

Cutting the Gordian Knot:

A Novel Solution to the Smart Meter Privacy Problem

Acute Technology Limited is pleased to submit this response to Ofgem's smart meter prospectus consultation.

We restrict our submission to a single topic: the role that "local processing" can perform in solving the data privacy problems that have been recognised by the smart meter programme. If not properly addressed the privacy issues will remain legal and political threats to the whole smart meter programme.

We note that the Dutch courts have found that the proposed Dutch smart meter programme violated the European Convention on Human Rights, as it mandated the export of an unnecessary level of privacy-compromising data. The same EU laws pertain in the UK, and so the UK smart meter programme is vulnerable to the same legal challenge.

Furthermore, the UK smart meter programme remains critically vulnerable to an orchestrated campaign targeting privacy deficiencies. You do not have to have a long memory to recall the damage done by irrational press campaigns targeting pay-as-you-drive road pricing ("spy-in-the-sky") and pay-as-you-throw rubbish collection ("chip and bin"). In Holland smart meters are referred to as "espionage meters", and in a sense they are.

Fortunately we are able to suggest an alternative privacy model for the smart meter programme, which:

- ◆ does not require the export of privacy-compromising raw consumption data from every home to a huge central database;
- ◆ instead, processes the raw consumption data within the home and exports only the processed data, dramatically enhancing privacy;
- ◆ intrinsically provides firewalls between different "authorised parties", so that each authorised party receives only the information that it is entitled to receive, so relieving the DCC from the onerous task of controlling access to the huge central database;
- ◆ does not compromise functionality or increase the risk of fraud;
- ◆ still allows consumers to share fine-grained consumption data with third parties, but only involving a process "informed consent";
- ◆ dramatically reduces the volume of data that needs to be transferred through the WAN communications channels and stored centrally;
- ◆ makes the system more distributed and thus reduces the risk that a security compromise at a single point could give an attacker control of the entire smart meter system and all customers' data.

How have we cut the Gordian knot of smart meter privacy? By recognising that smart meters which are truly smart can do all the necessary data processing within the home. And by identifying an existing set of technologies and standards that provide an elegant, secure and extensible platform to perform this processing.

We believe our proposal represents a good example of “privacy by design”, and commend it to the smart meter programme and to stakeholders.

Acute Technology is a member of the Project Hydra consortium, which is developing the technologies described in this response as part of a project to demonstrate the feasibility of deploying value-added services (such as telecare) on the smart meter infrastructure. The project’s website is <http://projecthydra.info>

The local processing architecture is described in an Appendix to this response. We advise readers to look at this Appendix first. We then answer a selection of the Ofgem Prospectus questions which have a bearing on privacy and security.

[REDACTED]

[REDACTED]

28 October 2010

Prospectus

Question 1: Do you have any comments on our overall approach to data privacy?

Ofgem are clearly aware of the potential for a poorly designed smart meter programme to leak personal data. This is evidenced by observations such as:

- ◆ “consumers should be able to choose how their consumption data is used and by whom” (p1, 3.11)
- ◆ plans to “assess all of the current and envisaged uses of smart metering data” and “assess where the data can be provided in an aggregated form” and “will ensure that it is clear why the data is required”.
- ◆ “minimising data collection, anonymising data where practicable, ... and ensuring data privacy and security is included in the detailed design” (3.4)
- ◆ “One of the key questions for the programme is to determine who has rights to access the data - and for what purpose.” (3.9)
- ◆ “We seek views...on what smart metering data, including the level of aggregation and frequency of it being recorded, should be...required by industry.... We would also like to understand where industry participants and interested third parties may wish to have access to information for other purposes” (3.13)
- ◆ adoption of a “security by design” approach (4.4, Appendix 2)
- ◆ perhaps strongest of all: “personal data will only be transmitted outside of the home where it is essential or where the consumer gives consent” (Consumer Protection document 2.32)

Ofgem’s evident unease is predicated on the assumption that to get the benefits of the smart meter programme fine-grained consumption data must be exported from every house and placed in a giant database run by the DCC. The privacy problem is one of controlling access to this database.

