Using Established, Proven Standards to Build a Secure Smart Meter Infrastructure

Abstract

The very need for flexibility in the global Smart Meter market could make it very difficult for vendors to build meters that comply with the varying levels of security and functional requirements for the Smart interface. The temptation is to cut back on security features to save on costs, simplify the infrastructure and reduce time to market. However, the very act of doing this potentially sabotages the very reasons for implementing a Smart Meter programme; accurate billing, managing demand, reducing fraud, cutting billing costs etc.

This paper compares some of the established and upcoming technologies and their suitability for building a secure Smart Meter infrastructure.

It will pay particular attention to secure devices which are emerging from other proven, established, high-value, high-security markets (particularly payment and Identification (ID)) and leverage already proven standards. MULTOS, an open, long-established, high-security operating system (and supporting eco-system) for secure microcontrollers has much to offer in securing Smart Meters and other Smart Grid devices and will be discussed in more detail.

MULTOS

Christopher Torr - Technical Manager
MAOSCO Ltd

Introduction

Let's be clear about this from the outset. Ordinary consumers, organized criminals, terrorists and even unfriendly nations WILL target smart meter infrastructures as they offer a unique opportunity for fraud, intelligence gathering and disruption.

As long as there has been electricity there has been a battle between supplier and the not-so-honest user. It only takes a cursory search on the Internet to find many reported examples of power theft. For example, between one-half and 2 percent of electricity in the U.S. is lost to theft, according to the U.S. Energy Information Administration [1]. In India energy theft has historically been endemic. As of 2013, nearly 20% of the electricity generated in India was lost to transmission and distribution losses, the majority of that being due to theft [2].

Huge financial losses for the power generation and distribution companies are of course not the only issue. Energy shortages due to theft result in blackouts with power-cuts being common, especially at peak hours [3].

Smart metering infrastructures finally offer the opportunity to detect fraud easily and remotely and make sure that power that should be paid for, is paid for. However, this is only true if the meters themselves are robust both physically and logically. Conversely, poorly secured smart meter infrastructures offer new ways for fraud and more serious attacks to be carried out, especially where meters are fitted with switches to disconnect the supply.

What constitutes a "smart" meter?

2012/148/EU Recommendation for smart meter minimum functionality:

Consumer

- *Provide readings directly to the consumer and/or any third party.*
- *Update the readings frequently enough to use energy saving schemes.*

Metering Service Operator

- *Allow remote reading by the operator.*
- *Provide bidirectional communication for maintenance and control.*
- *Allow frequent enough readings to be used for networking planning.*

Commercial Service Issues

- *Support advanced tariff system.*
- *Allow remote ON/OFF control supply and/or flow or power limitation.*

Security and Data Protection

- *Provide secure data communications.*
- *Fraud prevention and detection.*
- *Distributed Generation*
- *Provide consumed, generated, and reactive metering data.*

For this remote management to work smart meters need to have the following attributes:-

- A fixed, unique identity (that cannot be cloned or modified)
- Protection of sensitive data being sent from (e.g. readings, status messages) and to (e.g. top-ups and management commands) the meter.
- Methods for detecting and reporting of tampering with the meter (both hardware and software).

Essentially a smart meter is a networked computing device and the way that such devices are traditionally made more secure is through the use of cryptography. Cryptographic methods make it possible to guarantee authenticity, message integrity, privacy and non-repudiation BUT ONLY if performed at all stages in a secure manner.

Secure communications is not enough

Smart metering infrastructures consists of many interacting layers. The details of each layer vary depending on the topology and geography of any particular implementation, but in most cases each layer has some level of vulnerability somewhere, it is almost inevitable and practically impossible to eliminate every single risk.

Because communications mechanisms have evolved a level of security, one temptation is to rely solely on the security mechanisms of those layers. Whilst the cryptography involved is theoretically robust, there are common issues. Here are a few examples:

- Wireless protocols can be vulnerable to eavesdropping during pairing allowing keys and codes to be extracted [4][5].
- Placing any reliance on a Media Access Control address (MAC) as a form of unique identity is false as MAC addresses can be spoofed [6].
- Use of default or easily guessed keys, passwords and codes can make it easy to infiltrate networks
- Linux based devices may well (and in fact usually do) store network keys and passwords in the clear allowing them to be extracted and re-used. On Windows it is easy to access them also, especially with Administrator rights.
- Cryptographic functions carried out in general purpose micro-controllers and microprocessors are vulnerable to attack (e.g. key extraction, code modification, fault injection).
- The limited processing capability of some communications devices can mean that less than optimal algorithms and key lengths are employed.

