Smart Metering Implementation Programme: consultation on draft licence conditions and technical specifications for the roll-out of gas and electricity smart metering equipment (August 2011).

Smart Card Security for Smart Meters

A consultation response from Acute Technology Limited, October 2011

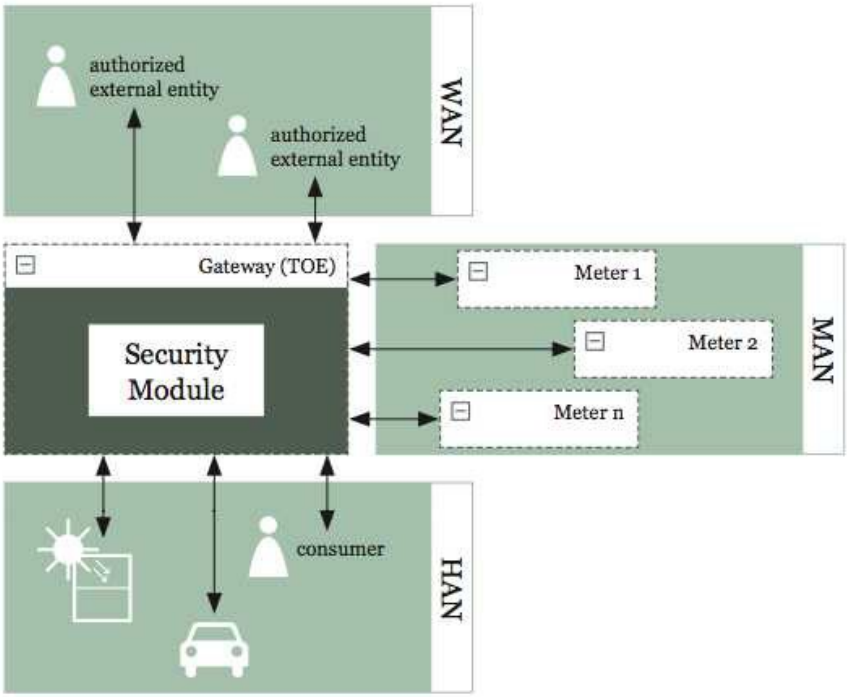
Introduction

Acute Technology Limited is pleased to submit this response to DECC's smart metering technical specifications consultation. In this response we are limiting ourselves to aspects of the security questions.

Acute Technology and our Project Hydra partners have been investigating reusing smart card security technologies for smart meters.

The approach has also been adopted by the German smart meter authorities.

The German Federal Office for Information Security recently issued the final draft of a Common Criteria protection profile for smart metering gateways. The profile defines minimum security requirements of future smart meter gateway devices to be used in household installations. The Gateway utilises the services of a Security Module (e.g. a smart card or equivalent secure element) as a cryptographic service provider and as a secure storage for confidential assets. The German system is shown schematically below.



This contrasts with the approach promoted by the UK smart meter manufacturers and utilities, which are resisting the use of secure elements on the grounds of cost. We have heard informally that STEG wanted to mandate a secure element in the IDTS security requirements but this was rejected by meter manufacturers and utilities.

We are one year on from the Stuxnet attack which showed that cyber attacks can disable embedded computing equipment, not just PCs. Considering the potential costs of security failures, we think that this “roll-your-own” approach to security is short-sighted in the extreme. Industry best practise is represented by smart card technology currently deployed in billions of smart cards and mobile phones. Smart meters deserve this level of security.

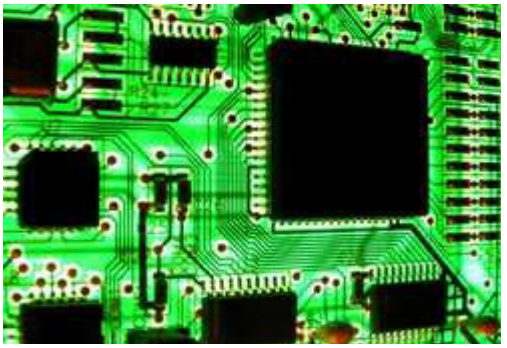
We urge DECC to mandate industry best practice when it come to smart meter security. It is not sufficient to leave security to market forces, since competition will eliminate hard security in a race to the bottom. DECC must regulate for hard security.

