ESB Networks Smart Metering Project

Full Rollout Security Principles

Approved By	Neil McGuinness, ESB Networks Smart Metering Project Manager
Current Status:	**Final**
Document Classification	**Public**
Issue Date:	28/11/2012
Version:	2.0

Table of contents

1 Executive Summary

This document summarises the major security principles which should be considered during the design of the Smart Metering Infrastructure (SMI). These principles provide guidance to project staff when evaluating the security and data privacy capabilities of any proposed technology or service. They also provide assurance to other stakeholders that security and data privacy requirements are fully respected during all aspects of the design process and that all possible safeguards are put in place to maintain the security and privacy of customer data.

The security principles which will guide the design for the Smart Metering Infrastructure can be summarised under seven headings:

- Confidentiality and Privacy
- Integrity
- Availability
- Authentication and Identification
- Authorisation
- Non-Repudiation
- Auditing and Accounting

Applying these principles will help the design teams to focus in on the key requirements associated with ensuring the security of the infrastructure and the privacy of the data being processed. These key requirements include

- Provable device and user identity
- Role based authorisation based on least privilege principle
- Secure hardware architectures
- Secure manufacturing and software development lifecycles plus
- Secure device delivery logistics
- Secure firmware upgrade and device re-configuration
- Strong encryption of all data in transit and at rest
- Ability to refresh keys and update encryption algorithms
- Intrusion detection and prevention
- Comprehensive security auditing coupled with regularly reviewed security policies

There are a number of areas within the proposed Smart Metering infrastructure where security has a direct impact on end customers. These are briefly discussed within this document under the headings of:

- Managing devices within the Home Area Network (HAN) and securing data stored on or moving between devices in the HAN
- Securely operating the contactor within the Electricity Meter or the valve within the Gas Meter

Best Practice Enterprise Security principles will be applied to all backend IT Systems deployed to support the operation of the Smart Metering Infrastructure.

2 Background

Infrastructure security and data privacy requirements and standards are still evolving for Smart Metering infrastructures. Many solutions available today rely on proprietary security mechanisms which are poorly documented and not well understood. Utilities, SMI Vendors, Standards Organisations and Regulatory Authorities are all involved in on-going initiatives to improve the security capabilities of the next generation of Smart Metering and Smart Grid infrastructures. Initiatives by the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) in the US to standardise the security solutions used in SMI environments are helping to raise security awareness, set device security requirements and encourage vendors to improve the security services available within their products.

Work on Privacy Standards and Guidelines taking place in many jurisdictions is also helping to ensure that the coming wave of Smart Meter deployments worldwide will give priority to maintaining the privacy of the metering data being collected.

These efforts are already beginning to show progress and it is assumed that the security capabilities of most SMI offerings will have advanced sufficiently before the procurement phase for the National Smart Metering rollout in Ireland.

3 High Level Security Principles

In any Information Technology (IT) or Operational Technology (OT) implementation, the following basic security core principles should apply:

- Confidentiality and Privacy
- Integrity
- Availability
- Authentication and Identification
- Authorisation
- Non-Repudiation
- Auditing and Accounting

Achieving compliance with these principles should protect against the following types of events

- Reputational Loss - Attacks or accidents that destroy trust in SMI services, including their technical and economic integrity
- Business Attack - Theft of money or services or falsifying business records
- Gaming the system - Ability to collect, delay, modify, or delete information to gain an unfair competitive or monetary advantage (e.g., in energy markets)
- Safety - Attack on safety of the SM infrastructure, its personnel or users
- Assets - Damaging physical assets of the SM infrastructure or assets of its users
- Short-term Denial or Disruption of Service
- Long-term Denial or Disruption of Service (including significant physical damage to the SM infrastructure)
- Privacy violations
- Hijacking control of neighbour's equipment
- Physical and logical tampering
- Subverting situational awareness so that operators take fatal actions that disrupt the system
- Cause automated system to waste resources on false alarms.
- Hijacking services
- Using SMI services or the supported communication mechanisms to attack end users residential or industrial networks (e.g., allowing end-users to compromise other end-users' networked systems)

3.1 Confidentiality and Privacy Principle

Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. It ensures that any desired resource is only accessible under the designated conditions.