Having just pointed out some of the issues it is still worth implementing these security protocols because the best defense is defense in depth. However, they should not be relied upon to provide the only protection.

PROBLEMS SECURING THE METER ITSELF

Accepting that security has to be brought into the smart meter itself, many issues still remain. A safe cryptographic scheme relies on at least five things:-

- Key sharing: must be done such that the clear keys used cannot be intercepted or modified.

- Key storage: any secret keys must be stored such that they cannot be read except by the programs using them.
- Cryptographic processing: must be done such that secret keys are not exposed, either directly or indirectly (through side channel attacks).
- The ciphers and associated keys being used are “strong”. i.e. the algorithms are proven and the keys are long enough to not be obtained through brute force.
- The code being executed has not been tampered with.

These requirements are not easily achieved by general purpose microcontrollers and microprocessors and are on top of the general remote management requirements listed earlier. Although a little dated, [7] is a good introduction to reverse engineering techniques which can be used to learn about applications and their data (including keys).

One argument is that if the meter is sealed, and tamper protected (for example with micro-switches or foil seals) that it does not matter if the internal device is not secure. However, this still leaves the possibility of the substitution of a modified clone device where the credentials are extracted from the original (which is effectively broken) and placed into the clone. The clone then operates as normal from an external viewpoint but is in fact compromised. Alternatively, with just the keys and credentials any computing device can be programmed to mimic a meter.

These kinds of attacks may sound extreme, but they are not. Spanish smart meters were found to be vulnerable to exactly these sorts of attacks [8] and the initial plans for the UK smart metering scheme were found to have extremely weak encryption [9].

Clearly an alternative solution is required. Happily none of the problems and requirements listed above are actually new problems. The world of electronic payments, ID and mobile telephones have been engaged with exactly these sorts of problems for the last twenty years.

AVAILABLE TECHNOLOGIES

Secure Elements (SEs) and SAMs

SEs are specialist microcontrollers that have hardware anti-tamper measures. They contain cryptographic accelerator hardware supporting standards such as RSA, ECC, AES, and SHA-2. Traditionally they have also had limited input / output capability so as to reduce costs and limit attack options.

SEs are used in smart cards, SIMs, mobile phones, passports and Security Access Modules (SAMs). A SAM is essentially a smart card, but typically cut into the same shape as a mobile phone SIM card. Alternatively SEs may be in surface-mount packages for mounting on a PCB, for example in smart phones.

An SE provides a secure physical and logical environment for the storage of keys (and other sensitive data) and a secure environment for cryptographic calculations. In a smart meter their typical use is for authentication of the meter and head-end system and encryption of the communications between them. It can also hold other sensitive credentials such as a unique serial number, customer information, and/or a limited amount of readings.

There are two classes of SE, those which run an application coded in the native environment of the host microcontroller and those that run a secure multi-application operating system (e.g. MULTOS or JavaCard) which in turn executes applications in a virtual machine. The benefits of the latter are that many of the logical security countermeasures required are built-in and do not have to be considered by the person coding the end application.

The advantages of using an SE are:

- They are relatively cheap.
- They consume very little power.
- They are a proven technology and already have security evaluations and certification in many cases.
- Some offer a guaranteed unique identity.
- Generally applications are easy to develop either in 'C' or Java.
- Existing smart card services can be used in a smart meter context.
- It may be used to help secure the boot of the main processor.

Some disadvantages include:

- Interface hardware between the SE and the rest of the smart meter may be required, depending on the overall architecture, increasing component count and cost beyond that of the SAM itself.
- SEs may only have very limited secure storage so may not be, for example, suitable for storing many key-pairs, certificates or meter readings over a long period

Trusted Platform Modules

TPMs are a form of SE in that they make use of secure microcontrollers. Unlike SEs, they are not programmable and have fixed functionality. Also they do not provide a secure execution environment.

Their main purpose is to more securely store artifacts used to authenticate and check the integrity of a device. These artifacts include keys, passwords and certificates. The TPM generates the keys used on board. In PCs the stored keys are used for such things as full disk encryption and digital rights management. Without a TPM such artifacts would normally be stored in an unprotected form.

The TPM can in fact be used to encrypt any data using its binding key in a process called "sealed storage". However, as TPMs do not provide a secure execution environment encryption keys must ultimately be used in the clear by the device's main processor when performing encryption functions making them vulnerable to extraction.

