Gemalto answer to DECC

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)

October 13, 2011 – Version 1.0

www.gemalto.com

gemaltax
security to be free

Introduction

In relation to the above mentioned UK public consultation, considering its expertise gained in addressing security risks from other industries such as wireless telecommunication, payment systems, identification systems, pay TV, Gemalto would like to share its understanding of the security risks associated with smart metering roll out and how they can best be addressed using already proven technologies and standards.

Note that Gemalto would be happy to share its experience both in security technologies, field returns, certifications and more during any face to face event that could be organized. A security workshop would be a good way to proceed.

For more information on Gemalto, please visit; www.gemalto.com

Gemalto is already actively contributing to the standardisation organizations and industry associations linked to smart energy. We can mention the following ones:

European commission, Smart Grid Expert Group 2 on Smart Grid Security
European commission mandate 441 on smart metering
European commission Smart Grid Information security group (SG-IS)
ETSI technical committee on Machine to machine communication (chair of security working group)
European Smart Metering Industry Group (Communication Technology Group)
Smart Energy Demand Coalition
DLMS (application in progress)

As a general statement, we consider that AMI (Advanced Metering Infrastructures) will raise the following security issues:

Fraud: this is mainly a business issue for energy provides and one might think that the market forces will solve the problem and find the best compromise between losses due to fraud and security costs. However, we can also mention that deployment of a trustable AMI is a pre-condition to enable a healthy market were consumers can benefit from competition between numerous energy providers and from innovation by service providers.

Critical infrastructure protection: this area clearly has to be regulated as it fell in the government responsibilities.

Privacy protection: this area has also to be regulation in order to offer sufficient

protection to consumers according to European directives and local law that may apply.

An architecture like the one presented in IDTS is interesting as it could separate the fraud issue (concerting mainly the meters themselves) and the infrastructure protection (a maximum protection could be applied the hub that will act as a firewall protecting the HAN). In that case, the metering security level could be decided by the industry (if we discard the argument of enabling a trusted AMI for a healthy marketplace) and the hub security level could be regulated to protect the national grid infrastructure.

Consultation questions related to security

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

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.

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.

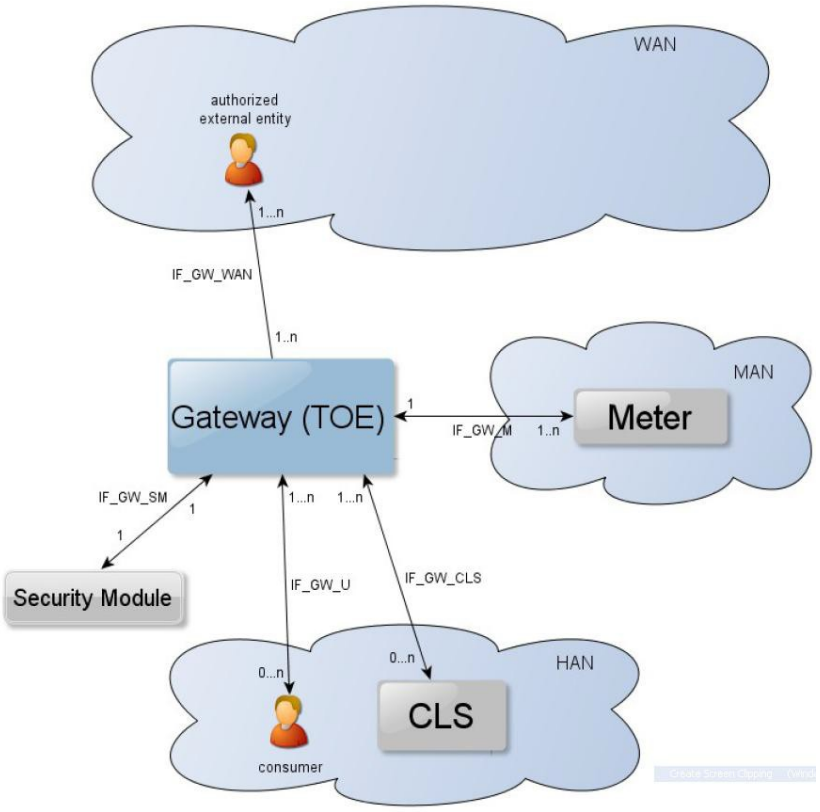
We are thinking that requirements defined onto the IDTS are not sufficient. For example the threats like tampering, transaction repudiation, information disclosure or Denial of Service cannot be properly addressed without strong physical security (i.e. tamper resistance). Any kind of pure software solution for those threats will not be sufficient to maintain a good security level.

There are several different risks associated with Smart Meters as considered in the SMETS. The first issue is the prevention of frauds and the security of financial transactions that may relate to the energy consumption. It seems reasonable to believe that this requires similar security measures as what is adopted in traditional payment solutions, which generally rely on tamper-resistant hardware for the storage and protection of authentication and identification credentials.

