

PROJECT+HYDRA

An Architecture for Security, Privacy and Accountability in Smart Metering

This document describes methods by which security, privacy and accountability can be provided in a smart meter system. It draws on work being undertaken by the Project Hydra consortium, and expands on this work.

1 Project Hydra

Project Hydra is a collaborative R&D program part funded by the UK's Technology Strategy Board. The project will demonstrate the feasibility of using the smart meter infrastructure to support a range of value-added services. Our proof of concept demonstrator will transfer telehealth data – daily weight and blood pressure measurements – across the smart meter comms network to health care professionals, thus showing that the health of patients can be monitored remotely using the smart meter comms infrastructure.

The rapidly aging population is the motivation for exploring the ways that technology can be used in people's home to improve their health care and social care. There are benefits in using the smart meter infrastructure to do this remote monitoring. The network will be ubiquitous (in the UK every house in the country will have a smart meter by 2020), it will be reliable (users cannot switch it off accidentally or deliberately) and the costs of the infrastructure will be borne mainly by the energy suppliers. By extension, other value-added services can also be deployed. If one assumes that each value-added service will generate a revenue stream, then the extension of the smart meter system to support value-added services will improve the economics of the smart meter programme.

Project Hydra will demonstrate that it is possible to deploy new value-added services onto the smart meters dynamically and securely, while preserving the integrity of existing applications and maintaining a separation of the data between the different applications (such that health data will not be available to the energy supplier, and vice versa). Project Hydra will make use of existing technology from the financial services industry to do this. This technology is discussed in the next section.

2 Secure Microcontrollers, GlobalPlatform and Java Card

This section describes the secure microcontroller hardware that is essential to prevent attacks on computer hardware that is accessible to malicious actors. It then describes the GlobalPlatform software platform that is used to manage multiple computer programs that can run on these secure microcontrollers. Finally it discusses the Java Card programming language, which is commonly used to implement these computer programs.

The secure microcontrollers, and the GlobalPlatform and Java Card software model described here are mature and well tested, and are ripe for reuse. Since they have been designed for the financial services industry as one of the main users, and since they have been deployed in billions of smart cards and SIM cards, these technologies are an obvious choice for applications where protection of valuable assets, security, a standardised architecture and platform independence is required – as in smart meters for example.

2.1 Secure Microcontrollers

Secure microcontrollers are most commonly used in mobile phone SIM cards and in smart cards. They are also used as the cards that control access in subscription television receivers.

In all of these cases they are used to guard access to a valuable resource, where there could be a temptation to defraud the rightful owner of his or her money. Since smart meters measure commodities of value, and since pre-pay meters involve financial transactions, it is prudent to place electricity and gas meters into this category.

So what distinguishes a “secure microcontroller”? A secure microcontroller is designed to resist attack by malicious individuals who are attempting to read or change data or programs within the microcontroller, typically with the aim of stealing something.

The term “tamper-resistance” is often used in this context, and a list of counter-measures listed by Atmel (a manufacturer of secure microcontrollers) indicates the range of attacks possible:

- ◆ High and low voltage detectors
- ◆ High and low frequency detectors
- ◆ Temperature detectors
- ◆ Illegal access code detection
- ◆ Illegal opcode detection
- ◆ Tamper monitor
- ◆ Non invasive attacks: side channel attacks, fault injection attacks
- ◆ Invasive attacks: reverse engineering, microprobing, laser attacks

The secure microcontrollers typically include hardware functions to facilitate security operations:

- ◆ Secure memory management, access protection
- ◆ True random number generator

- ◆ CRC engine
- ◆ Hardware DES/triple DES or AES
- ◆ Crypto-processor and elliptic curve options

It is worth noting that while secure microcontrollers are usually manufactured in the familiar SIM card or smart card formats, they may also be implemented in conventional microprocessor packaging and soldered to printed circuit boards. In such manifestations they can include the full range of peripherals found on conventional microcontrollers.

It is inevitable that the new smart meter system will prompt new attempts to defraud energy suppliers. Successful attacks on smart meters will be potentially much more serious than those on existing meters, since they are networked, and thus potentially many meters could be attacked remotely. Regular visits to inspect the meters will cease. Since there is a proposal for meters to disconnect electricity and gas supplies under software control, extortion and terrorism also need to be considered.