What's all this Smart Card Stuff Anyway?

Smart card technology is all around us, implemented in billions of devices we use daily. Some examples are shown below:

- Smart cards
- SIM cards
- Secure elements embedded in the NFC-enabled smart phones
- Soldered to printed circuit boards in embedded applications
- Electronic passports
- Oyster cards

Common to all of these is the “secure element” or “tamper-resistant microcontroller”.



The Need for Tamper-Resistant Secure Elements

Beneath the gold-plated contacts of the smart card or SIM card is a “secure element” - a microprocessor that has been hardened against a wide range of attacks. The attacks are designed to read or modify the code or data contained within the secure element. These tamper-resistant secure elements have evolved because conventional microcontrollers – those proposed by the UK smart meter manufacturers – are susceptible to these attacks.

Hackers have learn to attack conventional microprocessors by methods including:

- Running the chips at the wrong temperature or wrong voltage.
- Running the chips at the wrong clock frequency.
- Injecting faults, such as noise spikes, onto the chip's pins.
- Shining high intensity lasers at the chips.
- Monitoring in real-time the electrical noise emanating from the chips, or the power being consumed by the chips, to determine the data that they are processing.

It has been shown repeatedly that off-the-shelf microcontrollers can be attacked, and we should assume that smart meter microcontrollers will also be attacked in this way. Attacks might occur on any of the components of the smart meter system: electricity meter, gas meter, communications hub, and even in-home display.

An added threat is the possibility of trojan-horse software being installed during the manufacturing process. The threat if this should be considered very real as manufacturing of meters is likely to be done in low-cost foreign countries. In contrast, personalisation of the secure elements can be performed late in the deployment cycle.

To avoid these attacks, secure microcontrollers should be implemented in smart metering systems to store cryptographic secrets and to perform cryptographic operations.

Project Hydra's Work with Smart Card Technologies

Project Hydra (http://projecthydra.info) is a TSB-funded collaborative R&D project that has demonstrated:

- that it is possible to re-use the smart meter communications infrastructure to deploy value-added services into the home – in our case telehealth.
- that smart card technologies can be re-used in smart meters for privacy and security.

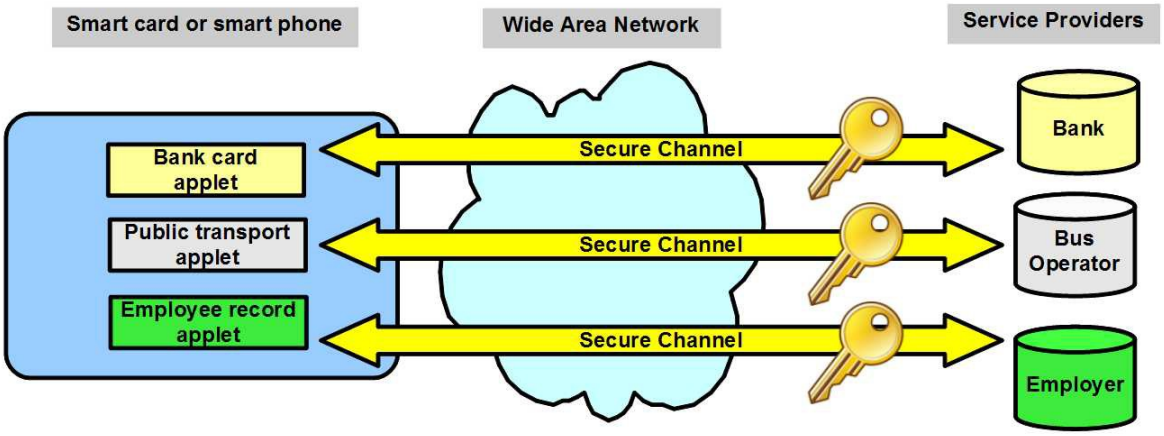
Acute Technology has submitted two other consultation responses covering the results of our work. The first, which is entitled "Whatever happened to Telehealth?", addresses support for value-added services within the Industry's Draft Technical Specifications. The second, "Local Processing – a Solution to the Smart Meter Data Privacy Problem", is a submission to the Data Access and Privacy consultation.

