Technical Document

Response to Smart Metering Implementation Programme (11D/836)

Project	DECC Smart Metering Implementation Programme
Document Ref.	DSMIP/TD000001/V1.0/rcc
Date	13/10/11
Status	Release
Distribution	

Revision History

Version	Date	Description
1	13/10/11	First release

Contents

Table of Contents

1 Introduction

This document is the response by Gridmerge Ltd. to the Smart Metering Implementation Programme: A consultation on draft licence conditions and technical specifications for the roll-out of gas and electricity smart metering equipment (August 2011) published by DECC on 18th August 2011 to the questions requiring response by October 13th 2011.

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.

1.2 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, electric vehicle communication 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 lwig working group	Co-Chair
IETF 6lowpan working group	Contributor
IETF roll working group	Contributor
IETF core working group	Contributor
IETF homenet working group	Contributor
UCAIUG OpenSG OpenHAN	Contributor
NIST SGIP Cybersecurity Working Group (CSWG)	Contributor
SAE J2836 J2847 J2931 J2953 Work Group	Contributor
ISO/IEC 15118 Electric Vehicle Communication Standard	Contributor

1.4 Gridmerge Ltd and the UK programme

Due to heavy and focussed involvement in the US, Gridmerge Ltd. has not had any specific involvement in the UK programme up to now. However, Gridmerge Ltd. is in a unique position to apply experience and knowledge gained in the US Smart Grid and Smart Meter industry to the developing programme in the UK being lead by DECC and Ofgem E-Serve, especially in the Home Area Networking, electric vehicle 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 No particular comment

Programme questions regarding response to which Gridmerge Ltd. has no particular comment are:

1 – 3, 6 – 7, 11 – 23, 29, 31 – 33, 43 – 45, 47, 50 – 52.

2 Prospectus Questions

4. Do you agree that Smart Metering Equipment should be compliant with the SMETS extant at the time of installation and that it should continue to be compliant with that version of the SMETS through the operational life of the equipment? Please explain your reasoning.

Smart Metering Equipment should be compliant with the SMETS extant at the time of installation. Smart Metering Equipment should not necessarily continue to be compliant with the original version of the SMETS as there may be valid reasons for modification, for example:

- Enhanced functionality
- Security upgrading due to compromise of specific algorithms

Smart Metering Equipment therefore needs to be capable of being upgraded due to future revisions of the SMETS and have sufficient flexibility and contingency to be able to support upgrades. This primarily means having sufficient code and data storage for the software capable of proving operation throughout its lifetime, which may be up to 20 years for certain types of devices.

5. Do you agree that in some exceptional circumstances suppliers should be required to retrofit Smart Metering Equipment that has already been installed? Please explain your reasoning.

It may be necessary in exceptional circumstances but should be strongly discouraged and Smart Metering Equipment manufacturers should provide evidence that their equipment is capable to the best of their knowledge to meet its lifetime requirement.

8. What contribution do you think the interoperability licence condition as drafted could play in ensuring that suppliers work together to ensure Smart Metering Equipment is interoperable? Please explain your reasoning.

The interoperability licence condition should ensure that stakeholders agree on ubiquitous standards and Smart Metering Equipment manufacturers adhere to those standards. This will greatly enhance the likelihood of equipment interoperating successfully and limit the likelihood of equipment replacement due to change of supplier.

9. Do you think the licence conditions as drafted effectively underpin the policy intention to ensure Smart Metering Equipment is interoperable? Please explain your reasoning?

The licence condition statements AA 8.a.i and BB 7.a.i disallowing replacement of equipment essentially underpins the intent for interoperability. However, licence condition statements AA 8.a.ii and BB 7.a.ii state that remote modification or reconfiguration is allowed. Remote configuration is acceptable, however routine remote modification should be discouraged as this does not ensure that system developers will work to a common standard. Nevertheless, it is necessary to include a secure firmware update facility (preferably over the air) for essential updates.

10. What role could a dispute resolution mechanism have a role in ensuring interoperability? What key features should such a mechanism have?

A proactive approach is the preferred way to deal with ensuring interoperability through the use of common standards and an associated rigorous test and conformance programme. A dispute resolution mechanism may need to exist but should be a last resort and not encourage as the primary mechanism for agreeing on interoperability.