However, we believe that this assumption is unnecessary.

Instead, *by default the raw consumption data should stay in the meter*. Software running in the meter can process the raw data and export digested data to those entitled to it, such that the most sensitive personal information is no longer available in the digested form. Additionally, the fine-grained consumption data *may be* exported from the meter to entities who can process it to provide valuable services for the consumer, *but only with the informed consent of the consumer*.

Once this conceptual leap is made, the privacy problems essentially vanish. Knot cut.

We provide a detailed explanation of how this can be achieved in the Appendix at the end of this response “Local Processing – a Solution to the Data Privacy Problem”.

In-Home Display

Question 1: We welcome views on the level of accuracy which can be achieved and which customers would expect, in particular in relation to consumption in pounds and pence.

Ofgem suggests (in paragraph 2.20) that prepayment customers should be given accurate account balance information in near real-time but that credit customers need no more than monthly accurate balances (presumably estimated the rest of the time). Ofgem also seems to assume that the accurate account balance information will be transmitted from the DCC to the IHD (see also the Design Requirements document “credit balance update” service, p96).

We believe that there is no need to restrict credit customers to an accurate balance only monthly, nor for the transmission of credit balance information from the DCC. Our reasoning follows.

Prepay meters will need to deduct credit instantaneously and accurately based on a local calculation of energy consumption and a knowledge of the prevailing tariff. Since all meters can be credit or prepay, then credit meters will *also* be able to calculate the credit balance accurately and locally. The calculation is complicated somewhat by the need to account for VAT and standing charges (2.15), but these could be added into a billing calculation program that runs in the smart meter system in the home, for both credit and pre-pay customers.

There is no need for any communications to and from the DCC, in order for the DCC to perform these calculations centrally. The role of the DCC can be limited to downloading new tariff information infrequently.

The Appendix to our responses “Local Processing – a Solution to the Data Privacy Problem” provides further details of how this can be achieved.

Communications Business Model

Question 1: Do you agree that access control to secure centrally-coordinated communications, translation services and scheduled data retrieval are essential as part of the initial scope of DCC?

It is clear that communications to the meters must be secure and that management of the secure communications channel is part of the role of the DCC. As the actual communications channels will be provided under contract by telecoms operators the DCC must oversee these services.

The translation service proposition is predicated on the assumption that all meter data needs to flow into a giant database in the DCC. We do not accept this model as necessary or desirable. (See our answers to the Data Privacy and Security questions, and the Appendix at the end of our response “Local Processing – a Solution to the Data Privacy Problem”.)

We believe that it is practical and desirable to establish secure end-to-end logical communications channels between functions in the smart meter system and corresponding authorized parties such as energy suppliers, network operators and others. The role of the

DCC would thus be to manage the access to these communications channels for the authorized parties. A corollary of this model is that the DCC would not store or process the data as it traveled between the meter and the authorised party (unless this was a service which the authorised party contracted back to the DCC).

We do not accept that translation services should be required. The Smart Meter Design Group is charged with defining specifications for the smart meter system. As part of this we would expect that they would also specify the format of messages that travelled through the communications network. We would expect that there would be no more than one or two message formats. Consequently there would not be a need to translate data.

In any event, in the local processing model that we propose the messages from the meter to the intended recipients would be encrypted with a key shared between the meter and the recipient. So the DCC would not be able to read this data to perform translation, or other processing.

Scheduled data retrieval is a reasonable role for the DCC, provided that authorized parties may also initiate data reads when required. Most smart meter traffic will not be time-critical so a central scheduling process by the DCC is likely to make efficient use of communications resources.

Question 3: Should data processing, aggregation and storage be included in DCC's scope and, if so, when?

