SMART METERING IMPLEMENTATION PROGRAMME: A CALL FOR EVIDENCE ON PRIVACY AND DATA ACCESS (AUGUST 2011)

BAE SYSTEMS DETICA RESPONSE

13 October 2011

Copy 1

10 pages including cover

Detica

BAE SYSTEMS

LIST OF CONTENTS

CONFIDENTIALITY

All information in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without prior permission in writing and shall be held in safe custody. These obligations shall not apply to information which is published or becomes known legitimately from some source.

Many of the product, service and company names referred to in this document are trademarks or registered trademarks. They are all hereby acknowledged.

1 INTRODUCTION

Purpose of this document

This document contains BAE Systems Detica's answers to the specific questions posed in the Smart Metering Implementation Programme: A call for evidence on privacy and data access (August 2011) consultation document.

The SmartReach consortium partners, BT, Arqiva and BAE Systems Detica, have collaborated closely in answering the questions for this consultation. The answers provided in this response by BAE Systems Detica are therefore identical to those provide by BT or Arqiva. SmartReach has only answered questions where SmartReach is well placed to provide comments and we have not sought to address questions more pertinent to energy suppliers or other stakeholders.

2 OUR RESPONSES

This section includes our responses to the questions set out in the "A call for evidence on privacy and data access (August 2011)" consultation.

Ref	Response
1.	Please submit any further evidence, such as surveys or consumer research, regarding privacy issues and smart metering. In particular is there evidence available about the effects of the availability and aggregation levels of more granular data (for example daily)?
	No comments
2.	To what extent would different rules for access to data between suppliers and third parties be expected to impact on the development of an energy services market (in terms of product and tariff innovation and / or entry to the energy market by third parties)? What are the particular data uses to which these concerns apply?
	No comments
3.	Are there any data uses, apart from those set out below, where the arrangements for access to data could have an impact on the benefits of the programme. How does this analysis differ for the gas market?
	No comments
4.	What types of energy services and energy advice could be provided by the market (by suppliers and / or ESCOs / potential new entrants) that require access to specific levels of data? What level of data granularity (frequency, time-lag) are needed to provide such services and what is the potential impact of these services in terms of percentage energy savings? Please provide empirical examples and explain the basis of any assumptions and distinguish between gas and electricity.
	No comments
5.	Should theft management be considered a regulated duty for which suppliers should have access to a certain level of smart metering data? What level of data would be required and how would this be used to manage theft? Please provide practical examples.
	No comments
6.	Does data need to be collected from all customers all of the time, for theft management, or could there be a trigger for accessing more detailed data (for example where theft is suspected)?
	No comments
7.	What level of take-up of time-of-use tariffs could be expected under different scenarios for access to data? What information is needed to design time of use tariffs? In particular would sample or anonymised

	data be sufficient?
	No comments
8.	Do you agree that individual half-hourly data is not currently required for suppliers to meet their obligations in relation to settlement? Over what timescale are any changes to settlement likely to take place and what might the implications be in terms of data requirements?
	No comments
9.	How far would aggregated or sample data provide suppliers' with what they need in the area of wholesale hedging? Please provide examples of how the data would be used and where possible quantify potential benefits and costs.
	No comments
10.	What level of data would be required and how would this be used to manage debt? Please provide practical examples.
	No comments
11.	How would suppliers envisage using daily data to support debt management and what evidence do they have to support claims of additional savings that could be achieved with access to daily data as opposed to less frequent data?
	No comments
12.	How could smart metering data be used to identify and protect vulnerable consumers? Should such activity be considered a regulated duty and are any licence changes needed to create particular duties on suppliers in this area?
	No comments
13.	Do you consider that use of data by network companies to support them in maintaining an efficient and economic network should be considered a regulated duty?
	No comments
14.	Do you agree with the requirement for such data to be anonymised or aggregated wherever possible, and how should this be monitored?
	We believe the SMIP must ensure any data required for regulated duties needs to be anonymised and aggregated where possible. The SMIP should also ensure that the data is not excessive, remains fit for purpose and aligned to the DPA 1998. In addition, the SMIP must ensure that any anonymised data retain its accuracy. Monitoring of anonymised or aggregated data should be required by assuring compliance to monitoring requirements as defined by the SMIP.