So, in conclusion the only benefits of using a TPM in smart meter may be to securely store credentials and help to secure the boot of the device.

Code Obfuscation

This is a method whereby the code running in the microcontroller or microprocessor of the smart meter is made very difficult to reverse engineer and understand. This is done at the point it is turned from human readable source code into machine readable executable code. Some of the techniques involved are:

- Control flow obfuscation.
- Data obfuscation.
- Dummy code insertion.

- Path merging.
- Instruction substitution.
- Symbol shuffling.

The idea then is that standard micro-controllers and microprocessors can still be used but with some level of protection for the loaded applications. These techniques certainly make static analysis of extracted code more difficult but are less effective against dynamic analysis. Code sizes may well increase and performance may decrease depending on the techniques used.

Trusted Execution Environments

The TEE is an isolated environment within a microprocessor or microcontroller that runs in parallel with the operating system, providing security for the rich environment.

Originally developed for smart phones, ARM have recently released versions of its TrustZone technology for smaller microcontrollers aimed at IoT applications.

A TEE is more secure than the OS and offers a higher level of functionality than an SE (though less physical security), using a hybrid approach that utilizes both hardware and software to protect data. Trusted applications running in a TEE have access to the full power of a device's main processor and memory. Software and cryptographic isolation inside the TEE protect the trusted applications contained within from each other.

Writing trusted applications to run within a TEE is a complicated business and unsurprisingly products have emerged to make this easier. The most well-known of these is Trustonic.

Secure Microcontrollers

These have the same functionality as regular microcontrollers but have the security features of an SE. Some also offer on-board cellular connectivity and support for contactless (NFC). Combined with a secure operating system such as MULTOS or JavaCard they offer a very robust, flexible and inexpensive way of implementing a smart meter.

Programming these devices is very simple because everything is secured by the chip and operating system – the code, data, keys, passwords and even the operating system itself. No split needs to occur between the “secure” parts of the meter and the general parts. All can be done in one device, in one application.

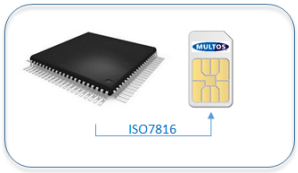
In situations where a more powerful processor is required secure microcontrollers can act as a security co-processor by using the various interfacing options that are available.

The MULTOS Secure Operating System

Introduction

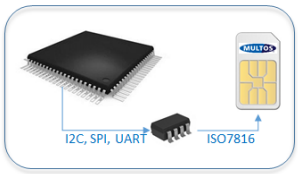
MULTOS is a proven technology with a 20 year pedigree. It has never to our knowledge been compromised. 2017 will see the billionth chip being shipped. With over 3000 business users, MULTOS is an Open Standard, industry backed and supported by a comprehensive vendor consortium.

It comes pre-installed on a range of SEs and microcontrollers from a number of major international vendors and can be packaged in multiple ways. Incorporating MULTOS SEs and microcontrollers into the design does not need to be expensive. From providing authentication and encryption functionality in a secure element to fully operating the meter or gateway with a MULTOS microcontroller the tools and processess are all the same, and free.

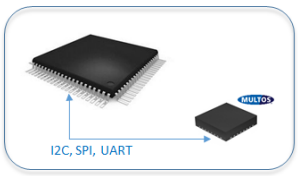


Directly connected SAM

Secure Microcontroller



Indirectly connected SAM



Secure co-processor

With the latest MULTOS secure microcontrollers, the role of microcontroller and secure element is combined into one chip. Standard interfaces (GPIO, SPI, I2C, UART and NFC contactless) provides several options for interfaces to communications controllers and peripherals allowing systems to be tailored to match the application thereby reducing cost.

Naturally a MULTOS device allows customer data to be protected within the device and in transit, regardless of the security or quality of the communications links used.

With MULTOS, every chip is unique when manufactured. Thanks to the way they are enabled for use and applications are deployed to them, it is impossible to clone a MULTOS device or load fraudulent applications.

MULTOS chips are designed to be in use for many years. For example, passports have a lifetime of at least 10 years. The ability to remotely update the device, even after many years and the potential loss of the original records for the device means that should the protocols and infrastructure change on the grid, it will be possible to securely update the meters.

Key Management Simplified

One of the hardest tasks when considering smart anything is the use and handling of digital encryption keys.

There are currently essentially two choices; symmetric key encryption (where each party shares a key) or asymmetric key encryption (where each party holds a pair of related keys, keeps one private and shares the other public part). The latter is often referred to as PKI, or Public Key Infrastructure.