The components of the SMI Security solution which enforce this principle are concerned with ensuring that data is collected, stored and transmitted securely so that only those authorised to use the information have access to it. The security mechanisms used to enforce this principle concern themselves with strong encryption of data while it is in transit and storage, strong access controls on all components of the infrastructure (including on-going enforcement of minimal access rights required to carry out a given role), deletion of data which is no longer required and compliance with Data Protection Law etc.

3.2 Integrity Principle

Integrity ensures that any desired resource contains accurate information and performs precisely as intended.

The components of the SMI Security solution which enforce this principle are concerned with ensuring that data cannot be modified while in storage or in transit by any unauthorised entity. They also ensure that any modifications carried out by authorised entities are fully audited and can be proved to have been carried out by the recorded entity. Again strong encryption is used to protect data in storage or in transit and strong access controls combined with comprehensive and regularly reviewed audit logs are used to protect against and detect unauthorised modification of data.

3.3 Availability Principle

Availability ensures that the desired resource is available at the time it is needed and that it is accessible in the intended manner by the appropriate entity.

The components of the SMI Security solution which enforce this principle are primarily concerned with disaster recovery and preventing (or at least detecting and mitigating) denial of service attacks against the SM infrastructure. The security solution must be capable of dealing with automated failover to standby/backup infrastructure in the event of a disaster without any loss of system functionality or any lowering of the security posture. In addition, the security solution must detect denial-of-service attacks or other events which could lead to degraded performance or total loss of availability and must take automated action to remove or bypass the source of the performance impediment.

3.4 Authentication and Identification Principle

Authentication and Identification ensures that any entity accessing any component or data structure within the infrastructure can be uniquely and completely identified.

This is one of the core principles of any security policy – without the ability to uniquely identify a given entity wishing to interact with the SM infrastructure, it is impossible to enforce many of the other security principles described here. The use of usernames with strong passwords, digital certificates and digital signatures are some of the mechanisms used to authenticate entities within the infrastructure. Multi-factor authentication should also be applied, where feasible.

3.5 Authorisation Principle

Authorisation ensures that an authenticated entity is given access only to those infrastructure components and data structures for which access has been specifically approved.

Again, this is another of the core security principles. Authorisation works hand in glove with Authentication to ensure that only properly identified entities gain the appropriate level of access to resources within the SM infrastructure. The authorisation principle ensures that all required resource access is formally approved and enforced across the entire infrastructure.

Authorisation is generally implemented through the use of granular security groups associated with specific roles, so that every resource challenges any entity attempting to access it for the appropriate authentication credentials (digital certificate, session key, password etc). The authorisation features within the security solution not only concern themselves with who has access to a resource but also with the level of access available (view/modify/create/delete etc).

3.6 Non-Repudiation Principle

Non-Repudiation ensures that any action carried out on the infrastructure can only have been initiated by the entity identified by the auditing/accounting components and that the entity cannot deny having carried out the action.

The Non-Repudiation principle will be critical in SMI environments where actions are carried out which impact customers or the operation of the electricity grid itself. Instructions to disconnect/reconnect one or many customers will be a feature. These actions if improperly executed could have significant consequences for customers and for the stability of the Grid itself. Hence, it will be necessary to ensure that the Security Solution only allows such actions to be carried out by fully authenticated and authorised users/systems. The mechanism by which these users/systems are authenticated and the mechanism by which the commands are processed by intelligent components within the infrastructure must ensure that the component executing the command can be absolutely sure that the command initiated from an authorised source.

3.7 Auditing and Accounting Principle

Auditing and Accounting ensures that system activities can be reconstructed, reviewed, and examined from transaction inception to output of final results. It also ensures that system controls are provably compliant with established policy and procedures.

The Auditing and Accounting components of the SMI Security Solution must be tightly integrated with all of the other components. Without auditing and accounting many of the other security controls are rendered less effective. For example it is not very helpful to know that *some* authorised user carried out a command which had a negative impact on customers without being able to identify specifically *which* authorised user carried out the command. Similarly, auditing and accounting of unsuccessful attempts to carry out actions can alert administrators to possible attempts to compromise the security of the infrastructure or to mis-configured processes.