24. Do you think that there are other requirements that the Government should adopt in the SMETS? Please explain your reasoning.

The SMETS should use open standards. Gridmerge Ltd. recommends that those open standards should be based on the Internet Protocol (IP) wherever possible, including WAN and HAN communication, with the preference for IPv6 and use ubiquitous protocols on top of IP, e.g. HTTP/XML or equivalents being developed in standards development organisations (SDOs).

There should also be requirements for the development of an associated PICS (Protocol Implementation Conformance Statement) and Test Plan in conjunction with the SMETS. In conjunction with conformance testing, this will ensure interoperability between Smart Metering Equipment.

25. Do you agree that all the requirements recommended in the IDTS should be adopted by the Government in the SMETS? Please explain your reasoning.

The final revision of requirements recommended in the IDTS should be adopted by the Government in the SMETS. On review of the IDTS, the author believes there are some significant issues yet to be resolved in the IDTS and the requirements hence the emphasis on the final revision of the IDTS.

26. Do you agree that the security requirements recommended in the IDTS are proportionate to the level of risk that the End-to-end Smart Metering System faces? Please explain your reasoning.

The security requirements are generally proportionate to the level or risk the end-to-end Smart Metering System faces as they identify the key requirements pertaining to a system which has critical assets and also maintains private data.

The delegation between SM HAN and the customer HAN as shown in the IDTS Figure 26 needs some consideration as the security requirements for an IHD as a core device may be onerous (e.g. FIPS 140-2 validation) and the placement of critical assets (EV and DER) in the consumer HAN also needs some consideration.

27. Do you agree that the process outlined above is a suitable way forward to develop the SMETS? Please explain your reasoning.

Based on the author's considerable experience in Smart Metering rollouts in the USA, the author believes that the IDTS in its current state has some issues and these need to be considered further, in addition to the legal and regulatory review recommended. Gridmerge Ltd. will be happy to provide a comprehensive review of the IDTS.

28. Do you think that the SMETS should ultimately be governed as part of the Smart Energy Code? What alternative arrangements could be adopted for the ongoing governance of the SMETS? Please explain your reasoning.

The SMETS needs to be under some sort of governance. Whichever governance it is, it must provide a certification, assurance and enforcement framework to ensure interoperability. The author has experience of organisations such as the NIST SGIP and the UCAIUG in the USA and would recommend a similar model for the UK.

30. Do you agree that the Government should include a requirement for a Communications Hub in the SMETS? Please explain your reasoning.

It is not clear if the question specifically refers to a *separate* Communications Hub. The most important issue here is to ensure that the Communications Hub can be either separate or included within another device, e.g. electricity meter. On that basis, the HAN technology choice must be able to be flexible enough to accommodate these different architectures.

34. Do you agree with the Government's proposal that fully integrated electricity meters and Communications Hubs will not comply with the SMETS? Please explain your reasoning.

The SMETS may cover a number of aspects of functionality and implementation details therefore aspects of fully-integrated electricity meters and the Communications Hub may well be covered in the SMETS. For that reason, to say that a particular device should not comply to a wide-ranging specification isn't granular enough and it would make more sense to break down the components of these devices and the component parts of the SMETS and make a more comprehensive statement.

35. Do you think the Smart Metering Implementation Programme objectives would be better met by:

a. Using the SMETS to mandate a separate Communications Hub with a fixed WAN transceiver? Or

b. Giving suppliers flexibility over options for configuration of the Communications Hub?

Please explain your reasoning.

Providing the functionality of the devices is clearly specified and various architectures can be accommodated and the component parts together in a system all interoperate (as noted in the footnote), there is no particular need for solution (a), therefore (b) would be preferable.

36. Do you agree there should be no restrictions on the HAN standards adopted by suppliers, provided they are available as a European (CEN, CENELEC or ETSI) or International (IEC or ISO) standard? Please provide evidence to support your position.