In this response we briefly summarise how we have found smart card technology can be used in a smart meter system.

First, there are three technologies we are using. These are all well-established smart card technologies, and are standardised, mainly by ETSI:

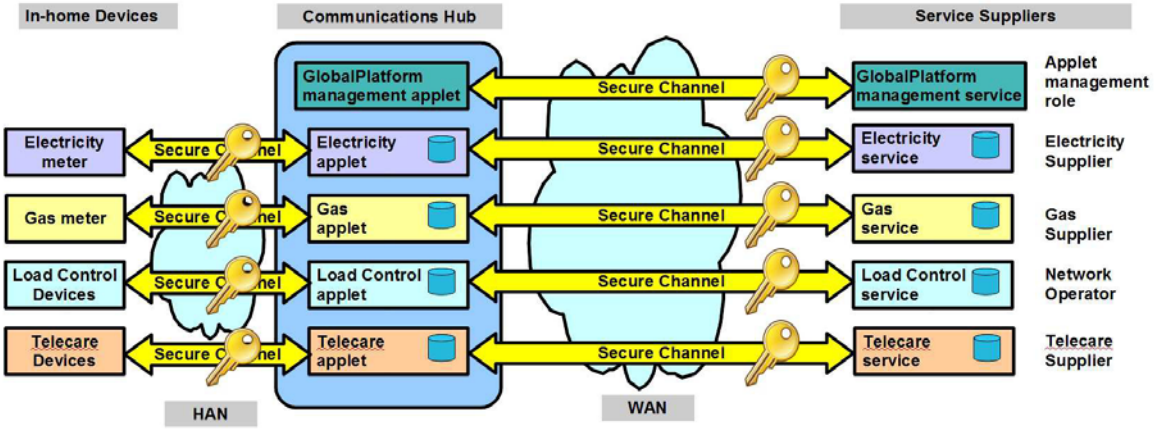
- Tamper-resistant secure elements (described above)
- The Java Card programming language, which allows multiple "applets" on a single secure element, separated by firewalls.
- GlobalPlatform protocols, which manage the applets remotely and securely, and which establishes multiple secure communications channels linking each applet to its corresponding server-side entity.

A conventional smart card implementation looks like this:



Each function has its own applet with its own separate secure communications channel to its corresponding server. The box on the left represents the secure element – a smart card for instance.

The next figure shows how this model can be implemented in a smart metering environment. It does not particularly matter whether the secure element is located in the smart meter or the communications hub, but the communications hub seems the better location, and this matches what the Germans are doing.

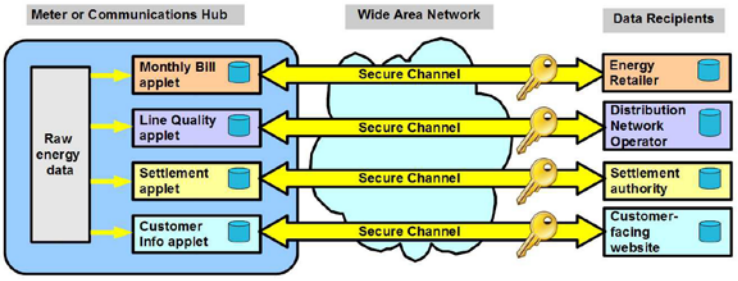


This diagram shows that each smart meter function could be implemented as a different applet. Each applet links to its own server-side entity (routed through the DCC, for instance). In keeping with the telehealth aspect of Project Hydra, we have shown that a new value-added service – here teleheath – can be implemented by loading a new applet to the secure element.

We find that this approach maps well onto the smart meter domain:

- The secure element provides the level of tamper-resistance that is missing from the conventional approach.
- Cryptographic keys and certificates are now stored securely.
- Cryptographic and security protocols are implemented by the security professionals at the smart card companies, and subject to the rigorous "Common Criteria" evaluation and certification process. This contrasts with the roll-your-own alternative.
- Meters can be provisioned with cryptographic material late in the manufacturing or commissioning process (as with credit cards and SIM cards), and the existing GlobalPlatform key management systems can be re-used to manage keys.
- Software updates no longer pose severe security risks as the well-established GlobalPlatform protocols for applet management can be re-used.
- Java Card is a "write once, run anywhere" language, so the same applet can be used in smart meters from any manufacturer.
- The system represents a general-purpose computing platform, so new functionality can be easily added after systems are deployed in the field, by adding new applets.

