



Technical Document

Response to Smart Metering Prospectus for October 28th 2010

Project	Ofgem E-Serve Smart Metering Prospectus
Author	[REDACTED]
Document Ref.	OSMP/TD000002/V1.0/rcc
Date	28/10/2010
Status	Release
Distribution	

Revision History

Version	Date	Description
1	28/10/10	First release

Contents

Table of Contents

1	Introduction.....	4
1.1	About Gridmerge Ltd.....	4
1.1.1	Contact details.....	4
1.2	About Robert Cragie.....	4
1.3	Involvement in USA Smart Grid activities.....	5
1.4	Gridmerge Ltd and the UK programme.....	5
1.5	Gridmerge Ltd.'s Prospectus Questions response.....	6
1.5.1	Response provided.....	6
1.5.2	No particular comment.....	6
2	Prospectus Questions.....	7
2.1	Question 2 response.....	7
2.2	Question 5 response.....	7
2.3	Question 15 response.....	7
3	Detailed analysis of Data Privacy and Security.....	8
3.1	Communication flows.....	8
3.1.1	Meter to IHD.....	8
3.1.2	Meter to Direct Third Party Service Provider.....	8
3.1.3	Meter to Indirect Third Party Service Provider.....	9
3.2	Clause and figure comments.....	9
3.2.1	Section 2.....	9
3.2.2	Section 3.....	9
3.2.3	Section 4.....	10
3.3	Questions from Data Privacy and Security.....	11
3.3.1	Question 1.....	11
3.3.2	Question 2.....	12
3.3.3	Question 3.....	12
3.3.4	Question 4.....	12
3.3.5	Question 5.....	12

1 Introduction

This document is the response by Gridmerge Ltd. to the Smart Metering Prospectus published by Ofgem E-Serve on 27th July 2010 to the questions requiring response by October 28th 2010.

Gridmerge Ltd. provides this response as an individual.

1.1 About Gridmerge Ltd.

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

- Pacific Gas and Electric Company
- Grid2Home Inc.

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

[REDACTED]

1.1.1 Contact details

[REDACTED]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.3 Involvement in USA Smart Grid activities

Pacific Gas and Electric are one of the most progressive utilities in the USA with regard to Smart Grid and Smart Metering. They have already installed 6.7 million Smart Meters in a programme of installing 10 million Smart Meters. They have employed experts and consultants (including Gridmerge Ltd.) in the wide ranging area of Smart Grid development in the state of California.

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

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

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

1.4 Gridmerge Ltd and the UK programme

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

1.5 Gridmerge Ltd.'s Prospectus Questions response

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

- Network Communication Protocols
- Application Protocols
- Cybersecurity

1.5.1 Response provided

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

Question 2: Do you have any comments on our overall approach to data privacy?

Question 5: Do you have any comments on the proposed approach to smaller non-domestic consumers (in particular on exceptions and access to data)?

Question 15: Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?

1.5.2 No particular comment

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

Question 1: Do you have any comments on the proposed minimum functional requirements and arrangements for provision of the in-home display device?

Question 4: Have we identified the full range of consumer protection issues related to remote disconnection and switching to prepayment?

Question 8: Do you have any comments on the proposals that energy suppliers should be responsible for purchasing, installing and, where appropriate, maintaining all customer premises equipment?

Question 9: Do you have any comments on the proposal that the scope of activities of the central data and communications function should be limited initially to those functions that are essential for the effective transfer of smart metering data, such as data access and scheduled data retrieval?

Question 10: Do you have any comments on the proposal to establish DCC as a procurement and contract management entity that will procure communications and data services competitively?

Question 11: Do you have any comments on the proposed approach for establishing DCC (through a licence awarded through a competitive licence application process with DCC then subject also to the new Smart Energy Code)?

Question 12: Does the proposal that suppliers of smaller non-domestic customers should not be obliged to use DCC services but may elect to use them cause any substantive problems?

Question 13: Do you agree with the proposal for a Smart Energy Code to govern the operation of smart metering?