Another issue that may have been underestimated in preparing the current security requirements is related to the presence of an Off switch functionality potentially blocking the energy delivery. Proper countermeasures need to take into account the costs of the associated risks but also the potential motivation of attackers and the means that may be at their disposal considering who such attackers may be. The outlook of cutting the energy supply to factories by taking control of the Off switch may motivate foreign power who could start preparing their plans far ahead, possibly involving strategic infiltration, and later gathering huge means to perpetrate an attack at a time of conflict. This should justify the strongest security countermeasures throughout the whole chain, from the

creation and provisioning of security credentials involving the management of access authorization and proper accreditation of personnel to the certification assessing the tamper resistance of actual implementations of the required security measures in products to be deployed. Such security procedures bear their own cost, but this must be weighed against the costs of attacks that may endanger a country's vital supplies at critical time.

This exactly what the BSI already approved in Germany by defining a Protection Profile for the gateway of a smart metering system (i.e. communication hub) at the Common Criteria level EAL4+. An overview of the architecture featuring a Security Module (that will be itself certified) is the following:



The full document is available at :
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile

Do you agree with industry's proposals for an overall architecture of an
48. application layer standard with translation through a Communications Hub to a HAN? Do you believe there are any consumer, economic or technical issues
Where do you believe that translation is best managed:
49. 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?

From a security and privacy point of view the two best options are the following:

End-to-end applicative security: the data is secured at its origin (e.g. the metering device) and stays in a secured form until it reaches the consuming point (e.g. the DNO or the energy reseller). Data will never be exposed in clear at an intermediate point. However we acknowledge that this option may not always be technically feasible in all cases.

Local translation in a strongly secured communication hub: the data will be locally processed in a tamper resistant device and repackage securely for end point in the WAN on a need to know basis. Local processing will enhance the privacy protection (e.g.: data could be locally aggregated in order to fit the technical purpose and to disclose minimum information on consumer's life).

Do you think that an assurance framework, underpinned by regulatory
54. obligations, is needed to support the delivery of the required functionality, interconnectivity, interoperability, and security of Smart Metering Equipment? Please explain your reasoning
Do you agree that as part of any assurance framework adopted,
55. there should be a testing regime in place to support the delivery of the required functionality, interoperability and security? Please explain your reasoning
What are your views on the options outlined for a testing regime?
56. Are there other options that should be considered?

The experience gained from other industries shows that regulatory obligations combined with a certification scheme is the best option to control the security level of deployed equipments.

The most proven scheme for security certification is the Common Criteria one (ISO 15408). NIST standard FIPS 140-2 is also used in the US but tackles only part of the problem by testing only cryptography and is mostly appropriate for cryptographic modules and not complete systems like meters or hubs. Other private certification schemes exist like EMVCO and PCI (for payment card industry) or GSMA SAS.

Examples of successful certification scheme in Europe include:

- Secure Signature Creation Devices
- Electronic passports
- Payment cards
- Wireless network cards (aka SIM)
- Tachograph devices
- Point of Sale terminals accepting payment cards

This large number of certifications since years has resulted in a network of mature evaluation labs that can perform reliable and affordable security testing.

The DECC should consider either to rely on an existing certification scheme (CC for example) or create a new one. In any case a work stream should be created on that subject in order to work on evaluation scheme, security testing level and scope, labs accreditation, etc.

Finally it should be noticed that reaching a European agreement on certification would allow the industry to address a wider market with similar products and significantly reduce the design costs.

58. Do you think that the activities outlined above are a suitable way for achieving interoperability across Smart Metering Equipment cryptographic functionality? How else could this be achieved?

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

Key management system (KMS) is more than necessary, it's a crucial part of the system security. The key management system should offer best in class security (by including tamper resistant Hardware Security Modules (HSM)), reliability and scalability. It should be noted that KMS are already in use in other industries. For example existing KMS can manage the keys from millions of individual SIM cards to securely communicate with each of them.

60. Do you agree with the Government's assessment of the advantages and disadvantages of the cryptographic solutions identified above? What other options should the Government consider? Please explain your reasoning

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.

How do you believe the security approach should be applied to opted out

62. non-domestic consumers? Do you see any issues with the approach? Please explain your reasoning.

We strongly disagree with some disadvantages mentioned for asymmetric (PKI) solution. In particular the smart card industry routinely ships smart cards integrating asymmetric cryptography in large volumes. Just to take one example Visa and Mastercard mandate since January 2011 all the payment cards issued in Europe to be compliant with the asymmetric key version of EMV specification (aka EMV DDA). This shows both the maturity and the ROI of this technology.

Most of the modern secure system makes use of both symmetric and asymmetric cryptography in order to optimize both security and performances.

Concerning operation of Certification Authority (CA), the experience shows that certificates management for high security, high volume and low cost devices can be achieved.

As an example, StepNexus operates a highly secure Certification Authority in Warrington, England. The facility/systems in place here were originally designed to provide certificates for the Mondex electronic purse and MULTOS card scheme, and meet very high logical and physical security needs. As such they are very experienced in the production of large volumes of certificates to meet what might be termed, low cost and highly compact digital certificates for specific purpose schemes. They are currently generating tens of thousands of certificates daily. The systems operate around the clock and there is a redundant backup site to which production can be switched in almost real-time in case of an outage of the primary site.