As a bonus, we discovered that Java Card applets solve the smart meter privacy problem, as described in our response to the Data Access and Privacy consultation. The next figure shows how multiple Java Card applets can process energy consumption data locally, within the home. Raw data does not have to be exported, so the privacy problem is solved.



Consultation Response: Answers to Questions

In the remainder of this response we provide answers to specific questions posed in the consultation. In this response we are limiting ourselves to some of the security questions.

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

Question 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.

Question 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.

Cryptographic Modules

SP.4 relates to the appropriate security requirements of a "Cryptographic Module" but specifies a level that falls short of a "secure element" such as those used in smart cards or SIM cards. SP.5 notes that "Core Devices will be installed in locations where they are vulnerable, therefore a compromise of a device is likely to occur. Steps should be taken to minimise the impact of a compromise on the end-to-end system" and suggests that a Cryptographic Module might be considered. SP.14 says "Core Devices shall store security credentials and supporting data in a secured area or Cryptographic Module."

We consider that the recommendations fall well short of industry best practice for securing smart meters. These are systems, after all, that will be protecting significant revenue streams, and will be capable of remote disconnection of electricity and gas supplies. It is inevitable that these will be subject to systematic threats from well-resourced adversaries, including foreign states. The protection of these assets deserves the application of industry best-practice. When security breaches occur, who wants to stand up and say "we knew there was better security available, but we wanted to save money"?

We recommend that tamper-resistant microcontrollers, or secure elements, are mandated for all Core Devices, for storing of cryptographic material including keys and certificates, and for performing cryptographic operations.

At minimum, secure elements should be mandated in the Communications Hub. SP.39 says "The Communications Hub needs to act as the local point of trust within the customer premises." It has important jobs including authentication, authorisation, and translation between the HAN and WAN security domains.

We note that the German authorities have already mandated the use of secure elements in the communications gateway of their smart meter systems. See "Protection Profile for the Gateway of a Smart Metering System" at:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile

End-to-end Security

Question 26 refers to the " End-to-end Smart Metering System" and this invites a search for the term "end-to-end" within the IDTS. It only appears as a modifier to "smart metering system". There is no requirement stated for any end-to-end security.

If DECC are interested in end-to-end security, surely messages should be encrypted as they travel between a smart meter and the back-end server. And the meter and server should mutually authenticate each other. Instead, it appears that the security architecture requires the Communications Hub to act as "the local point of trust" - see SP.39 and SP.41.

- DECC should consider whether the architecture proposed is compatible with the expression "end-to-end".
- DECC should consider mandating end-to-end security with secure elements in the **end** devices (meters and perhaps displays).
- If the Communications Hub must bear responsibility for the security within the home, then DECC should mandate the use of a secure element within the Communications Hub, with all cryptographic operations being carried out within this.
- DECC should study the security architecture of the smart card industry. This does mandate the use of secure elements (e.g. smart cards or SIM cards), and uses the concept of multiple logical secure communications channels between each application within the secure element and its corresponding server-side service.

This presentation is worth examining: "Smart Grid Security: network layer versus application layer dilemma" by Pierre Girard of Gemalto:

http://docbox.etsi.org/Workshop/2011/201104_SMARTGRIDS/05_SECURITY/Gemalto_Girard_SGSecurity.pdf

Question 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

Question 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?

The architecture proposed is inelegant. It stems from the desire by technology vendors to sell their existing ZigBee Smart Energy v1.x products. While ZigBee Smart Energy v1.x does a certain job within the HAN, its scope does not extend back to the servers, and this has resulted in the need for a translation layer within the Communications Hub.

Furthermore, the ZigBee HAN security domain is not built to extend back to the servers. This results in a further requirement for the Communication Hub to decrypt HAN messages and the re-encrypt them for transfer across the WAN.

See answers to Question 26 above in connection with end-to-end security, and the key role of the Communications Hub in the security architecture.