Question 14: Have we identified all the wider impacts of smart metering on the energy sector?

2 Prospectus Questions

2.1 Question 2 response

Do you have any comments on our overall approach to data privacy?

This is addressed in section 3.3.1.

2.2 Question 5 response

Do you have any comments on the proposed approach to smaller non-domestic consumers (in particular on exceptions and access to data)?

Whilst there are similarities between domestic and non-domestic, there are also significant differences too. Based on experience in the USA, the programmes for commercial building and those for domestic have run independently. This is in part due to the different business models in the US but also due to incumbent building management systems being used for asset control and information distribution. This needs to be considered if trying to incorporate existing DR systems with the domestic smart meter rollout.

2.3 Question 15 response

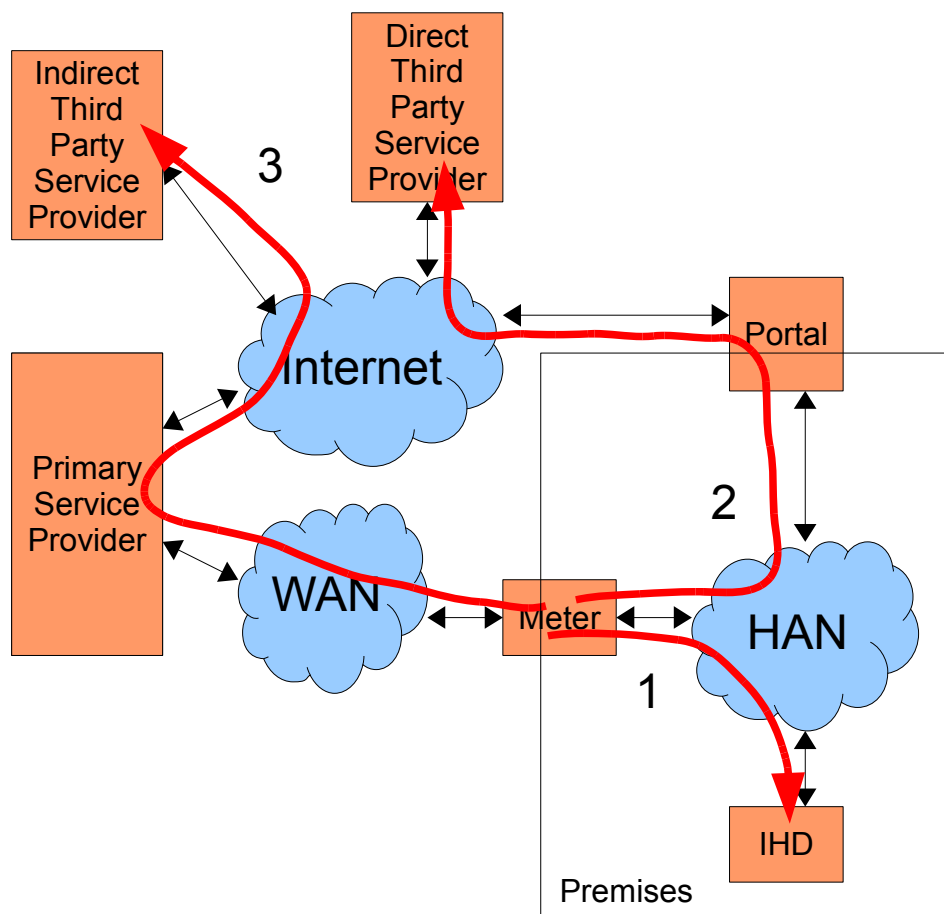
Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?

Comments can be found in section 3.

3 Detailed analysis of Data Privacy and Security

A detailed analysis of Ref 94e/10 Smart Metering Implementation Programme: Data Privacy and Security was undertaken to consider responses to this question.

3.1 Communication flows



Drawing 1: Example communication flows for consumption data

The above diagram gives examples of communication flows of consumption data. The purpose is to illustrate the complexity of data transfer between various parties in the smart metering system in a few typical scenarios.