The orthodox view is that meters will deliver up half-hourly readings, that these will be stored in a huge database by the DCC, who will then (a) control access to this data by authorized parties and (b) perhaps process this data itself before passing it to the authorized parties. Amongst other things there are problems of privacy and access control to solve.

Our view is that an entirely different approach to data storage and processing is possible: a "local processing" model in which most of the data processing is done within the smart meter (or WAN module). Different sets of processed data can then be sent via the DCC to different authorised parties, encrypted with different keys for the different parties to ensure secrecy. There is no need for a central database at the DCC. The "data processing, aggregation and storage" operations that are behind this question can still be preformed, but differently. The DCC's role can be limited to controlling access to the communications channels.

The Appendix to our response "Local Processing – a Solution to the Data Privacy Problem" provides further details of how this can be achieved.

Data Privacy and Security

Question 1: Do you have any comments on our overall approach to data privacy?

We have provided our response to this question in our answer to Prospectus question 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.

Ofgem's concern here assumes that the DCC will need to receive regular shipments of raw data from every home in the country. They rightly observe that this potentially provides personal data about individuals living in these homes, and Ofgem are keen to minimize this personal data by, for example, aggregating data from many houses, or by reducing the frequency to the point where meaningful personal data is hidden.

Fortunately, we are able to suggest an alternative approach. In our answer to this question we give a single example, and elaborate on this approach in the Appendix at the end of this document "Local Processing – a Solution to the Data Privacy Problem".

Take the case of the need for the electricity supplier to receive payment for electricity supplied to a customer. The baseline assumption of the prospectus is that the smart meter exports half-hourly data to the DCC, which passes this data to the energy supplier, who applies the prevailing tariff to the consumption in each half-hourly time-slot, sums the 48 figures for each day over the period of a month or a quarter, then issues the bill to the customer.

However, if the smart meter also has knowledge of the tariff then the meter is able to perform this calculation locally. The meter needs to send only the monthly or quarterly total to the energy supplier. The end result is identical, and privacy is enhanced immeasurably.

Indeed, we note that the smart meter system will already be performing this local processing in the case of pre-pay meters, so it is a small step to have credit meters perform the same processing and send the monthly charge through the DCC to the energy supplier.

We will demonstrate how this can be done in practice, and how the same approach is able to deliver the other data for the industry (network operators, for example) to fulfill regulated duties, in the Appendix at the end of this response "Local Processing – a Solution to the Data Privacy Problem".

Appendix - Local Processing: a Solution to the Data Privacy Problem

Ofgem has correctly observed that smart meters have the potential to leak personal information if fine-grained data is exported from the meters. The Dutch courts found that this violates European data protection laws, and the same laws pertain in the UK.

Fortunately there is a solution.

The Prospectus documents assume that the smart meter system is not very intelligent, and must pass raw half-hourly consumption data to the DCC (and beyond) to be processed on central servers. This is an unnecessary assumption. Smart meter systems which are truly smart are able to process raw data locally and export only digested data from which privacy-damaging information has been removed. Let's consider some use cases showing how this will work.

Prepay Meters

Actually, the smart meter programme already knows that local processing will be needed for prepay meters. These meters must observe power consumption in the home, be aware of the tariff (perhaps a complex time-of-use tariff), and calculate the amount to deduct from the account balance. The same software will need to take account of emergency credit and friendly credit provisions, and perhaps implement trickle disconnect and time-limited disconnect algorithms. All this computing must be performed locally as it is important that the prepay meter isn't disabled by a customer blocking the WAN or HAN links.

So we observe that "local processing" is already a mandatory aspect of the UK smart meter programme.

Credit Meters – Billing by Energy Suppliers

The energy supplier needs to bill their credit customers monthly or quarterly. For this to work the supplier does not need the half-hourly raw data. It is sufficient that a software program running on the meter can monitor consumption, apply the tariff and accumulate the bill. This is just what the prepay meter software will be doing. Then once a month the meter system sends the accumulated total to the energy supplier, encrypted with a key known only by the supplier. The supplier issues the bill.