Smart meter stakeholders would be well advised to draw on the experiences of the smart card community, and use the most secure hardware available inside meters as part of their security programme.

2.2 GlobalPlatform

To perform useful functions, there must be a means of securely installing, personalising and managing the software that runs on the secure microcontrollers. GlobalPlatform is an industry standard that does this.

The GlobalPlatform organisation was established by the main players in the smart card industry to establish standards for smart cards. It is derived from earlier work done by Visa for securing credit cards. Most of the rest of this section describes GlobalPlatform in terms of its use with smart cards, but the reader will see how these feature can be used for managing software on other secure embedded computing devices – such as smart meters. Similarly, in this section for “smart card” read “secure microcontroller”.

Amongst the GlobalPlatform standards is the GlobalPlatform Card Specification aimed at managing the life-cycle of smart cards themselves, and the application programs (applets) which run on them. The aim of this standard is to allow multiple applets, from multiple vendors, to be deployed on smart cards. Thus a single smart card could perform several different functions.

The GlobalPlatform Card Specification says:

The GlobalPlatform architecture is designed to provide Card Issuers with the system management architecture for managing these smart cards. Although GlobalPlatform is based on the paradigm that there is one single Card Issuer for a card, it offers to the Card Issuer the flexibility for managing an ever-changing array of business partners who may want to run applications on the Card Issuer's cards.

GlobalPlatform gives Card Issuers the power to manage their cards with the ultimate flexibility by enabling them to share control over part of their card with business partners. The ultimate control always rests with the Card Issuer, but through GlobalPlatform, the business partners of a Card Issuer can be allowed to manage their own Applications on the Card Issuer's cards as appropriate.

The Application Providers have their own “Security Domains” on the secure micro, which may manage the loading and installation of applications pre-approved by the Card Issuer. The multiplicity of Security Domains allows each Security Domain User’s security data (such as cryptographic keys) to be kept separate and private from that of other Security Domain Users and also from the Card Issuer. The Card Issuer has its own Security Domain.

Security Domains support security services such as key handling, encryption, decryption, digital signature generation and verification for their providers’ applications.

The Card Issuer and the Application Providers have corresponding “off-card entities” and GlobalPlatform allows for logical secure communications channels (“Secure Channels”) to be established between each of the on-card entities and their corresponding off-card entities for the secure exchange of messages.

When an Application Provider wants to install a new application (with the approval of the Card Issuer), its Security Domain verifies that the integrity and authenticity of application (using digital signatures).

Applications may call upon the services (listed above) provided by their associated Security Domains. This allows a separation of the application code from the cryptographic tools. It also allows an application to be associated with different Security Domains (and thus different off-card entities) from time to time without the need for changes to the application code or cryptographic functions within the application.

Typically, each application will communicate with its own off-card entity over a Secure Channel which is set up the the Security Domain. GlobalPlatform also provides tools to allow for:

- ◆ Authentication – this makes use public key cryptography, involving private keys possessed by by an application on the card and by its off-card entity to allow both parties to be assured that they are communicating with who they think they are.
- ◆ Message integrity – this makes use of Message Authentication Codes to allow the receiving party to be sure that the message has not been changed since it was sent.
- ◆ Privacy – this makes use of encryption to assure the transmitting and receiving parties that eavesdroppers cannot understand exchanged messages.

Cards, Security Domains and Applications pass through a number of life-cycle states. For example, an application can be loaded on the card (but not installed), or installed (but not ready for execution), selectable (that is, able to be executed), locked (temporarily disabled) or deleted. Transitions are managed by the Security Domains and the applications themselves, in accordance with privileges when stem, ultimately, from the Card Issuer. Optionally, off-card entities may receive “Receipts” which are digital signatures that show the life-cycle transitions have occurred. This allows off-card entities to synchronise their databases with the actual state of the card.

2.3 Java Card

Usually, but not always, the applications that run on the secure microcontroller are implemented as Java Card applets.