15.	Would suppliers be expected to advise consumers of network company usage of data given network companies do not have a direct relationship with customers?
	No comments
16.	Are there any alternatives to a basic opt-in or opt-out approach to consumer choice such as some form of prompted choice? What are the practical and consumer protection considerations in relation to different options(for example when and how)? From a consumer perspective what alternative approaches and vehicles (for example letter, email, phone) to seek customer consent are there?
	Any contract or service agreement must be written with fairness in mind to the consumer by ensuring all opt-in or opt-out statements are: • clearly written and must clearly articulate what data purpose the consent is being asked for; • preventing double negative questions such as “not, not”; • a proactive action rather than a default tick option. In addition, opt-in or opt-out statements should be done at time of contract and not during the installation process as consumers must be given time to consider their responses without any distress caused to the consumer. Further to this, we believe that consumer consent, for any usage of data, at point of install would not be feasible as the installers would need additional training to carry out these important responsibilities. Should SMIP and the suppliers decide to use prompted choice then the choice must be clearly explained to the Data Subject making them fully aware of the implications of agreeing or disagreeing.
17.	What evidence is there of likely take-up rates that could be achieved through different approaches to consumer choice?
	No comments
18.	What current and future technical options exist for energy consumption data minimisation / privacy enhancing technologies? How might aggregated or anonymised data be provided in practice? Would this imply additional services to be provided by DCC?
	There are many current and future technical options that exist which could be used for achieving data minimisation of consumption data, for instance data attributes can be filtered and anonymised according to configuration rules provided by a ‘data firewall’ that can redact (process to censor or obscure parts of text or data for legal or security reasons), encrypt, transform and reassemble data exchanged across multiple parties in the smart metering system. In practice to allow for flexibility in data transfer to multiple parties, data can be aggregated or anonymised by multiple configuration

	techniques, including, but not limited to: encryption, decryption, hashing (is a number generated from a string of text where the hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value), tokenisation (process of breaking a stream of text up into words, phrases, symbols or other meaningful elements), redaction, filtering, masking and validation. We believe that aggregation or anonymisation of data by using the techniques described above should be undertaken by the DCC directly or sub contracted out to a third party within their control.
19.	What parts of the privacy policy framework do you think should be delivered by regulation and why?
	No comments
20.	What is the most effective way to set out any sector specific protections around privacy (e.g. licence conditions or other alternatives)?
	We believe that a common approach to how privacy is presented to the consumers / Data Subjects (a living individual who is the subject of the personal information as defined by the Data Protection Act 1998) must be followed across the energy industry by energy suppliers, third parties or others organisations interacting with Data Subjects, however the industry could agree energy specific interpretations of the DPA if required. An example of such a common approach could be the adoption of consistent question structure and format for opt-in and opt-out statements in Terms and Conditions sections. Specifically for technical privacy measures, we believe that a similar approach should be adopted by ensuring that common standards are followed to facilitate consistency across the energy industry. Further to this, common technologies should be used to minimise interoperability issues across the energy industry as this should lead to reduced privacy breaches by parties in the smart metering system through unmanaged risk, unidentified issues or process errors.
21.	What practical options for authentication would provide the right balance between allowing easy access to consumer data in the home while providing the necessary privacy protection? Are there any other issues or options that the programme should be considering in developing the approach in this area?
	To ensure adequate security measures are in place to protect the privacy of Data Subjects proactive pairing of smart metering devices is required, such as IHD pairing to Communication Hub. This pairing can either be done by the installers at time of install or maintenance of the smart metering devices in the home or it could be done by the Data Subjects if they were to add additional devices to the Home Area Network which are over and above the default install.