Note that the message is encrypted with the cryptographic key of the energy supplier, and can pass through the DCC without needing to be decrypted, stored or processed. Different suppliers would have different keys, and the gas and electricity data would be passed with different keys in dual-supplier houses. There is no loss of privacy. Data can only be decrypted and accessed by the intended recipient. And data throughput and storage are drastically reduced.

Accurate account balance data can be presented to the customer on the in-house display using local HAN communications alone (no need to involve the DCC).

Smart Grid

The distribution network operators might have a use for information on the quality of the electricity supply. Let us say that they are interested in how voltage and harmonics vary over the course of a week. Then a program running on the smart meter system can

monitor the raw data and accumulate minimum, maximum and average values over time. Perhaps once a week this digested information could be packaged up, encrypted with a cryptographic key belonging to the network operator, and sent on to the operator. Little or no privacy-damaging information is included in such a digest.

Again, the desired end is achieved without having to pass half-hourly data to a central server.

Energy Management Services

As Ofgem has observed, consumers could reduce their bills and energy consumption if they could receive advice from third-party energy management service companies who had access to the consumption data. This data *does* contain information about the lifestyle of the consumer, and Ofgem rightly notes that such data belongs to the consumers and should remain under their control.

But the customer might choose to share this data, which remains on the smart meter. If so, another program running on the meter could encrypt the data with a key belonging to the third-party energy management service company and send this to the company.

Indeed, it may be that the customer could get better energy saving advice if the exported data was finer-grained than the half-hourly readings. Some companies have developed “appliance inference” algorithms that can identify household appliances with poor energy efficiency, based on near-real-time data. Energy-saving recommendations based on these algorithms are clearly of considerable value to individual householders and energy supply stakeholders – yet they carry considerable privacy dangers. So this data should leave the home only with the informed consent of the householder, and only if encrypted so it can only be processed by the selected energy management services company.

Future Services and Future-Proofing

We can already see that there will be a demand for other services to be supported within the house: feed-in tariffs for micro-generation, management of heating and other load management operations, support of electric vehicles, water metering, and non-energy services such as tele-healthcare.

There is thus considerable merit in having a smart meter system that is expandable, and on which future programs can be installed in the future to deliver the required new services.

We expect that as each new service is identified it will be possible to devise a method of processing the associated raw data locally and encrypting it with a key shared with the intended recipient. If so then there is no need for privacy-sensitive raw data to be stored centrally by the DCC.

An Architecture

We hope that it has demonstrated that by performing local processing within the meter it is possible to retain privacy-sensitive data inside the home, which is where it belongs. Furthermore, such a scheme provides benefits beyond those that can be achieved by a simple system based on a central database of half-hourly measurements. For example, energy saving analysis could be improved and the smart grid supported easily; and the volume of data moved and stored by the DCC is greatly reduced.

The question is then the following. How can we deploy these various software programs into the smart meter system?

The answer comes from the banking industry, which has already solved this problem for smart cards. A set of standards known as GlobalPlatform (already ETSI European standards) address precisely the problem of securely managing the life-cycle of software running on smart cards.

The security requirements of the banking, mobile phone and pay-TV industries are very similar to those of the smart meter industry: to protect revenues in a hostile environment, and to allow new software applications to be dynamically and securely deployed at the remote device (be that the smart card, mobile phone, set-top box or smart meter).

The GlobalPlatform protocols are designed to manage software remotely. Programs from several sources can be installed on the smart cards, activated, suspended and deleted, all under the control of the card issuer. Firewalls between the programs ensure complete isolation of one program from another. And each program operates within its own “security domain” which allows independent logical secure communications channels to be established between each application and its corresponding off-card entity. Each channel can have its own set of cryptographic keys to optimise privacy. The same technology is used in mobile phone SIM cards.