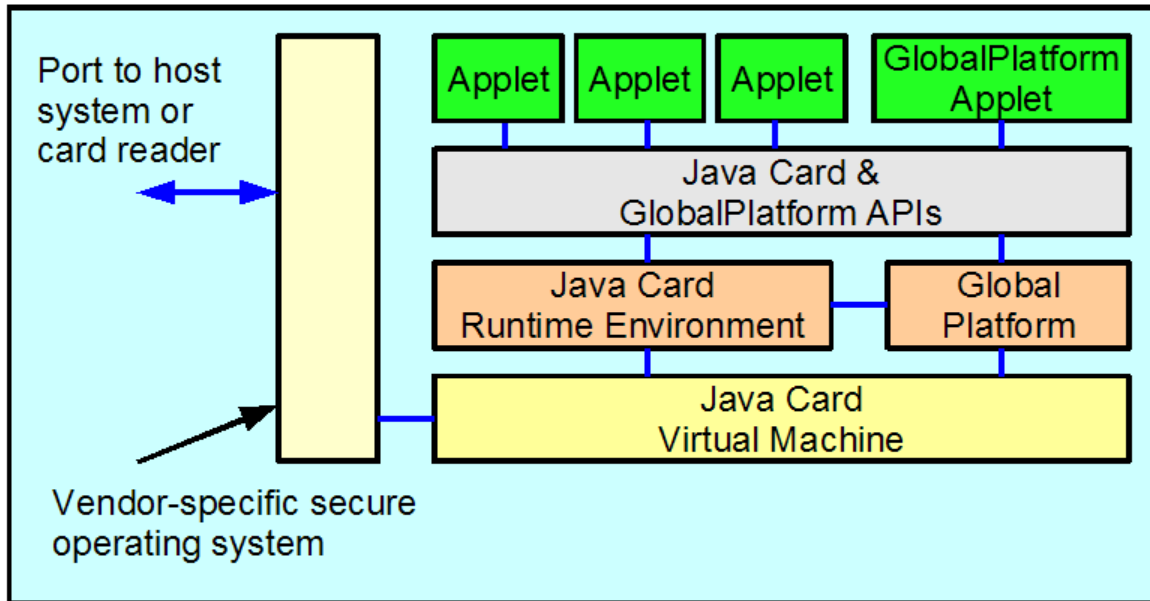
Java Card is a sub-set of the Java programming language. It provides a secure

environment for applications that run on smart cards and other devices with very limited memory and processing capabilities. Multiple applications can be deployed on a single card, and new ones can be added to it even after it has been issued to the end user. Applications written in the Java programming language can be executed securely on cards from different vendors.

Let us consider the advantages of using Java Card to deploy applications on secure microcontrollers. As you read this list, note how each point is equally applicable to both a credit card application and a smart meter:

- ◆ Java is a standard programming language – anyone who knows how to write a Java program can write a program for Java Card. Standard development environments and tools can be used.
- ◆ All the benefits of object-oriented programming – programmers have the benefits of code reuse, design patterns, and superior structure.
- ◆ Standardised development systems (such as Eclipse) provide good software tools, including tools to emulate and test the software before hardware is available.
- ◆ The secure microcontroller architecture, the security features of Java language and the controls imposed by the Java Card software stack make it possible for multiple applets to reside safely on a Java Card microcontroller. The number of applets is only limited by the amount of space on the microcontroller.
- ◆ GlobalPlatform provides standardised methods to manage the lifecycle of the applets, and of the card itself. Devices can be deployed in the field and additional functions added and updated over the lifetime of the device.
- ◆ Secure environment – Java is well known as a secure programming language. The Java Card architecture imposes a firewall between applets, and the GlobalPlatform standards manage the deployment of the applets. This provides automatic separation of the data belonging to each application, and guaranteed privacy of data as further applications are added.
- ◆ Platform independence – since Java Card applets are portable across different chip architectures, applets cost less to develop and maintain. This means that an application could be relied upon to work the same way on devices (smart cards or smart meters) from all manufacturers.
- ◆ Support for object persistence and atomic transactions is designed in. This removes from the designer the burden of having to consider what happens if the power fails in the middle of an operation.
- ◆ Security certification of the hardware/software combination which are typically evaluated according to Common Criteria for Information Technology Security Evaluation and ranked according to an Evaluation Assurance Level. This provides an independent evaluation and certification process of the security characteristics of a system.

The next figure shows the Java Card and GlobalPlatform software stack as implemented on a typical smart card.