There needs to be a single HAN standard, otherwise interoperability will be seriously compromised. The HAN standard which Gridmerge Ltd. proposes is the SEP 2.0 standard being developed in the ZigBee Alliance and endorsed by a consortium including the Wi-Fi Alliance, the HomePlug Alliance and the HomeGrid Alliance. The reasons SEP 2.0 is proposed is for the following reasons:

- Based on open standards
  - Internet Protocol (ubiquitous standards specified in the IETF)
  - HTTP/XML web standards (ubiquitous standards specified in the IETF and W3C)
  - CIM model (IEC 61968)
- Ability to run over multiple HAN MAC/PHY standards, thus providing a solution for problem sites
- Enhanced functionality to include electric vehicles and distributed energy resources
- Scalable over IP networks therefore suitable for WAN
- End-to-end security based on common networking protocol

The Application Specification has been approved and interoperability testing is due to start in November 2011. The ZigBee IP specification forms part of the SEP 2.0 suite and is an IPv6 stack for 802.15.4 devices (2.4GHz and 868/900MHz). All steps will be taken by the ZigBee Alliance to ensure that all aspects of the standard are formally accepted as work items by international standards bodies.

If the view is that the SEP 2.0 standard is too immature, then the ZigBee SEP 1.x standard is recommended.

37. The IDTS has recommended that all standards should be recognised or be in the process of being recognised by 31 December 2014; do you agree with this recommendation? Please explain your reasoning.

The timeframe stated is reasonable given the need to get the programme underway regarding Mandate 441.

38. Do you think that regulatory obligations are needed to underpin a systematic approach to testing of HAN standards during the Foundation phase? Please explain your reasoning.

The HAN standard chosen must meet the fundamental requirements of interoperability and scalability with a view to providing end-to-end security. It may be necessary to impose regulatory obligations to ensure that the testing of HAN standards meets the fundamental requirements.

39. Do you agree with industry's recommendation that DLMS should be adopted as the application layer for communications with the DCC? Do you believe there are any consumer, economic or technical issues with this solution which could be circumvented by an alternative approach? Do you have any economic, technical or consumer evidence to assist Government in evaluating industry's proposal?

Gridmerge Ltd. is ambivalent to some extent regarding the choice of application protocol for the WAN. To increase the likelihood of end-to-end security and commonality, a system based on the CIM (IEC 61968), which covers all aspects of utility and service provider operations, is recommended.

40. Do you agree with industry's recommendation that DLMS and Zigbee SEP 1.x should be adopted as the application layer for communications within the consumer premises, provided they install the necessary translation equipment? Do you believe there are any consumer, economic or technical issues with this solution which could be resolved by an alternative approach? Do you have any economic, technical or consumer evidence to assist Government in evaluating industry's proposal?

The HAN standard which Gridmerge Ltd. proposes is the SEP 2.0 standard being developed in the ZigBee Alliance and endorsed by a consortium including the Wi-Fi Alliance, the HomePlug Alliance and the HomeGrid Alliance. The reasons SEP 2.0 is proposed is for the following reasons:

- Based on open standards
  - Internet Protocol (ubiquitous standards specified in the IETF)
  - HTTP/XML web standards (ubiquitous standards specified in the IETF and W3C)
  - CIM model (IEC 61968)
- Ability to run over multiple HAN MAC/PHY standards, thus providing a solution for problem sites
- Enhanced functionality to include electric vehicles and distributed energy resources
- Scalable over IP networks therefore suitable for WAN
- End-to-end security based on common networking protocol

The Application Specification has been approved and interoperability testing is due to start in November 2011. The ZigBee IP specification forms part of the SEP 2.0 suite and is an IPv6 stack for 802.15.4 devices (2.4GHz and 868/900MHz). All steps will be taken by the ZigBee Alliance to ensure that all aspects of the standard are formally accepted as work items by international standards bodies.

If the view is that the SEP 2.0 standard is too immature, then the ZigBee SEP 1.x standard is recommended.

The use of DLMS in the HAN may be appropriate if it is used in the WAN. If an IP-based network is specified for the HAN, this may be able to be carried end-to-end from headend to electricity meter in a secure manner.

Gridmerge Ltd.'s involvement in the USA and in assisting in imminent SEP 1.x rollouts has been around helping the NIST Cyber Security Working Group (CSWG) and the NESCO (National Electric Sector Cybersecurity Organization) Task 1 analyse the security issues surrounding SEP 1.x. On that basis, although SEP 2.0 appears less mature, it is able to run on network infrastructures which have been more proven, e.g. IP over Wi-Fi.

This questions conflicts with question 48 to some extent in that Q48 assumes there will translation at the Communications Hub; this may not be the case if the application endpoint for DLMS resides on an electricity meter which is connected to the HAN. In this case, there would be no translation in the Communications Hub.

41. Do you think the Smart Metering Implementation Programme objectives would be best met by the proposed approach above? Or should a single, network-layer technology standard such as IPv6 be mandated? Please explain your reasoning.

Gridmerge Ltd. proposes that IPv6 (preferably) or IPv4 be mandated for network layer technology. IP can and does exist on an extremely wide range of underlying technologies from low bit rate serial modem to terabit-per-second fibre optics. IPv4 is still current but there is a strong push with the fact that no new IPv4 address pools are now available and therefore IPv4 addresses will run out at some point. If IPv6 is specified in the WAN and the HAN, this provides the possibility for a clean architecture and end-to-end security and high flexibility in the actual physical implementations of HAN topologies

Some of the concerns regarding packets size and efficiency have been looked at in the development of ZigBee IP (IP over 802.15.4 networks) and recent interoperability testing has shown a typical HAN pushed to its operational limits is capable of transporting all data necessary.

42. Is the provision of a single network-layer address for each Communications Hub a reasonable and sufficient functional requirement for the Smart Meter WAN? Will this requirement limit potential future capability or present challenges, for example, in multi-occupancy buildings?

It is a reasonable and sufficient functional requirement for the Smart Meter WAN. Almost all WAN technologies currently carry IP traffic and therefore using such a ubiquitous standard would bit limit potential future capability. IP would not present challenges in multi-occupancy buildings; on the contrary, it would actually help to use IP due to its ability to be routed across multiple different subnets.

46. Do you agree with the proposed approach for consumers to access data and transfer it from the HAN via a separate “bridging” device? Please explain your reasoning.

The 'bridging' device is the most sensible approach, especially if the HAN is based on IP. The bridging device may then end up being a simple router. End-to-end security is maintained through the subnets by means of using IP.

Alternatively, a bridging device which provides application layer translation is also acceptable.

48. Do you agree with industry’s proposals for an overall architecture of an application layer standard with translation through a Communications Hub to a HAN? Do you believe there are any consumer, economic or technical issues?

It would be preferable to have an IP-based system with a common application layer based on the CIM/SEP 2.0. This model can provide true end-to-end security and is scalable to incorporate future devices such as electric vehicles and DERs. Economically this may be preferable, as the device need not have any knowledge of the application layer and can thus function as a router, much like home router devices do today.

Alternatively, the proposal for application layer standardisation in the WAN, and (different) application layer standardisation in the HAN, with translation at the Communications Hub is the next best approach. It is harder to achieve end-to-end security with two different application layers and translation implies the data will be vulnerable at some stage during the unsecuring and resecuring at the Communications Hub.

49. Where do you believe that translation is best managed:

a) At the Communications Hub; Or

b) At the DCC?

Do you have any economic, technical or consumer evidence to assist Government in evaluating the options?

If the solution in Q48 is for application layer translation at the Communications Hub, then it has to occur there. Using a CIM-based solution would facilitate translation (if necessary) at the DCC and then the application payload can be carried all the way to the application endpoint.

53. Do you agree with or have any comments on the Government's proposals for the outstanding issues from the Response? Please explain your reasoning.

There are no particular issues with the outstanding issues in Table 6. Generally, Gridmerge Ltd. has concern that there is a distinct lack of progress in the selection of the HAN technology. Many of the vendors currently support ZigBee SEP 1.x and ZigBee SEP 2.0 is also now in a suitable timeframe. Gridmerge Ltd. believes one of these HAN protocols should be chosen and proposes SEP 2.0.

54. Do you think that an assurance framework, underpinned by regulatory obligations, is needed to support the delivery of the required functionality, interconnectivity, interoperability, and security of Smart Metering Equipment? Please explain your reasoning.

The Government should ensure Standards are chosen that provide the required functionality, interconnectivity, interoperability and security. The Standards chosen should provide their own testing and certification process that can be tested and validated by the Government rather than have a separate process established for the UK.