It is important to note that this is existing technology that is deployed in huge numbers and which has stood the test of time. We are borrowing this technology and putting it to work in smart meter systems. Indeed, Project Hydra already well advanced in implementing a demonstration system.

The key technology components of the architecture are:

(1) Secure Microcontrollers

Secure microcontrollers are used in SIM cards, smart cards and pay-TV access cards. They include tamper-resistance features aimed at stopping hackers from copying or changing code and data. Importantly, the secure microcontroller protects the cryptographic keys. There are a significant number of known attacks against conventional microcontrollers – which we should expect hackers will try to use against smart meter systems. Secure micros are the first vital line of defence.

(2) GlobalPlatform

There must be a means of securely installing, personalising and managing the life cycle of software that runs on the secure microcontrollers. GlobalPlatform is an industry standard that allow multiple application programs (applets), from multiple vendors, to be deployed on secure microcontrollers. Thus a single secure micro can perform several different functions.

The architecture proposed here uses GlobalPlatform to dynamically and securely deploy multiple software programs onto smart meters.

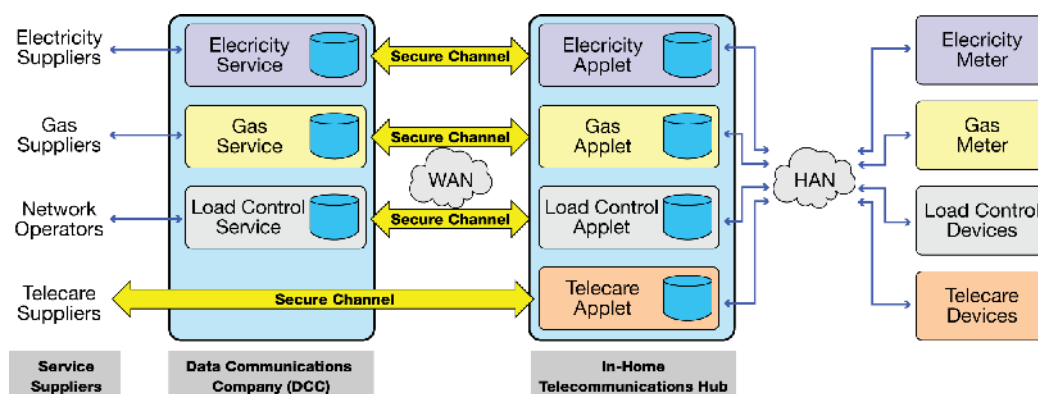
(3) Java Card

Java Card is a sub-set of the Java programming language, commonly used with secure micros and GlobalPlatform. Its design provides a secure environment for applications that run on devices with very limited memory and processing capabilities. Multiple programs (or “applets”) can be deployed on a single secure micro, and new ones can be added to it even after it has been deployed in the field.

Applets written in the Java programming language can be executed securely on smart

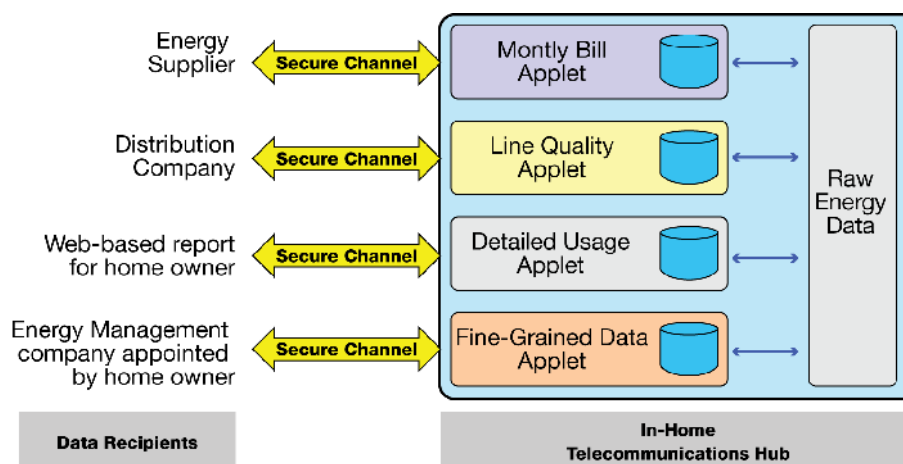
cards (or smart meter systems!) from different vendors.