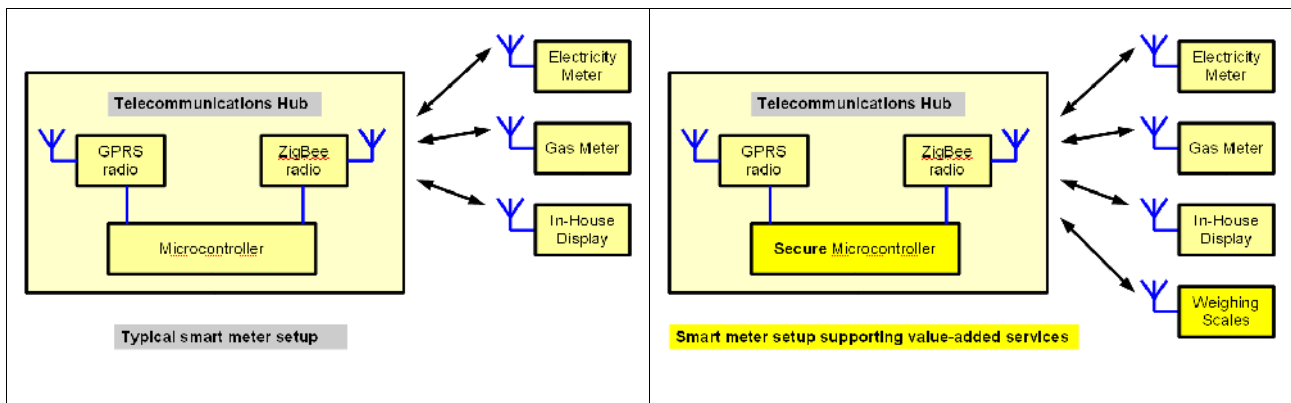
It is worth noting that a large proportion of mobile phones also use Java to deploy new functionality. In this case the flavour of Java is called "Java Platform, Micro Edition (Java ME)" (formerly J2ME). This is also a triumph for the philosophy of Java portability, since the same application can be written once and downloaded to mobile phones with widely varying levels of capability (screen size, colours, keyboard layout, sound capabilities etc). As more sophisticated phones arrive on the market the old applications can be expected to work without modification. This concept of standardisation is carried through to Java Card, and holds out the prospect of an individual program running on smart meters from any manufacturer.

3 Basic Project Hydra Architecture

The current expectation is that the UK smart meter system will involve the following elements within the home:

- ◆ Electricity meter
- ◆ Gas meter
- ◆ In-house display
- ◆ Telecommunications hub

All of these will be connected through a wireless home area network (HAN) and the telecommunications hub will include a wide area network (WAN) link to back-end servers. Examples of the HAN and WAN technologies are ZigBee and GPRS respectively. The first figure below shows this arrangement.

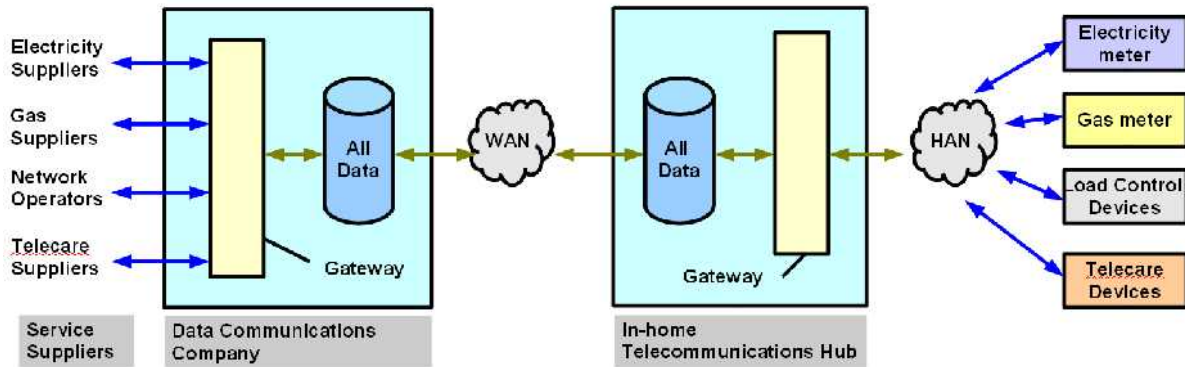


The second figure shows that Project Hydra extends this architecture by:

- ◆ Providing HAN links to other in-home devices, such as telehealth equipment.
- ◆ Using secure microcontrollers, GlobalPlatform and Java Card to add security and privacy, and for dynamic management of software.
- ◆ Each function that the telecommunications hub performs is performed by a different applet, each with its own cryptographic keys, and with each applet's data protected from the other applets by the firewalls enforced by the Java Card architecture. The applets are:
 - Electricity meter
 - Gas meter
 - Telecare/telehealth
 - Applets for other value-added services could be deployed later.

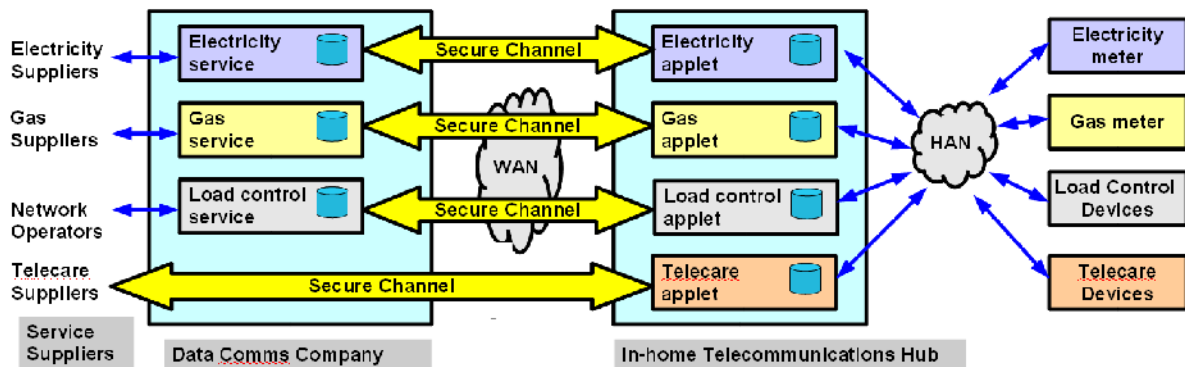
Let us now consider the privacy and data security problems that exist in a conventional approach to smart meter data handling, and how these can be addressed by the Project Hydra approach.

A conventional model (below) does not provide separation of different sets of data as it passes between the home, the communications network and servers of the Data Comms Company (DCC).



The Hydra architecture solves this. A single, well-tested security architecture – GlobalPlatform - is used throughout the smart meter system. Firewalls running on the secure micro keep each applet's data separate from other applets.

GlobalPlatform provides for a separate logical Secure Communication Channel between each applet and its server-side entity. Each Secure Communications Channel has its own cryptographic keys, so energy data can't be accessed by telecare suppliers, and health data can't be accessed by energy suppliers (or the Data Comms Company).



The GlobalPlatform architecture allows for dynamic management of the applets: new applets can be installed and old applets deleted. This is done under the auspices of the body taking the role of the “Card Issuer”, which can establish appropriate quality control over the applets. In a practical smart meter deployment this role could be taken by the Central Communications Provider or by another body.

Even leaving aside the benefits of the non-energy value-added services, this approach brings benefits to the smart meter stakeholders:

- ◆ Reuse of the well-tested secure microcontrollers/GlobalPlatform/Java Card technology.
- ◆ Separation of gas and electricity data.
- ◆ Secure mechanism for software upgrades and for altering tariffs.
- ◆ Mechanism to add support for new energy-related functionality, such as support for electric vehicles and home-based micro-generation.

4 Different Data for Different Stakeholders

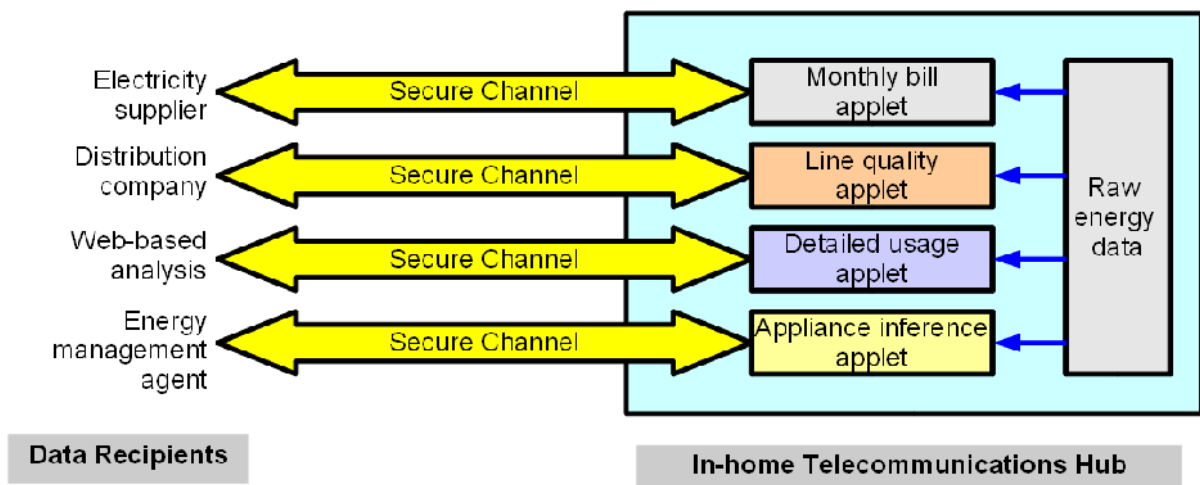
Smart meter technology is able to collect fine-grained information about the energy use patterns of householders, and it has been recognised that this poses potential privacy concerns. Rather than a meter reader visiting once a month to obtain a single energy consumption reading, the smart meters can tally energy consumption in 30-minute chunks, or even more frequently. This could be misused, for example to:

- ◆ Establish when the house is empty, or when it is likely to be empty.
- ◆ Infer information about the social behaviour of the occupants.
- ◆ Infer what appliances are in use in the house, and the pattern of their use.

The availability of extra data could have advantages and disadvantages. For example, it might be of use to the householder to receive advice on how to reduce energy bills based on an analysis of usage patterns by the energy supplier. On the other hand, some householders would find this intrusive, and energy suppliers could use the data to the disadvantage of the householder, perhaps by tailoring tariff offers to optimise profit. The threat to privacy could threaten the very viability of a smart meter system, either through a public outcry, or by legal challenge (as has happened in the Netherlands).

Fortunately, the Project Hydra architecture offers a solution to this problem. The same raw energy data could be processed by different applets within the smart meter, and the appropriate analysed data could be forwarded to server-side entities based on their need to know, and on commercial contracts between the householder and service providers.

The next figure shows four applets processing the same data on behalf of four different off-card entities.



For example, the energy supplier only needs to know that a householder has used energy to a certain value, calculated by an agreed tariff. The energy supplier can be assured of this if he receives a single monthly figure, cryptographically signed by an applet that implements a known tariff algorithm. Indeed, the energy supplier might well have written that applet and had it deployed onto the smart meter on its behalf. No fine-grained usage

information needs to be sent to the energy supplier. WAN data transfer and storage requirements are also dramatically reduced.

On the other hand, the householder might voluntarily ask for his energy consumption patterns to be monitored in further detail. For example, the householder might offer up further data to an “energy management agent” in exchange for advice on how to reduce bills or identify inefficient appliances that could be replaced. In this case another applet would be deployed onto the smart meter. This might send finer-grained energy data to the energy management agent, or perform analysis of appliance behaviour within the smart meter. The energy management agent might be the energy retailer, or some other organisation. The point is that this deeper inspection of energy use would be performed with the consent of the householder, under the terms of a contract agreed between the householder and the energy management agent. Data sent from this applet would be separate from the billing data sent to the energy supplier and would be protected by different cryptographic keys.

The householder might possibly enter into contracts with more than one energy management agent – one to provide detailed web-based energy consumption data and another to advise on replacing appliances, for example. Each would have separate applets, with the data secured by separate secure communications channels.

It is possible that the energy distribution companies would have bona-fide interest in some data collected by the smart meter. For example, analysis of voltage or harmonics on the electricity power line could identify fault conditions or help manage the grid. If it is established that such data should be made available to the energy distribution companies then this could be supplied by yet another applet, this time directed solely to the energy distribution company, and stripped of superfluous private data.

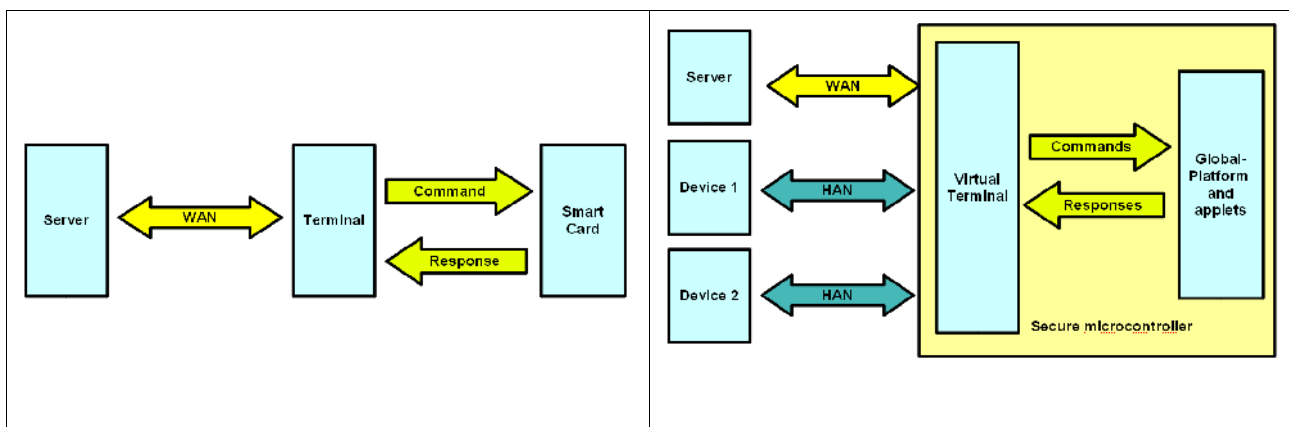
Another applet (not shown in the previous figure) could perform an audit function in the event that a householder queried his bill.

The source code of each of these applets could be made public. This would assure all parties that the operations being performed on the meter can in fact be trusted to do as they claim, and are not leaking any information above the minimum required, or cheating other stakeholders.

5 A Practical Implementation

It is worth considering a few points that relate to a practical implementation of the secure microcontroller, GlobalPlatform and Java Card technologies discussed in this paper.

First, there is a need to extend the current smart card communications model which is shown in the first figure below. This model is defined by ISO 7816. Current implementations of GlobalPlatform protocols involve a smart card (SIM card or credit card for example) inserted into a terminal (a mobile phone or a chip and PIN terminal in a shop). The terminal sends commands to the smart card which processes these and returns responses. As appropriate messages are exchanged between the terminal and a distant server across a WAN, to validate messages generated by the smart card. The smart card is the secure microcontroller; the terminal is typically not.

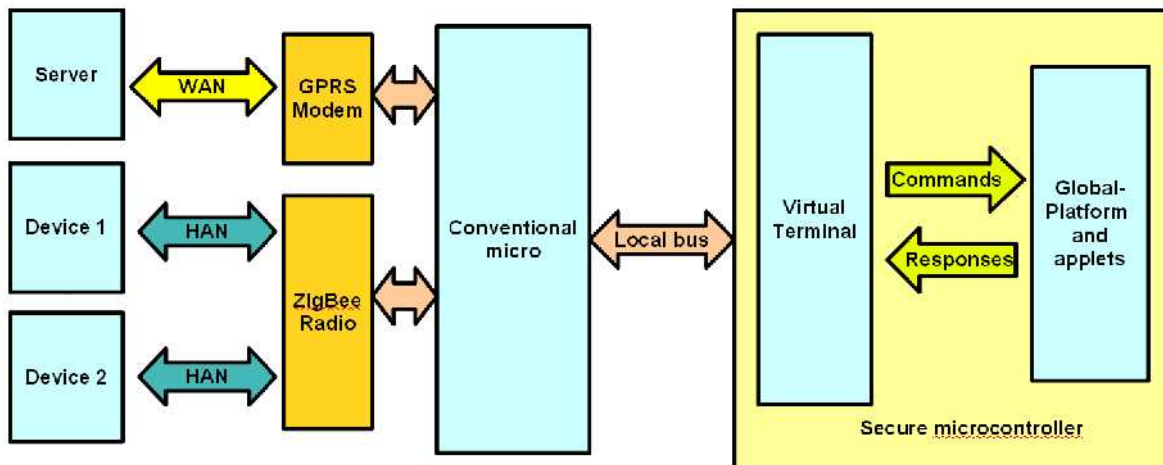


The Project Hydra architecture adds local devices which also need to communicate with applets – both energy meter devices and value-added service devices. Message flow is more complex as messages can be initiated by the server or by devices, and a message sequence initiated by one actor (the server for instance) might then require an exchange of messages with another actor (a device for instance).

The Project Hydra architecture adds a “virtual terminal” implemented within the secure microcontroller. This receives messages from local and remote sources and routes these to the appropriate applets using standard commands and responses. This is shown in the second diagram above.

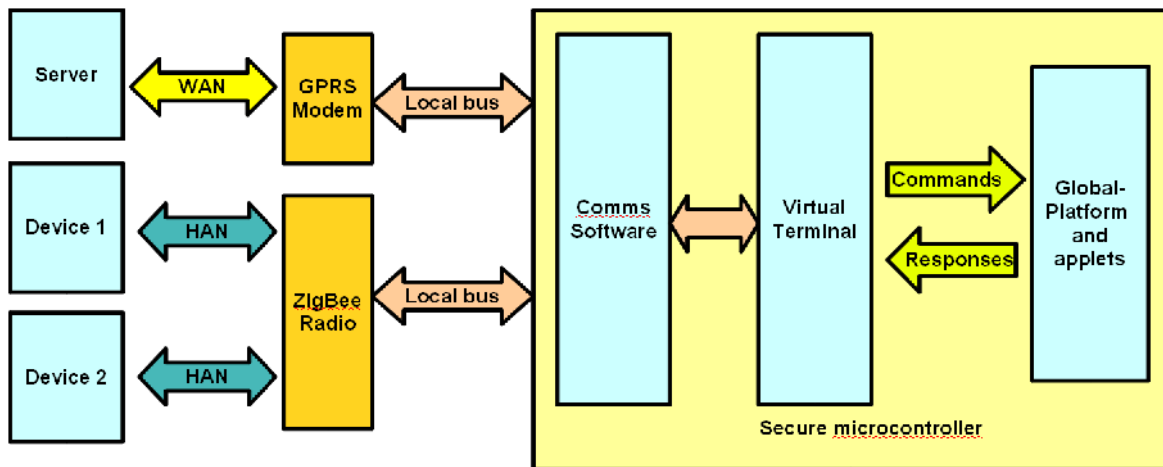
The overall architecture of the Hydra Telecommunication Hub in one implementation is shown below.

A secure microcontroller acts as a slave to a conventional microcontroller, which routes messages between the virtual terminal and the appropriate WAN or HAN communications subsystem.



It is worth noting that the SIM card conventionally associated with the GPRS modem shown in this figure can in fact be implemented as yet another applet within the secure microcontroller.

A second implementation is shown below. This dispenses with the conventional microcontroller. This pattern of increasing integration could be continued, with the secure micro chip eventually mopping up the WAN and HAN interfaces as well.



6 Summary

Security and privacy concerns could derail smart meter programmes.

There are real security problems that need solutions which draw on established security engineering principles and technologies. The problems include preventing fraud and protecting vital energy supply from attackers who would be motivated to disconnect supplies.

There are real privacy problems that also need to be addressed, with reference to established data privacy laws and good practise. The concerns relate to the release of data beyond that which is necessary for the task at hand. For example, does the energy retailer need data with 30-minute resolution in order to deliver a monthly bill? Does the government need this data?

To protect revenue, to protect national security, to satisfy data protection law and to keep the public on board, those who are implementing smart meter programmes must address these problems.

Fortunately they are not insurmountable. The Project Hydra architecture described here draws on well-established technologies that have been used successfully for many years. The approach described here reuses secure microcontroller, GlobalPlatform and Java Card technologies in a novel way to provide a high-quality secure computing platform within a smart meter.

Furthermore, the use of multiple Java Card applets and secure communications channels offers solutions to the privacy problems: raw energy measurements can be processed by code placed in the public domain for inspection, and the cryptographically signed results returned to authorised parties can be trusted by these parties. Thus, for example, the smart meter needs only release a single monthly billing figure to the energy supplier. Additional data could be released, but only with the permission of the householder, and only to parties that the householder contracts with.

Finally, by enabling the secure deployment and management of new application programs, the Project Hydra architecture provides an extensible platform capable of supporting a range of value-added services which will improve the economics of the smart meter programmes, and which will provide valuable services to householders and additional benefits to society as a whole.