	Any authorisation keys that would be required should be transported on a separate media controlled by the Data Subject, a trusted certificate-based third party system (e.g. Verisign that is used in internet based transactions) or another out of band mechanism, i.e. a different communications method to deliver the keys, e.g. delivered face-to-face, over the phone, etc. In addition, we believe that physical measures should be considered to protect the proactive pairing capability by using e.g. lock and key, special tools or tamper devices to hinder direct access to the physical authenticating and pairing component to ensure that any further pairing is authorised by the Data Subject after install. That said, the SMIP should ensure that the process for installing and initialising consumer HAN devices has suitable authentication and authorisation processes in place that are simple enough to be well understood during the install process by non-technical individuals. Finally, the consumers' interaction with the smart metering system will be through the HAN. We believe, this area presents one of the highest security risks to the programme and as such must be carefully managed by the SMIP. Consumers will have the ability to choose a range of different non-energy supplier provided In-Home Displays (IHDs) and associated services from various third party manufacturers which may cause interoperability and security issues. To achieve consumer authentication the SMIP could consider using two-factor authentication technologies.
22.	Are there other issues that need to be considered to make using the HAN a viable route for access to data in the home, from either a process or consumer perspective?
	The SMIP should ensure that if multiple bridges and technologies are used within the home, the Communication Hub must have the capability to keep these in separate logical security domains to avoid domains introducing risk to one another. Any data crossing these domain boundaries must therefore be authenticated, authorised and accounted for to ensure correct processing and integrity of the smart metering metrology data.
23.	What sort of arrangements would provide an appropriate balance between providing ease of access for consumers seeking to sign up to new services and adequate protection for consumers' data when accessed via DCC? Do you have any suggestions for alternative approaches?
	To ensure an appropriate balance between providing ease of access for consumers seeking to sign up to new energy services and adequate protection for Data Subjects' data when accessed via DCC, the SMIP needs to ensure that third party access is authorised by the consumer and that only relevant and not excessive data is shared.

	To achieve this, the DCC must be able to authenticate and authorise the Data Subject without going via their current energy supplier in case they feel distress / inconvenience - this is aligned to the principles set out in the Data Protection Act 1998 as the Data Subject may not want incumbent suppliers to be aware of their intention to switch services). Also any data transferred between parties must be accurate and up to date. In addition, the DCC must have a mechanism so that consumers have the ability to revoke consent given to third parties and that third parties do not retain any data if the consent has been revoked by the consumers. The consumers must furthermore have the ability to control the level and granularity of data they have granted the DCC or third parties.
24.	Are there other issues or options that the programme should be thinking about for the Foundation Stage or for non-domestic customers to facilitate access to data?
	We believe that for the Foundation Stage all eight data privacy principles from the Data Protection Act 1998 must be followed to protect consumers. Similarly, we believe that all eight data privacy principles from the Data Protection Act 1998 should be followed where appropriate to protect non-domestic customers before the enduring smart metering system is in place, i.e. to protect the individuals as these are the data subjects protected by the DPA irrespective of whether they are individuals trading or consumers.
25.	Do you have any suggestions as to how the Foundation Stage can be used to further learn about our approach to data access and privacy?
	We are firm advocates of using the Foundation Stage to gain insight and capture the lessons learnt of the various aspects of the smart metering system in preparation for the Enduring Stage by enhancing the Privacy Impact Assessment that we assume will be in place shortly. We would however, highlight that to maintain the privacy of consumer data and the lawful purpose under which the data was obtained, the SMIP needs to be careful that they do not change this purpose by getting access to the smart meter data for other purposes, unless the data is aggregated and anonymised or the Data Subjects have given explicit consent. We recommend that the SMIP should seek guidance from the Information Commissioner's Office (ICO) on how to ensure the smart metering Programme is compliant with the Data Protection Act 1998 in Foundation Stage when using captured data for lessons learnt which may not be the stated purpose of that data capture.

- End of Document -