Symmetric key encryption's main problem is securely distributing and storing the keys used, so only trusted people and things can use them.

PKI's main challenge is verifying that a public part of a key belongs to the person or thing it claims to belong to.

Keys are also used for many different things including:

- Locking a device at manufacture so that only authorised people can use it – often called Manufacturing Keys.
- Loading applications to a device; proving they are genuine, trusted, confidential, unmodified etc. – often called Personalisation Keys
- Performing typical crypto tasks as part of the user loaded application. E.g. authentication, confidentiality, integrity checking and non-repudiation. – called Application Keys

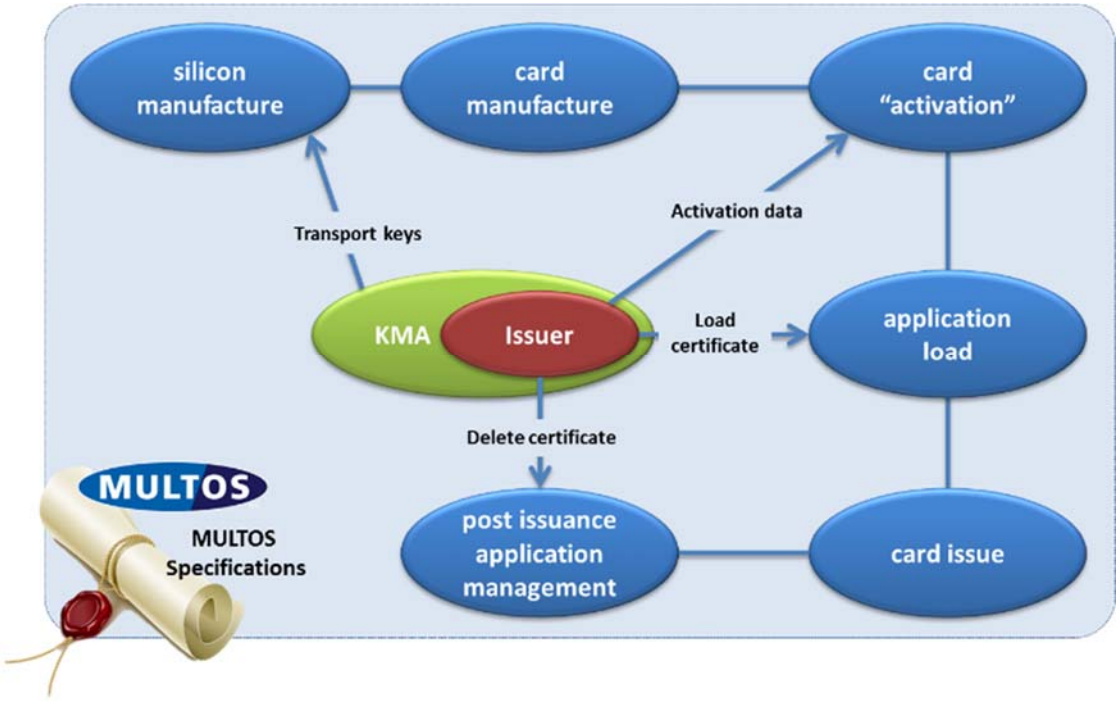
The MULTOS key scheme was very carefully designed from the beginning to make every stage as easy as possible to achieve but leave total flexibility for application designers.

At the heart of the scheme is the Key Management Authority. Think of it as a Certification Authority but handling much more than simply signing certificate requests.

In MULTOS application loading uses PKI methods, so the KMA is the source of the certified key pairs loaded into each MULTOS device when it is enabled. Enablement is the step of making an inactive stock chip active, loading its identity, keys and ownership. By having the certified key pair come from the KMA, encrypted under the unique manufacturing key of the target device, it is impossible to perform a man in the middle attack on the key pair.

There is a global KMA in the UK that is used for markets all over the world. It is in a high-security environment, hugely protected logically and physically and is super-scalable for high volumes. If preferred, the KMA can be operated in-house through licensing the technology.

Practically this means that as a meter manufacturer, each chip delivered is already unique cryptographically. There is no need for the manufacturer to handle any keys at all in your facility or have secure manufacturing.



Meter asset providers have no keys to manage. Once locked to the asset provider (through enablement which can be at any stage), the KMA controls what can be added to and removed from the meter.

Energy suppliers only need to handle keys related to their own services such as billing, pre-payment, top-up etc. The meter asset provider supplies certificates via the KMA to update the meters for consumers.