55. Do you agree that as part of any assurance framework adopted, there should be a testing regime in place to support the delivery of the required functionality, interoperability and security? Please explain your reasoning

There needs to be a testing and certification regime in place. This will ensure that approved and certified products have been through rigorous testing and therefore will interoperate with other approved products. The ZigBee Alliance is an example of an organisation which provides such a test and certification regime.

56. What are your views on the options outlined for a testing regime? Are there other options that should be considered?

The most appropriate way forward is a certification or accreditation scheme based on common standards. It should not be necessary to have to legislate, nor should it be necessary to have a government-led body to oversee testing and accreditation. There are many examples of such

schemes which have been used successfully to ensure interoperable products based on common standards.

57. Do you think that a different approach to assurance is necessary for the Foundation and enduring phases? Please explain your answer.

No, on the basis of using a testing and certification programme. The testing and certification should be based on common standards and developed in conjunction with those standards if it does not exist already. If there are any gaps, it may be necessary to develop additional alliances with their own testing and certification scheme.

If there is an insistence on legislation-based or government-led approach, this may not be appropriate for the foundation phase.

58. Do you think that the activities outlined above are a suitable way for achieving interoperability across Smart Metering Equipment cryptographic functionality? How else could this be achieved?

Development of an end-to-end trust hierarchy and cryptographic key management, along with common cryptographic interfaces and underlying standards and algorithms provides the ability for true end-to-end secure communication and would greatly increase the likelihood of interoperability. Such a system must be scalable so it can suit the wide range of devices present in the Smart Metering Equipment and DCC.

It may not be necessary to have a single PKI (public key infrastructure) and indeed may be preferable to distinguish the PKI for Smart Metering Equipment and DCC devices. If there are distinct security domains due to cryptographic differences, these must meet at entities trusted in both domains and at that point can have some vulnerability due to need to resecure communication data between the domains.

59. Do you agree that cryptographic/ key management is necessary to secure the End-to-end Smart Metering System? Please explain your reasoning

Cryptographic key management is necessary to secure the end-to-end Smart Metering System and this should be preferably be based on public key cryptography and PKI. If symmetric keys are used, a clear key distribution and management policy must be in place.

Direct management by DCC of symmetric keys for devices in the SM HAN may add unnecessary administrative burden on the DCC infrastructure.

60. Do you agree with the Government's assessment of the advantages and disadvantages of the cryptographic solutions identified above? What other options should the Government consider? Please explain your reasoning

In a complex system, it is unlikely that it will be an either/or choice. It is noted that the advantages and disadvantages as listed do not actually recommend one method. Fundamentally, the hybrid approach is by far the most common approach, and the public keys used for a hybrid approach can also be used independently for e.g. data signing and verifying.

The use of symmetric keys on a wide scale is usually impractical, due to the issue of having to securely distribute the symmetric keys.

Therefore, Gridmerge Ltd. proposes the hybrid approach generally, which uses symmetric keys in certain parts of the system and asymmetric keys in other parts of the system.

Some of the assertions in table 7 are incorrect, e.g.

- Digital certificates do not provide repudiation protection; individual message signing provides some repudiation protection

- Shared keys are typically established using key agreement in the hybrid approach but can also be securely transported

It is suggested that the hybrid approach, as consistently used in all information networks is the one adopted.

61. Do you think that it would be appropriate for the DCC to be responsible for cryptographic key management for the End-to-end Smart Metering System? What other options should the Government consider? Please explain your reasoning.

Cryptographic key management is a wide-ranging subject. There are aspects of cryptographic key management which may be appropriate for the DCC to maintain or at least specify a single subcontractor to maintain. There are other aspects of cryptographic key management which product manufacturers may wish to control themselves, e.g. firmware signing,

62. How do you believe the security approach should be applied to opted out non-domestic consumers? Do you see any issues with the approach? Please explain your reasoning.

It would be preferable if there is a common security approach where possible. In the case of certain devices which receive data, it is important that the data is secure to the application endpoint within that device. Beyond that, it is up to the owner of the device what they do with the information received to a large extent. As an example, a meter manufacturer is responsible for displaying an accurate reading of electricity consumption on the display. This data may have significant privacy issues, however, should a homeowner choose to put a webcam on the meter and post readings periodically on a publicly-accessible web site, it is entirely the homeowner's responsibility.