4 High Level Security Requirements

A number of assumptions can be reasonably made about the security architecture required to satisfy the design principles outlined earlier in this document.

It is assumed that the well tried and tested Public Key Infrastructure (PKI) used to secure critical communications over the Internet would be deployed as the base security architecture. This makes use of Digital Certificates to give every device and user in the infrastructure a verifiable identity against which they can be authorised and authenticated. It also allows devices and users to digitally sign their messages so that the recipients can definitively confirm the source of the message and the sender cannot later repudiate the communication. The Digital Certificates with their associated Private & Public Keys may be installed on each device during the manufacturing process.

Where data is stored on devices, the data will be encrypted.

It is further assumed that Application Layer encryption will be used in addition to link level encryption whenever metering protocol sessions are established between devices.

Finally, it is assumed that critical commands which materially alter the state of the SM infrastructure or devices attached to it, must be checked to verify their origin.

The following sections expand these basic assumptions in more detail.

4.1 Provable Device Identity at Network Join

No device may join any of the SMI networks (HAN, LAN or WAN) without first definitively proving its identity. This proof of identity will most likely be provided by way of a Digital Certificate which will be securely injected into the device during manufacturing. This certificate will be signed by an appropriate Certificate Authority (CA) and for LAN and WAN devices will contain data values unique to ESB's network.

This requires that a number of conditions be satisfied:

A suitable Certificate Authority must be chosen.

1. The CA must generate a device certificate for each new network device (Meter, IHD, Data Collector and Router) and securely deliver it to the device manufacturer.
2. The device manufacturer must securely inject this certificate into the device during the manufacturing process.
3. A suitable risk based process will be required to manage possible certificate revocation.

Note that checking for certificate revocation may not be required if a suitably robust authorisation check can be performed at the backend security servers for all devices attempting to join the network. (See the detailed description of a possible HAN Security design later in this document for more details on this approach.)

4.2 Provable User Identity

It will be mandatory that all users prove their identity before being allowed access to any devices or systems within the Smart Metering Infrastructure. There are a number of ways in which users can prove their identity ranging from the use of Usernames/Passwords to the use of Digital Certificates or similar unique credentials. Whatever mechanism is used, it is essential that the credentials are unique to the user in question – solutions which rely on shared usernames, passwords, certificates or other credentials will not be acceptable. In line with the multi-layered approach to implementing security, some devices or systems may require a user to provide multiple credentials in order to gain access (so called two, three or four factor authentication mechanisms).

4.3 Secure Hardware

The security elements of the Meter, Data Collector and Router hardware must be implemented so that an attacker with physical access to the device cannot extract the security data or interfere with the operation of the security services.

The input interface used by the device manufacturer for injecting permanent cryptographic data (such as the device certificate) into the device should be disabled after the material has been injected.

Any interfaces between the core components in the device and the various communications interfaces on the device (WAN modems, LAN modems, HAN Interface, Optical or Serial ports locally) must be fully secured and all data passing over these interfaces must be encrypted.

4.4 Secure Manufacturing and Software Lifecycle Processes

The device manufacturing process and the lifecycle for device firmware/software development and delivery should be fully secure. All firmware and software images should be digitally signed by the author and securely delivered to the manufacturing site. The validity of the signature should be checked in the manufacturing process before the firmware/software is loaded into the device.

All design and development documentation passed between the entities involved in the design and manufacture of the devices (in particularly the security hardware components) must be securely maintained.

Test/Diagnostic Points on the hardware boards must be secured (or ideally disabled/removed) after manufacture and successful testing.

4.5 Secure Firmware Upgrade after deployment

It is certain that the firmware on deployed network devices will have to be upgraded at least once during their lifetime (probably many more times than once). Hence, the mechanism for delivering firmware updates to SMI devices should be secure. As mentioned earlier, all firmware images should be digitally signed by the provider and this digital signature should be fully validated before the firmware image is accepted and deployed by any device on the network.

4.6 Regular Dynamic Encryption Key Refresh

All data in transit between and stored upon publicly accessible devices must be encrypted, using a strong encryption solution. It is assumed that a PKI type infrastructure will be implemented and maintained to facilitate the frequent refreshing of keys used for data encryption.