The first figure below shows these elements in action in the Project Hydra technology demonstrator. The telecoms hub is implemented in a secure microcontroller running Java Card and GlobalPlatform software. Several applets run together, with their data separated by the intrinsic firewall features of the software architecture. The applets are managed remotely by GlobalPlatform server, and GlobalPlatform establishes multiple “secure channels” each with their own cryptographic keys. The data processed by each applet is sent to the corresponding data recipient, encrypted by a key shared only with the data recipient.



This figure suggests that the DCC might be the end point of secure channels for the energy suppliers, with the DCC taking on processing functions in behalf of these bodies. But of course the DCC might simply route the secure channels through to the energy suppliers, network operators without processing, as is shown for the telecare supplier.

The second figure shows the extension of this model to solve the data privacy problem. Here we see four different applets which each process the raw energy data differently, and dispatch it from the home to the intended recipient, over secure communications channels which are each protected by a different cryptographic key.



More detailed information is available at <http://projecthydra.info/technology>.

Security

Does the approach described here have poorer security characteristics? For example, we propose a billing application running on a smart meter that returns only a single monthly figure: the charge for the energy consumed that month. Could the computer program that calculates that bill be compromised so that it under-reports?

Careful consideration of the software architecture proposed will show that this is not the case. The measures to protect the billing application that submits the monthly charge are no more severe than the measures that are required to protect the raw data that would be exported to the central database. If you can trust that the raw data can be exported reliably then you can trust can monthly charge calculated in the home based on that raw data.

Indeed, by performing all of the processing within a tamper-resistant chip, which also protects cryptographic keys, overall system security is enhanced.

One final word is due on “tamper-resistant microcontrollers”. These are familiar as smart cards and SIM cards although any microprocessor can be built with tamper resistance – so we envisage a purpose-built secure microcontroller being used in smart meters, rather than a conventional smart card or SIM card. If the security architecture described here is implemented in a WAN module using GPRS radios then there is no need for a separate SIM card, as the SIM functionality can be just one of the applets. The good news is that adding tamper resistance adds only a small amount to the price of the chips.

Software Updates

A spin-off benefit is in the area of remote software updates and remote tariff updates. This is always likely to be a point of security weakness in a smart meter system. The whole design rationale of the GlobalPlatform standards is to provide a highly secure remote software management process. So the security problems of software and tariff updates are also solved.

Cost Implications

So this sounds all very promising. But won't it cost a lot more? Well, no actually.

We have already observed that the current-spec smart meter system needs to be able to process the raw data in the way we have described: to support the prepay functionality that must be present in every meter. Ofgem has noted that meters will be required to store 12 months of consumption data, and also notes the plummeting cost of chip-based data storage. And the need for software updates is mandatory.

So the smart meter system currently envisaged by Ofgem must calculate charges locally based on data that is stored locally, and be able to securely receive software updates from the DCC. These hardware features – no more and no less – are what is needed for the local processing operations described here.

In contrast, significant savings seem possible beyond the house.

For each operation described here the volume of data transferred across the WAN is substantially reduced when compared to the simplistic half-hourly reading approach. So too are the data storage requirements in the DCC – the need for the giant database of personal data is gone. Of perhaps greater value could be the reduction in system and management costs at the DCC if it no longer has to secure and administer access to the database.

Summary

We trust that we have demonstrated that, by “cutting the Gordian knot” the privacy problems of smart metering can be essentially eliminated. At the same time other benefits accrue: lower data transmission and storage volumes, better functionality, better security, and future-proofing. We look forward to discussing this in greater detail with Ofgem and stakeholders.