and UK energy retailers are expressing functionality that is above what is currently being developed in EU working groups. British Gas has already made publicly available their smart metering requirements and name specifically ZigBee Smart Energy Profile within these documents. CENELEC/TC 13 WG2 have already reserved a place in their schedule of works for ZigBee Smart Energy Profile as a possible mechanism for transporting DLMS COSEM objects within the HAN.

The new work item proposal (reference CEN/TC 294 N 289) is to submit the following documents:

- "ZigBee Cluster Library Specification (Document 075123r02ZB)" (reference CEN/TC 294 N 292)
- "ZigBee-2007 Layer PICS and Stack Profiles (Document 08006r03)" (reference CEN/TC 294 N 290) and
- "Draft ZigBee Smart Energy Profile Specification (Document 105638r08ZB)" (reference CEN/TC 294 N 291)

(or the latest revisions of these docuements published at time of implementation) as a Committee Draft for review by the working group with the intention of publishing the already mature defacto standard for smart metering home area network (HAN) communications.

The UK (BSi) is proposing a convenor for the joint TC working group who would be responsible for liaising with CEN TC 294, CENELEC TC 205 and CENELEC TC 13 to seek involvement of experts to assist with the preparation, review and development of these documents as European Standards.

Under CEN/CENELEC procedures the proposal is to have a D-type relationship established between the ZigBee Alliance and this work group for the maintenance of the standard going forward.

This new work item proposal is on the agenda to be discussed and voted on at the upcoming 17th plenary session of CEN TC 294 on 10 h November 2010 (reference CEN/TC 294 N 296).

Appendix D: ZigBee as an Open Standard

1. Open Standard Definition

There are numerous definitions for 'open standard', and there is much debate about some definitions being so strict as to restrict free markets, or eliminating very popular 'defacto standards' such as WiFi and Bluetooth. The EU definition, used by the Interoperability Framework, has been criticised for being too strict, while attempts within the EU to loosen the definition have been met with equal criticism. The EU defines open standards thus (from http://www.digistan.org/open-standard:eu);

a. The standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.).
b. The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee.
c. The intellectual property - i.e. patents possibly present - of (parts of) the standard is made irrevocably available on a royalty-free basis.
d. There are no constraints on the re-use of the standard.

How does ZigBee measure up?

ZigBee arguably meets the conditions for being an open standard according to the EU definition;

(a) The ZigBee Alliance is a not-for-profit organisation. Ongoing development of ZigBee standards occurs on the basis of an open decision-making procedure, which involves member companies making proposals and discussing specifications via weekly conference calls and an email reflector, and a document management system hosted on the ZigBee portal. Although membership costs $9,500 for Participants and $3,500 for Adopters, anyone can join the ZigBee Alliance, and there are currently 380 member companies Worldwide. In some cases the ZigBee Alliance has signed liaison agreements with other organisations that are not members to enable them to participate in standards activities; e.g. WiFi Alliance, HomePlug Alliance, ESMIG, DLMS User Association, Engage Consulting (on behalf of ERA). We do not see the cost of membership as prohibitive to an organisation wishing to influence the development of the standard, and for organisations that are constrained legally or otherwise and cannot become members, we can find ways to liaise with them and get them involved, as we have done.
(b) All ZigBee standards are published when released and the specification documents are available for free to non-members from the ZigBee web site (http://www.zigbee.org/Products/DownloadZigBeeTechnicalDocuments.aspx).
(c) As a condition of joining the ZigBee Alliance, each member agrees to grant a RAND licence to other members relating to any IPR that they bring to the ZigBee standards (a typical way to deal with IPR in standards).
(d) To release a commercial product using ZigBee standards, there is a requirement to become at least an adopter member of the ZigBee Alliance at a cost of $3,500. While not free, this should not be seen as prohibitive or a significant constraint for people building commercial smart metering products, as for instance this is comparable to the cost of development tools required for an engineer to build a ZigBee application. For example, for a manufacturer selling 1m units of product per annum World-wide, this equates to $0.0035 per product shipped. In the context of smart metering this can hardly be seen as a constraint.