4.7 Role based Authorisation based on least privilege principle

It is a requirement that the users or devices which are granted access to the SMI network are only permitted to carry out tasks for which they have been authorised. This applies not only to devices such as Meters, Data Collectors or Routers but also to access to backend IT applications such as Head Ends, Network Management Systems, Meter Data Management Systems etc.

Implementing Role Based access requires that each physical device or software application segment its operations into distinct groups of tasks which can be selectively exposed to suitably authorised users or devices.

4.8 Intrusion Detection/Prevention

The Smart Metering System should support adequate Intrusion Detection and Prevention services.

Intrusion Detection relies on a device building up knowledge of “normal” operations and alerting to a higher authority when it detects any activities which do not match that learned profile.

Intrusion Prevention relies on the device watching for known rogue actions and blocking these actions before they can be executed. The device must be regularly updated with a set of known rogue activity ‘signatures’ to watch for.

A risk based approach to implementation of Intrusion Detection and Prevention measures will be taken at each component within the solution. This may be a particular challenge for Smart Meters as they will be constrained in terms of their CPU and Memory capacity and may rely on a low bandwidth, intermittent communications channel via the LAN

4.9 Comprehensive Auditing and Security Policy Reviews

For security policies to be verifiably enforced, it is necessary that all devices and systems maintain adequate audit logs of all activities. These logs must identify what was done, when and by whom. These logs must be retrieved and analysed regularly and security policy and operations must be continuously updated to respond to any new threats identified.

Because the Smart Meters are expected to have a lifetime of 15 years, it will be necessary to adapt the security solution deployed as new threats emerge and must be dealt with.

5 Overarching Data Security and Privacy Principles

A key principle is that all energy data collected from the customer must be adequately secured.

There are a number of overarching principles which must be applied when considering the storage and transport of customer data in any system. These principles will be enforced in the design of the Smart Metering Infrastructure for Ireland.

- All customer data must be encrypted while being transported so that it cannot be interpreted or altered by anyone with access to the networks providing the transport.
- All customer data must be adequately protected while stored in repositories so that only authorised and authenticated users and systems have access to it
- Where customer data is stored on devices which are located in publically accessible places, the data must be encrypted, so that even if it is exposed to unauthorised access it cannot be interpreted.
- Customer data must only be collected and used for approved purposes.
- Customer Data must be deleted when it is no longer required for the purpose for which it was originally collected. Data archiving and deletion policies must be defined and enforced.
- Individual Customers must be provided with a means of reviewing data which relates to them for accuracy and validity.
- The holder of customer data must define a Privacy and Security Policy which is relevant, enforced and regularly audited/updated.

Where Data Encryption is implemented, the encryption solution chosen will be strong enough to make it impractical for someone with access to the data flow or data repository to decipher the data using currently available hardware. However, hardware capabilities will improve over time (assuming Moore's Law continues to apply) so potential attackers will continue to improve their ability to decipher encrypted data using brute force methods. Some elements of the Smart Metering Infrastructure are expected to have a lifetime of over 15 years. Therefore, the encryption solutions chosen for these elements of the infrastructure ideally should be capable of being updated to take advantage of new encryption algorithms and techniques and to facilitate the use of longer encryption keys.

A defence in depth approach will also be taken to the Smart Meter Infrastructure security design. This means that security services will be layered on top of each other so that a failure of one protection will not compromise the security of the data. This layered security approach has been used in enterprise security designs for many years and is well proven there. Applying it to the myriad components of a Smart Metering Infrastructure poses many challenges, but possible architectures are beginning to emerge from the major security companies, national standards bodies and the Smart Metering/Smart Grid vendors.

6 Security Principles for Interfaces to Customers

There are a number of areas within the proposed Smart Metering infrastructure where security has a direct impact on end customers.

These are:

- Adding devices to the HAN, removing devices from the HAN and securing data stored on or moving between devices in the HAN
- Securing access to operate the contactor within the Electricity Meter or the valve within the Gas Meter

6.1 HAN Security

The Home Area Network (HAN) technology chosen will determine the security mechanisms available to facilitate secure pairing of HAN devices and secure transfer of data within the HAN.

The HAN technology options available are limited given that the HAN must support Electricity and Gas Metering, a dual-fuel In-Home-Display and the capability for Customers to add additional energy management and display devices in the future.

At present a Dual-HAN design is proposed. A Utility HAN will be created initially which will contain the E-Meter, G-Meter and mandated IHD. This HAN will be fully secured as follows:

1. The Utility HAN at each premise will be created by the Communications Module in the E-Meter.
2. Devices joining the Utility HAN will definitively prove their identity. It is assumed that Digital Certificates will be used for this purpose.
3. Devices joining the Utility HAN will be pre-Authorised. Hence, the unique identifier to be presented by every device attempting to join the Utility HAN in any premise must be pre-loaded into a backend authorisation server. The E-Meter will check with this backend server to confirm that a device attempting to join the local HAN has been pre-authorised. If the unique identifier for the joining device does not exist in this backend authorisation database, then the E-Meter Communications Module will not allow the device to join the Utility HAN.
4. Devices wishing to exchange data within the Utility HAN will establish encrypted sessions over which the data is transferred. The mechanism for encrypting data will depend on the HAN technology chosen.
5. The keys used for data encryption and other security services in the Utility HAN will be regularly refreshed.
6. Devices storing data in the HAN will only expose that data to authorised sources.
7. Since the E-Meter will be responsible for creating the HAN in each premise, the replacement of the E-Meter has significant implications for all other devices in the HAN. Hence, the security services deployed in the HAN will be capable of securely re-joining all devices to the new HAN created by the new E-Meter and ensuring that all data sharing rules are enforced when updating data stored on In-Home Displays and other energy information devices.

A Customer HAN may also be created in some premises in the future. The Customer will own and manage all devices in this HAN. However, it may be necessary for the Smart Meters in the premise to send some data to devices in the Customers HAN. In this scenario a single Gateway Device in this Customer HAN would also be allowed to join the Secure Utility HAN. ESBN would approve only certain gateway devices for this purpose and these would join the utility HAN with all of the same security requirements described above. ESBN would approve a selection of gateways which had been tested and certified as enforcing the necessary security interfaces between both HANs required to protect the security of the Utility HAN.

6.2 Remote Operation of Meter Contactor or Valve

Unauthorised remote operation of either the electricity meter contactor or the gas meter valve can have significant adverse effects on customer safety and customer service. In addition, unauthorised switching (off or on) of large numbers of customers can have an adverse impact on the stability of the electricity/gas grids. It is therefore essential that remote access to the contactor/valve be very tightly controlled so that unauthorised operations are not permitted.

The Availability Principle outlined earlier requires that all commands which can negatively impact customer safety or service or which have the potential to impact grid stability will be digitally signed. Devices receiving these commands will be required to verify the validity of the digital signature before executing the commands. In addition, switch on / switch off commands will never be delivered via broadcast or multicast mechanisms. This restriction may have implications for some proposed use cases which may require rapid switch out of load to provide network protection or response to safety issues.

7 Backend IT Systems Security Considerations (High Level)

The backend systems (Head Ends, Meter Data Management System, Billing Systems, Network Management Systems, Hubs/Middleware, Customer/Supplier Portals etc.) are generally delivered using standard IT infrastructure and protocols. The mechanisms for securing such systems are well understood and documented and have been implemented successfully in ESBN and BGN for many years.

These security mechanisms are many and varied, but include

- Firewalling
- Intrusion Detection and Prevention
- Least privilege rule for all users of systems
- Authentication, Authorisation and Accounting (AAA) for all users and processes
- Published and Enforced Security Policies
- Application of all security patches from vendors
- Anti-Virus solution on all clients, servers and networks
- Use of demilitarised zones between public and private networks
- Defence in Depth philosophy so that security is implemented in overlapping layers ensuring that if one layer fails to detect a threat another layer is likely to do so.
- Role based access rights for all staff with regular reviews and process for removing/granting rights as staff roles change.
- Focus on sizing infrastructure for likely worst case scenarios
- Full Disaster Recover incorporated into system design
- Component redundancy and automatic failover

Stakeholders can be assured that best practice enterprise security principles will be applied to the design and implementation of all backend IT systems in the Smart metering Infrastructure.