Cambridge Consultants

Memorandum

To	Smart Metering Implementation Programme – Roll-Out team smartmetering@decc.gsi.gov.uk
cc	
Prepared by	Cambridge Consultants Ltd – [redacted]

Subject: Smart Metering Implementaion Programme August 2011: Response to a Call for evidence on data access and privacy, Reference: URN 11D/838

1 Introduction

This memorandum presents Cambridge Consultants response to the DECC:-

> "Smart Metering Implementation Programme: Smart Metering Implementaion Programme August 2011: Response to a Call for evidence on data access and privacy, Reference: URN 11D/838

Our response covers Questions 1 to 25. Direct responses to each of the questions are provided.

We have not considered certain questions. Theses are answered "Not Comment" indicating neither agreement nor disagreement with the stated position.

2 Response to the Questions

The numbers below correspond to the questions numbers in the Call for evidence document

1 No Comment

2 Restricting 'third party' data beyond the restrictions on energy supplier data seems to us essential to address privacy and data aggregation concerns. For instance the consumer may want to have the ability to 'cut off' a third party from their data, without necessarily being able to cut off their supplier from their data, which implies different access rules for third parties and suppliers. On frequency of data, we suspect that billing (suppliers) requires the least granular data, but third party innovative services may operate well with highly granular data. This implies different controls on third parties (for instance to enforce that granular data never leaves the home) vs. suppliers (who are allowed to have infrequent data sent from the home).

3 The distinction between local data (services that third parties offer into the home, via a website if they want, that make calculations on local data and give a local answer, without sending the data out of the home) and remote data (sent to and stored by the

third party linked to an online customer account, can be linked to all sorts of other data, sold on etc) is very important. This distinction applies to services run by both suppliers and third parties. The data uses suggested in other consultation responses could be tested against their suitability for local operation as a first cut on whether they will be privacy friendly.

4 No Comment

5 More granular data is clearly useful for Theft Management. Alternatively local systems could measure at a granular level and only send an alert if something was 'up'. This granular type of analysis does need to be directly traded off against consumer privacy.

6 An alert based on local analysis could certainly trigger more detailed data analysis

7 Time of use can be used at a local level by appliances, if they can access the currently applicable tariff across a 'bridge' or via a web service. We speculate that suppliers can use anonymised data to design the tariffs.

8 No Comment

9 No Comment

10 No Comment

11 No Comment

12 End to end identification of the individual consumer at the server side is useful for identifying vulnerable customers. This may imply more identification of the individual that is using the service by the supplier than is currently expected (household+account holder only). Perhaps extra assurances would be needed that this identification was 'opt in' or would not naturally be applied to all consumers.

13 No Comment

14 Yes, this sounds like a good idea.

15 Yes

16 This is where a universal identification system based on PKI comes into its own - with the right asymmetric PKI, a user's meter, or display, or other connected bridge, could list exactly which companies had access to their data (and which data), and with limitations, allow the consumer to turn on and off particular companies. This is

probably more applicable to third parties rather than the supplier which may be regulated to have access to data. This should be thought of as a constant availability of a service to see what companies can currently access data, rather than a once off 'opt-in' 'opt-out' decision. With a suitable user interface available (display, smartphone, web page rather than meter) a prompt to the user is certainly possible for specific choices, if they can be explained clearly enough.

17 No Comment

18 There are two upcoming techniques for privacy by design - portable data privacy, where privacy information accompanies all packets of data (but this needs to be standardised and built in at a low level into all systems), and homomorphic encryption, where various operations can be performed on data without having access to the data. Both of these require work before being suitable for widescale standardised adoption in smart metering.

19 No Comment

20 No Comment

21 Upcoming low cost pairing techniques from smartphone type devices to products involve push button pairing, authentication chips (in some peripherals), scanning a QR, Datamatrix, or similar code (Optical), or for NFC enabled devices such as smartphones, scanning a passive NFC tag. These techniques can identify the pairing to a remote server which can authorise the pairing (perhaps consulting the consumer via a web service) and send appropriate tokens/credentials back to the devices. For a bridging or HAN device to locally gain access to SMHAN in a secure manner without reference to a server, suitable security credentials would need to be pre-deployed onto the new device or a shared key (not a public serial number!) typed in to the device. ID Brokerage companies can comment on the suitability of a consumer device for running a full ID brokerage system between two federated security domains (likely to also require the online link).

22 Cambridge Consultants can comment further on this if required

23 A universally available web interface where the user can log in and observe which companies currently have access to their data (and possibly turn some of them on/off) would be a very useful addition to the system. This would be enabled by a universal identification system for smart metering companies (enabled by a PKI)

24 No Comment

25 The earlier the IDs and security are built into the system, the less expensive it will be.