Furthermore, there are characteristics that enhance the appeal of ZigBee as a communications standard and the ZigBee Alliance as a standards organisation;

- There are currently 380 ZigBee Alliance members, roughly split 40% US-based, 30% European, 30% Asian.
- Membership includes silicon vendors, product manufacturers (including the leading meter and display manufacturers) and end users (including energy suppliers / retailers).
- Many of the engineers and companies active within the ZigBee Alliance are also active in other standards organisations such as the IPSO Alliance, IEEE, NIST, CEN, CENELEC, ETSI, Continua Alliance etc.
- The ZigBee PRO networking stack is available in 11 different certified platforms based on silicon from 6 different chip vendors, providing real competition, innovation and choice for manufacturers and ultimately for end users.
- ZigBee makes use of the IEEE standard, 802.15.4 for medium access (MAC) and physical (PHY). In other words, all ZigBee platforms are built on top of IEEE 802.15.4 standard radios.
- ZigBee includes standards at a networking layer, such as ZigBee PRO, but also standards at an application layer, such as the ZigBee Cluster Library and application profiles like ZigBee Smart Energy. Application layer standards enable interoperability with other communications standards such as WiFi and HomePlug.
- ZigBee uniquely addresses the vision of mandate 441, to have a common standard to be used for smart metering and home automation. Indeed ZigBee is a broadly adopted networking standard across multiple markets of interest to smart grid and smart metering; electric meters, gas meters, home appliances and other home automation. ZigBee can satisfy requirements currently covered by multiple disparate EU technical committees (CEN TC 294, CENELEC TC 13 and CENELEC TC 205).

2. Evolution of ZigBee as a standard

The ZigBee Alliance, as a true standards organisation, is always looking at ways to make adoption of its standard more acceptable and available generally. Three key initiatives are under way;

ZigBee Smart Energy 2.0 and IP networking

To facilitate the stated preference of the National Institute of Standards and Technologies (NIST), responsible in the US for the definition of standards for smart grid activities, and energy utilities and retailers in the US, the ZigBee Alliance has embarked upon it biggest transformation yet. For ZigBee Smart Energy 2.0, ZigBee will adopt IETF (IP) standards for networking and application protocols, while at the same time incorporating the Smart Energy application profile as an IEC CIM. Networking engineers from leading ZigBee Alliance members are working within IETF to help define and make successful, standards such as 6LoWPAN and ROLL. At the completion of this transformation, the ZigBee Smart Energy 2.0 platform will consist of IEEE, IETF and IEC standards.

ZigBee Smart Energy 1.1 and CEN/CENELEC

In an initiative designed to support EU mandate 441 and the requirements of GB smart metering, the ZigBee Alliance has initiated a new work item proposal which will be on the agenda of the November meeting of CEN TC 294. This work item involves a joint working group across CEN TC 294, CENELEC TC 13 and CENELEC TC 205, led by CEN TC 294 and backed by BSi mirror groups, to take the ZigBee Smart Energy 1.1 application profile, ZigBee Cluster Library and ZigBee PRO networking specifications and make them available as European Standards.
While it has already been argued that ZigBee is already an open standard, and as such should be acceptable for GB smart metering, ZigBee will soon offer 2 options based on IEEE 802.15.4 radios; an IP networking solution based on IETF and IEC standards; and a ZigBee PRO networking solution based on European Standards.

ZigBee Alliance and ANSI

The ZigBee Alliance has been a full ANSI Organizational Member as of October 2009 and has submitted an application for accreditation as an ANSI Accredited Standards Developer and proposed operating procedures for documenting consensus on proposed American National Standards. This process is ongoing.

3. Summary

ZigBee is well suited to the requirements of GB smart metering as it covers the current and future requirements of the home area network and in the case of many of these features, will implement them in the USA ahead of the official GB smart metering rollout.

That ZigBee is a well supported defacto standard is undeniable, with 380 member companies in the ZigBee Alliance, multiple vendors of platforms and products, and significant deployments Worldwide in markets including smart metering and home automation. It can also be argued that ZigBee is an Open Standard and that it meets, or comes very close to meeting the strict definition of Open Standard within the EU.

Finally, the ZigBee Alliance and ZigBee is always striving to become a better and ‘more open’ standard, by working openly with other standards organisations; developing an IP solution and standard based on IEEE, IETF and IEC standards; and by offering its existing standards to be adopted as European Standards.

So, it can be argued that ZigBee is fit for purpose, already meets most people’s definition of open standards, and is working to satisfy even stricter defintions of open standard.