Key management, application development and personalisation are all big topics. Thankfully the MULTOS Consortium's membership includes many experts and vendors that can provide help.

Provisioning

The MULTOS application provisioning mechanism is designed to be performed in the field. This means that standard, modularised meters can be built and configured just before or actually when installed. This configuration could be performed over the air, via a hand held device or even via a mobile phone.

Switching supplier could involve a change of keys or even a change of application code. This is easily achieved.

Because each MULTOS device contains a unique, certified public key, it can be verified and the content subsequently modified (load/delete apps) by just asking the chip for its certificate. Assuming permissions allow, with appropriate Load and Delete certificates from the MULTOS KMA, the update can be encrypted to the target device so that only the target device can decrypt and use the update (by using its private key).

Secure Operation

The operating system is designed, and thoroughly tested (up to Common Criteria EAL7 in some cases) to ensure that attempts to compromise applications and data resident in the device fail.

Every application is firewalled from the others and can only communicate through tightly controlled mechanisms. This means that it is perfectly OK to install a payment application (such as Rupay) alongside the application for controlling and communicating with the meter.

Extra applications can be added later in the field, perhaps for example for a marketing campaign or to add extra features.

Every device has a unique, cryptographically verifiable identity from the point it is manufactured. This, and the PKI provisioning mechanism ensures that only genuine devices can be used. Every Smart Meter using MULTOS technology therefore has a hardware root of trust.

Prepay Metering

Prepay metering is hugely important in many markets in the world, so it is very relevant to mention some of the ways in which MULTOS could help to build a better, more secure, pre-pay infrastructure. For example, a MULTOS SAM could be used in the globally used Secure Transfer Specification (STS) protocol and similar code transfer systems for prepay meters [10]. These use shared symmetric key cryptography to either create a) a numeric code to be keyed-in on the meter or b) a cryptogram to be transferred via a memory token or smart card to the meter. The generation of these codes and tokens needs to be done securely; use of a MULTOS SAM would ensure that the keys are stored and used safely in the code generation vending machines. In the meter themselves, a MULTOS SAM could be used to store the keys, perform the token decryption and validation and securely store the credit value.

Furthermore, in a meter that is fitted with a MULTOS microcontroller that supports contactless card mode, it would be possible to load the STS token from an NFC enabled mobile phone. This would make it possible for the user to buy a top-up online (for example using M PESA), receive it directly into their phone and load it to the meter. Another possibility would be to use a MULTOS SAM or microcontroller to provide in-meter payment services in conjunction with an NFC terminal.

Whatever the approach, use of MULTOS devices would greatly enhance and support the security of prepay mechanisms without adding greatly to the cost of the systems.

Summary

MULTOS products are built to last. They are built for hostile environments and are easily upgradable in the field for example to change keys, change algorithms and change communications protocols.

Conclusion

Adequately securing smart meters against the array of physical and logical attacks to which they will be subjected to is not trivial. It is especially difficult if everything has to be invented from scratch.

A number of well-established technologies do exist and newer ones are constantly emerging. By employing well proven technologies risk is reduced as products are already thoroughly tested and well supported by tools and services.

The use of a hardware root of trust should be considered an absolute requirement as without one the whole foundation on which remote management of smart meters relies, trust, is absent. Secure Elements from the payments, mobile and ID worlds are well placed to meet these needs as are their related secure microcontroller siblings.

The renowned choice amongst these devices is MULTOS which has an unparalleled pedigree of security and flexibility over a 20 year history.

****

Reference

[1] Rural Electric Magazine, June 2015
http://remagazine.coop/power-theft/

[2] US Energy Information Administration, October 2015
http://www.eia.gov/todayinenergy/detail.php?id=23452

[3] Indian Power Sector, 2012
http://indianpowersector.com/home/about/

[4] WonderHowTo
http://null-byte.wonderhowto.com/how-to/crack-wps-with-wifite-0161588/

[5] InfoSec Institute,
http://resources.infosecinstitute.com/hacking-zigbee-networks/

[6] Various
https://en.wikipedia.org/wiki/MAC_spoofing

[7] Igor Skochinsky, 2010
http://hexblog.com/files/recon%202010%20Skochinsky.pdf

[8] BBC News, October 2014
http://www.bbc.co.uk/news/technology-29643276

[9] Financial Times Online
https://www.ft.com/content/ca2d7684-ed15-11e5-bb79-2303682345c8

[10] IEC 62055-41
Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems