

Response to the UK consultation on a Smart Metering Implementation Programme : Prospectus

This document contains responses to the Consultation being run by Ofgem E-Serve on behalf of the Bluetooth Special Interest Group.

Introduction – The Bluetooth SIG

The Bluetooth Special Interest Group (SIG) is an industry based standards organisation responsible for developing and maintaining the Bluetooth short range wireless standard and administering a qualification and interoperability program to ensure that all products released to the market based upon that standard meet interoperability, backwards compatibility and compliance requirements. The Bluetooth standard and IP contained within it are licensed free of charge on a RANDZ basis to Bluetooth members. Membership currently stands at over 13,000 companies worldwide. Membership is open to all, with a free membership level available to those companies that want access to use the standard. Paid membership levels confer the right to participate in specification development.

The Bluetooth SIG is active in the smart energy field, with the Bluetooth wireless standard already being used in numerous devices. The Bluetooth SIG contains a Smart Energy Engineering Task Force, which is working with a variety of smart metering standards bodies and which has produced this response. The Bluetooth SIG has recently released a low energy version of the Bluetooth standard, which is targeted at secure, ultra-low power applications and is particularly relevant to smart metering and home area automation. The low energy version uses a 2.4GHz radio design that is robust, even in the presence of interference from other radios. The Bluetooth SIG believes that this is an ideal solution for smart metering.

Detailed Response:

The following is the Bluetooth SIG's response to the high priority questions, where a response has been requested by 28th September 2010.

Smart Metering Implementation Program

Question 3. *Do you have any comments on the proposed approach to ensuring customers have a positive experience of the smart meter rollout?*

The Bluetooth SIG endorses the approach to providing a positive customer experience. The SIG's experience of shipping over 3 billion wireless devices has shown that the challenge of connecting wireless devices is difficult. Unlike products that connect using a cable, there is no intuitive method to associate wireless devices with each other, or determine which devices are connected.

The Bluetooth SIG recommends defining a standardised user interface for this connection as a requirement, so that consumers would be able to add devices to the HAN, or replace the IHD with a compatible unit with greater functionality. Without that, it will be difficult for users to extend their ecosystem of connected smart energy products.

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?*

The Bluetooth SIG does not have any comments on the Functional Requirements. It considers these are complete and appropriate for purpose.

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

The Bluetooth SIG does not believe that any short range wireless technology is currently mature enough to be considered as a complete technical solution for a smart meter. However, The Bluetooth SIG believes that Bluetooth is closer than any other wireless technology in this respect.

The Bluetooth SIG bases this view on the observation that completion of a specification is not sufficient to prove the maturity of a wireless technology. Maturity of a wireless technology does not come with the approval of a specification; it comes only after significant numbers of deployed products appear in market place, so that their performance can be tested in real world conditions in a particular use scenario. Key areas where this is apparent are:

- **Susceptibility to interference** from other wireless devices operating in the same band and vulnerability to jamming from fixed channel technologies. Specifications attempt to predict interference when they are being written, but the proliferation of new radio standards and use cases means that interfering sources can evolve before any standard is complete. Moreover specification writers rarely anticipated what consumers will actually buy and deploy within their home. Hence many wireless standards have proven to be inadequate only at the point that they have been deployed. Early ZigBee implementations and RF4CE are examples of standards that worked in the laboratory, but have failed in significant numbers in the field. [1].
- **Security.** Responsible wireless specification development organisations always do their best to address security, but hackers generally operate from a different perspective, discovering flaws that had not occurred to the specification writers. These may be in the core standard itself, or in practical implementations which have other security holes. These only appear after enough products have been shipped for hackers to feel it is worth spending time looking for flaws. Bluetooth and Wi-Fi technologies, which have shipped billions and hundreds of millions of devices respectively, have experienced this and have addressed these issues to improve their security. Standards that have only shipped in small volumes, such as Z-Wave, wireless MBUS and ZigBee have either not come under scrutiny, or only just beginning to attract it [2]. Whilst every standard must present a risk as hackers try new attacks, the risk for an untested specification is much higher. In reality, it means that an untested standard is likely to need further years of development and testing after its initial completion date and real implementations appear on the market before it can be considered as an acceptable risk to integrate the standard into devices which have a security requirement.

- **Power Consumption.** The gas meter's battery capacity defines the lowest common denominator for power consumption of a HAN technology. Being able to operate in a long-term battery-powered environment is the level of performance that must be met.

Different wireless technologies have very different power consumptions. For example, that of Bluetooth low energy is around 15µAsecs for each item of meter data transmitted compared to 1.5mAsecs for ZigBee. That difference of one hundred means a meter using Bluetooth low energy can operate with a battery having only one percent of the capacity needed by other radios. In practice, other parts of the meter will also determine battery capacity, but Bluetooth low energy will minimise the effect of the radio.