A more elegant solution would be to reduce the role of the Communication Hub and mandate end-to-end security and communications between the end points (meters) and the servers.

Here we suggest reusing existing architecture from the smart card industry. An application running inside a secure element on the meter can establish a logic secure communications channel all the way through to the server. See the introduction to this response for a description of how smart card technologies can be used within a smart meter system.

However, if the Communications Hub must translate between the HAN and WAN – both in terms of application level messages and cryptography – then the translation and cryptographic operations should take place within a secure element. The alternative approach (with conventional microcontrollers) makes the Communications Hub the obvious point for cyber attacks.

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

DECC proposes three options for Accreditation, Certification and Testing:

- a market-led approach
- a mandatory industry code and body to deliver and govern a testing regime
- a certification or accreditation scheme

In many technology domains accreditation or certification is carried out, with independent test houses applying standardised test processes to products submitted by vendors. This should be done for the smart meters as well.

We are particularly concerned that rigorous testing, including “penetration testing” should be carried out on the cryptographic aspects of the smart meter system. There is a danger that sound cryptographic protocols could be poorly implemented by vendors, resulting in the deployment of large numbers of devices containing vulnerabilities.

The smart card industry certifies its products using the Common Criteria evaluation approach. We suggest that this is adopted for the security aspects of the smart meter systems. Note that the re-use of existing smart card technologies, including existing secure elements, will reduce the work involved with this accreditation process.

Reuse of this well-established and well-tested technology will also improve the quality of the security deployed in the smart meter systems.

We note that the German smart meter programme is adopting Common Criteria evaluation of their smart meter communications gateway. See “Protection Profile for the Gateway of a Smart Metering System” at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile

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

The security of the smart meter system depends on the integrity of the cryptographic keys. Asymmetric cryptography is preferred as this allows end points to mutually authenticate each other, and provides roots of trust.

DECC should note that the smart card industry already has an advanced key management infrastructure, applicable to supporting millions of remotely deployed devices. Also in existence are companies and systems ready and able to manage personalisation of devices and management of keys. It would be wise to reuse these technologies, systems, and expertise, rather than asking meter manufacturers to approach a steep learning curve and reinvent all of this again.

DECC should also be aware of the dangers that exist if certificate authorities (CAs) are compromised. This has happened recently, in the case of DigiNotar (see http://en.wikipedia.org/wiki/DigiNotar).

In the case of a smart meter system, if a certificate authority were compromised then it might be possible to fabricate messages that appeared to come from a trusted party. These could be sent to many thousands of devices.

An article by Professor Ross Anderson discusses the dangers of compromised certificate authorities, and proposes some options to ameliorate this, including multiple certificates within meters. See:

http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

DECC should ensure that the smart meter system is designed to accommodate the compromise of a Certificate Authority.

Question 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.

The DCC is the most logical entity to assume overall responsibility for administering security, including key management.

However this is an opportunity to make two or three related points.

The security of any system is likely to be improved if the entity responsible for security is also the entity that stands to suffer if the security is compromised. That way the proper incentives are in place. On this principle, security responsibility should rest with the energy retailers, who stand to suffer both financial loss and reputation loss in the case of security failures. It is not clear that the DCC or its subcontractors are properly incentivised, according to this principle.

We cannot avoid noting that the DCC does not yet exist. Yet the security architecture that it will be responsible for administering is being designed now, and furthermore it is being designed by a set of ad-hoc committees that will shortly be disbanded. This cannot be optimal. Can the DCC be expected to take responsibility for failures in a security system designed in this way? Will the Government grant it immunity for such breaches?

Finally, the broader issue of liability should be considered. In the case of a security failure, particularly a dramatic security failure resulting, say, in the disconnection of thousands of electricity and gas meters, who will bear responsibility? Here are some candidates:

- The energy retailers
- Meter manufacturers
- Manufacturers of Communications Hubs
- Chip manufacturers who supply ZigBee communications stacks
- The DCC
- The DCC's communications service providers
- The DCC's data service provider
- Members of the ad-hoc smart metering specification committees
- The Government

What will product liability clauses in supply contracts look like, and will anyone want to accept these?

The Government and the industry should consider not just the cost of smart meter security, but the cost of the failure, and plan accordingly. Best-practice security, please.