3.1.1 Meter to IHD

The flow labelled 1 above shows the typical case where the IHD uses consumption data recorded by the meter for display within the premises.

3.1.2 Meter to Direct Third Party Service Provider

The flow labelled 2 above shows a case where the consumer has authorised a third party service provider direct access to the consumption data on the meter via a portal in the premises.

3.1.3 Meter to Indirect Third Party Service Provider

The flow labelled 3 above shows a case where a consumer has authorised a third party service provider indirect access to the consumption data via the primary service provider who has access to the consumption data on the meter. This would require brokering a three-way authorisation.

3.2 Clause and figure comments

3.2.1 Section 2

3.2.1.1 Clause 2.5

The authors agrees that the strong security background and track record at the transmission and distribution level needs to be acknowledged but does not agree that it provides a foundation to build upon for the required changes for smart metering. The one clear difference between a smart meter and an existing meter is a communications network, both into the home via a HAN and to other parties (suppliers, network operators and other third parties) via a WAN. On that basis, the foundation for security must be based on the security applied to communications networks, not that applied to electricity and gas distribution networks.

3.2.1.2 Clause 2.8

The clause says that 12 months of data is stored. Presumably this only refers to the half-hourly consumption data as described in the Statement of Design Requirements, however the clause also mentions additional data such as power quality and 'other key parameters'. On this basis, the author feels that more clarity is required regarding the data stored in a meter, its persistence and to whom it is accessible.

3.2.1.3 Clause 2.14

The author believes that the detailed data collected through meters indisputably reveals information about a consumer's habits and therefore the phrase 'has the potential to' is not strong enough.

3.2.2 Section 3

3.2.2.1 Clause 3.4

It is possible that the requirement to minimise data collection is in conflict with the requirement for a smart meter to store half-hourly consumption data for 12 months. If there is a clear reliable delivery mechanism from the meter to the various consumers of the data held within, there may be an argument for limiting the amount of data stored in a smart meter.

3.2.2.2 Clause 3.8

To some extent, if the consumer is considered the owner of the consumption data, it is difficult to apply safeguards and restrictions to which third parties the consumer negotiates with. Any imposition of restriction from the data custodian may well be considered to be a breach a freedom of choice regarding what a consumer is able to do with the data he or she owns.

If the third party is requesting the data from the service provider then three-way authorisation must be in place.

3.2.2.3 Clause 3.12

It depends on what is meant by “smart metering data”. It is likely that industry will want access to all the data on a smart meter or conversely the smart meter would only collect data the industry requires. It is possible industry would also want access to additional information from other devices in the home but this clause makes no such distinction.

3.2.2.4 Clause 3.19

If the consumer is considered to own the data, it is difficult to put a qualification on the data collected through a meter being used for legitimate purposes only. For example, consider the following unlikely but nevertheless possible case achievable now where a consumer points a video camera at an electricity meter and then broadcasts the results over the Internet using a webcam. Any third party would potentially be able to use this information for whatever means. Would this be considered illegitimate use of meter data and would the consumer be liable for prosecution? It would seem unlikely, as the consumer would argue it is their data and they are at liberty to do what they like with it.

3.2.2.5 Clause 3.20

Again, this clause tends to suggest that unless the data is anonymised in some way, storing half-hourly consumption data for 12 months may be too long. Anonymisation of data stored in a meter is difficult to do by virtue of the fact the meter is inextricably bound to a premises.

3.2.2.6 Clause 3.23

A question arises as to whether the consumer would be able to access all metrology data collected by the meter. Some of this data may not necessarily be for consumption purposes but for, e.g. grid stability. Would the consumer have a right to access this data as well, even if its usefulness in a domestic scenario was limited?

3.2.3 Section 4

3.2.3.1 Clause 4.3

See section 3.2.1.1

3.2.3.2 Clause 4.3

It is not clear to the author how security by design principles as outlined in Appendix 2 clause 1.3 ensure that security is built into the smart metering systems and processes from the start of the programme. Security by design needs a much more comprehensive and rigorous description than the one given.

3.2.3.3 Clause 4.5

There is no description of what the risk-based approach is and the statement itself is insufficiently clear.

3.2.3.4 Clause 4.6

There is not enough detail on the contents of the risk assessment undertaken or the identified outputs from the risk assessment.

3.2.3.5 Clause 4.7

The meta-process for refining the risk assessment process needs more detail.

3.2.3.6 Clause 4.8

The identification of only two key risks seems rather incomplete in comparison, say, to some of the studies done in the USA from the [UCAIUG AMI-SEC group](#) and the [NIST CSWG](#).

3.2.3.7 Clause 4.9

It is not clear why there is no transparency regarding the risk assessment and the results are only available to certain stakeholders under controls. The information from a risk assessment should not in itself compromise the security of any systems. "Security by obscurity", in any shape or form, is not the way to move forward.

3.2.3.8 Clause 4.10

Certain critical components (e.g. meter) do need to be adequately protected from tampering but it is better to design the system on the basis that in-premises devices can be tampered and will be compromised. This requires a loose coupling between these in-premise devices and the smart metering system, decoupled at the meter/ESI (energy services interface).

Ensuring that security events are detectable and that incidents can be managed appropriately cannot be assumed as a requisite for security policy. The first thing an attacker will attempt to ensure is untraceability. This is evident in sophisticated methods in computer security, e.g. rootkits.

3.2.3.9 Clause 4.12

The bullet point unsurprisingly lists every interface on the diagram. What is needed is a qualification for each interface. This activity has been undertaken by the [SG Communications](#) subgroup in the UCAIUG and is also explained in the NISTIR 7628 Cybersecurity report produced by the NIST CSWG.

3.3 Questions from Data Privacy and Security

3.3.1 Question 1

Do you have any comments on our overall approach to data privacy?

The following statement is presented in the prospectus:

"The customer shall choose in which way consumption data shall be used and by whom, with the exception of data required to fulfil regulatory duties."

This statement does not clarify the owner of the data or the custodian of the data. This is complicated in the case of a Smart Meter:

- The Smart Meter premises equipment will typically be owned by the DNO
- The customer will be the owner of the data pertaining to consumption on the Smart Meter
- The energy retailer or more likely the DCC will be the custodian of the data pertaining to consumption on the Smart Meter.

These statements only start to show the complexity with regard to ownership and custodianship of the consumption data and the surrounding legalities.

The author recommends that the practices undertaken in the telecommunications industry with regard to CPNI (Customer Proprietary Network Information) should be analysed and considered in relation to Smart Meter data as there are clear similarities.

The does however agree with the engagement with a number of groups and standards bodies for further guidance, especially with regard to the NIST SGIP activities which the author has participated in.

3.3.1.1 Recommendations

1. Clarify ownership and custodianship of all smart meter data

3.3.2 Question 2

We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

The author has no particular comment on this question.

3.3.3 Question 3

Do you support the proposal to develop a privacy charter?

The author supports the proposal to develop a privacy charter on the basis that this is a new scenario with regard to data ownership and custodianship and therefore may well not be completely covered in existing charters.

3.3.4 Question 4

What issues should be covered in a privacy charter?

The author considers at a high level that the following points are important. There may well be other points which are equally or more important but the author would need to perform a more detailed analysis of existing studies to identify these.

- Information access model
- Granularity of user data
- Content of user data
- Anonymity
- Indirect third party service provider negotiations

3.3.5 Question 5

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

The author considers that the high level aspects with regard to ensuring the end-to-end smart metering system is appropriately secure have been touched on but there is a lot more work needed

3.3.5.1 Recommendations

1. Look carefully at the existing work done in the US under the NIST CSWG and analyse the NISTIR 7628 document
2. Look carefully at the existing work done in the US under the UCAIUG AMI-SEC group
3. Develop more detail regarding security analysis, for example:
 - Detailed analysis of system topology

- Identification of information flows
- Threat models of typical system scenarios
- Identification of ingress and potential attack points
- Determined required security on information flows and equipment based on the outcome of the threat analysis