In the real world, issues such as interference and physical location can mean that a radio needs to be active for much longer than an ideal analysis would suggest. Even a simplistic calculation like the one above can be changed by orders of magnitude when location (range) and interference are taken into account.

Other requirements also affect power consumption. A need to support IPv6 over the air will require a radio support longer or a greater number of packets, increasing power consumption. Similarly, a protocol that requires host acknowledgements instead of baseband acknowledgments will increase power consumption. Although these may seem to be fine details, they can result in a lifetime that bears no relationship to what is often quoted in data sheets. A thorough analysis needs to be performed for the HAN choice, based on the impact of all of these operational parameters. Unless that is done, it is likely that the gas meter requirements will not be met.

Question 16. *Do you have any comments on the proposals for requiring suppliers to deliver the rollout of smart meters?*

The Bluetooth SIG agrees with this strategy.

Question 17. *Do you have any comments on our implementation strategy?*

The Bluetooth SIG agrees that the rollout prior to DCC services becoming available constitutes a higher risk, but the resulting benefits of early experience would appear to significantly outweigh these.

Question 18. *Do you have any other suggestions on how the rollout could be brought forward?*

The Bluetooth SIG does not believe the meter rollout should be brought forward. There is already considerable risk in generating the technical specification in the proposed timescale. Accelerating the roadmap would require an earlier completion date for the technical standard, which we believe would carry an unacceptable level of risk. This would increase the likelihood of needing to replace meters or HAN modules and extend the date for a fully functioning system.

As well as completing the technical specification, it is also necessary to produce test equipment and test procedures. Products which are shipped must be proven to comply with these specifications. As well as qualifying these products against the specification, there is a necessary phase where products are tested against each other to ensure interoperability. As well as ensuring that they conform to the specification, this is a valuable exercise to test individual implementations to determine whether the specification has been interpreted differently by different companies, which may highlight errata which need to be fed back into the technical specification. This typically happens in the period after the specification is approved. If the timescale is shortened it is likely to mean that products are not fully tested as being compliant or interoperable. It also means that test equipment may not be able to be deployed in a timely manner to certify meters and IHDs and that field test and installation equipment may not be available.

Question 19. *Do you think that the technical specifications can be agreed more quickly than the plan currently assumes and, if so, how?*

As stated above, the Bluetooth SIG does not believe the technical specification can be accelerated. Security, robustness to interference and interoperability all need to be tested before a standard should be incorporated into the technical specification.

In addition, wireless standards typically include a large element of Intellectual Property, for which member agreements need to be obtained and reviews performed to ensure that it is legal to implement the specification. Standards bodies do not generally formally adopt a specification until they have performed this IP review, which can add up to three months to the adoption process. As there is no suitable adopted HAN standard in existence today that fully meets the technical requirements, then this needs to be considered within the development timescales.

Because of this the Bluetooth SIG does not believe that any HAN standard can realistically compress their timescales. Achieving the current timescales is already a significant risk, although the Bluetooth SIG believes that the Bluetooth standard is sufficiently mature that it will be capable of doing so.

Question 20. *Do you have any comments on our proposed governance and management principles*

The Bluetooth SIG agrees has no comments on the proposed governance and compliance principles.

References:

1. Interference:
 - a) Multichannel reliability in real homes for wireless sensor networks - <http://cse.wustl.edu/Research/Lists/Technical%20Reports/Attachments/926/infocom11.pdf>
 - b) WLAN interference to 802.15.4 http://cs.sch.ac.kr/cs_now/SEMINAR/english/080111_WLAN%20Interference%20to%20IEEE%20802.15.4.pdf

c) PG&E lays blames other devices for being susceptible to interference – <http://www.smartplanet.com/technology/blog/thinking-tech/wait-california-smart-meters-do-have-problems/5148/>

d) Interference from Eon meters – <http://www.learningconversations.co.uk/main/index.php/2008/05/21/eon-smart-meter-and-my-wireless-network?blog=5>

e) EMF Safety Network - http://emfsafetynetwork.org/?page_id=1223

f) Example of inaccurate technical communications to consumers from utilities - SDGE - <http://www.sdge.com/smartmeter/faq.shtml>

"If the premise also has a gas meter, the frequency from the electric meter to the gas meter is 2.4 GHz (gigahertz). The electric meter frequency is similar to a cell phone and the gas meter frequency is similar to a computer router. *Neither device will interfere with any wireless devices in the home.*"

2. Security Issues

a) Security Firm Finds Smart Meter Problems

<http://www.cooperativefinancecorporation.org/security-firm-finds-smart-meter-problems/>

b) Buggy 'smart meters' open door to power-grid botnet

http://www.theregister.co.uk/2009/06/12/smart_grid_security_risks/

On behalf of the Bluetooth Special Interest Group

Contacts:



Cambridge Silicon Radio (CSR) Ltd.



WiFore Consulting Ltd.