ESB Networks Smart Metering Project

WAN Technology Strategy

Approved By	Neil McGuinness, ESB Networks Smart Metering Project Manager
Current Status:	**Final**
Document Classification	**Public**
Issue Date:	28/11/2013
Version:	2.0

Table of contents

1 Executive Summary

One of the key components of the Smart Metering Infrastructure (SMI) will be the Wide Area Network (WAN). The WAN is the communications infrastructure that facilitates communications between the meter in the consumers premises and the back office systems in the data centres.

This WAN system will be required to function for a minimum of 15 years, operate in 2.2 million end devices, provide full national geographic coverage and 100% availability. Selection of an appropriate and capable technology is critical to the success of the full rollout and to the ongoing operation of the system.

Based on the outcome of the technology trials, the ongoing technology developments internationally and uncertainty over the final functional and performance requirements for smart metering, ESB Networks will not specify a specific technology or technologies at this stage in the process.

The objective of this document is to outline a strategy for how ESB Networks will select a suitable WAN technology or combination of technologies to accommodate the Irish SMI roll out.

The strategy will involve a number of steps:

Before commencing procurement:

- Develop the volumetric, performance and latency requirements of the WAN based on business processes and performance requirements emerging from the industry workshops
- Develop the security requirements including security related payload impact
- Conduct some small scale technology trials on emerging technologies as required
- Confirm the suitability of IP as the networking standard
- Confirm the suitability of DLMS/COSEM as the application standard
- Develop meter communications module technical requirements
- Identify other network parameters in terms of coverage and availability
- Develop technology risk management framework for WAN and acceptable risk profiles for WAN technology and vendor
- Development of Data Room
- Finalise WAN requirements document for procurement.

Technology selection process (during procurement):

- Overall approach is to select WAN solution with the lowest total cost of ownership which meets the WAN requirements.
- Important factors to be considered will include areas such as : Technical Risk Assessment and evaluation / pre-deployment stage.

2 Background

The WAN will consist of a number of key components, the communications module (which will be in the meter), an aggregation device (which can be a router, data concentrator, etc….) and the communications head end system. ESB Networks has carried out investigative trials into a number of WAN technologies which were available in 2008. Based on the outcome of the technology trials, ongoing progress with some technologies and uncertainty over the final requirements for smart metering, ESB Networks will not specify a specific technology or technologies at this stage in the process

The objective of this document, in the light of the above, is to outline a strategy for how ESB Networks proposes to select a suitable WAN technology or combination of technologies to accommodate the Irish SMI roll out.

The strategy is first of all dependent on the definition of the business requirements, functionality and performance, for the systems. WAN volumetric and performance requirements of the WAN and the relevant technologies will then be developed from these requirements. This process will be outlined in later sections of this document.

While the technology will not be specified, there are a number of key industry protocol standards which are likely to be mandatory.

The strategy will also outline the security policy/principles for the SMI and develop a technology risk approach.

In the procurement process, vendors will be asked to detail how they will satisfy the requirement and meet the performance levels described.

3 Data Requirements Definition

As a first step it is necessary to receive clear policy decisions from the CER policy work streams, which will enable definition of the business requirements of the system which the WAN will serve.

In order to develop an understanding of how the system is proposed to operate, these detailed business requirements will be further refined into a catalogue detailing the various devices, events, data flows, transactions and transports.

The performance and volumetric attributes for these various business requirements will include;

- When (Timing)
- Frequency (How often)
- Availability (When needed)
- Where (coverage)
- Latency(time taken for command to complete)
- Application payload (Data volume for transaction)
- Numbers of devices
- Concurrency (numbers of simultaneous transports)

Based on the security rules the following additional requirements and their impact on the payload will be considered:

- Security
- Confidentiality
- Integrity
- Availability

Volumetric, latency and performance requirements will be developed from the information above and a catalogue of data requirements will be produced.

4 Other Requirements for Consideration

The points below outline other, non technology specific network requirements which must be specified to allow for selection of an appropriate WAN technology

- Coverage – 100% geographic coverage is required.
- Availability – 100% availability is required
- Capacity – network capacity network capable of satisfying the traffic requirements
- Low Latency
- Security
- Technology Risk
- Standards based Interoperability and openness
- Longevity (claimed lifetime of technology, in years)
- Management
- Reliability
- Meter Communications Module Technical Requirements

5 WAN Security

Security must be considered at every layer of the communication protocol stack, from the physical layer to the application layer. For the WAN components this can mainly be concerned with the physical and media access control layers and implies the inclusion of additional protocol and traffic events to achieve security signalling functionality as in the case of authentication and authorization, and additional bytes to existing payloads to achieve encryption.

The Wide Area Network devices will be storing and transmitting valuable Customer and Business data. The WAN solution must ensure that this data is securely handled at all times.

The following Security Services will be required from all components within the WAN, it is essential that these aspects are thoroughly covered by any technology offering.

- **Tamper Detection** : Because most WAN devices will be located in non-secure locations, it is necessary that the device enclosures be sealed and fitted with tamper detection circuitry.

- **Provable Device Identity** : Every device should be capable of definitively proving it's identity when challenged to do so by the Network.

- **Authentication into the Network** : The network must provide capabilities to authenticate every device attempting to join it.

- **Authorisation to join the Network** : Only devices which have been authorised should be allowed to authenticate into the network.

- **All Data must be encrypted while in transit** : Data encryption can be implemented at multiple layers within the network and application protocol stacks.

- **All Data must be encrypted while stored on publicly accessible devices** : All Customer and Business data stored within publicly accessible Network Devices must be encrypted.

- **Network must transparent to Application Protocols** : The network must not inhibit the deployment of higher layer security protocols, such as DLMS/COSEM High Level Security.

- **Secure Manufacturing and Software Development** : Device manufacturers will be expected to prove that secure hardware manufacturing techniques and secure software development lifecycle techniques are used to produce the network equipment and software/firmware.

- **Secure Firmware Distribution and Configuration Management** : All devices must be capable of being upgraded and reconfigured remotely

- **Auditing of all activity** : All significant actions and events which are related to the security of a network device must be recorded to a secure local log.

- **Ability to Update Security Algorithms** : It is desirable that network devices are designed to facilitate the addition of enhanced encryption algorithms or the introduction of longer keys in the future.

6 Meter Communications Module Technical Requirements

The communications module in the meter may be either fully integrated or in a replaceable format, whereby the module will be capable of being swapped in the event of failure, upgrade or technology refresh.

It will be necessary to have a standardised interface between the meter and the replaceable module to ensure interoperability between modules and meter vendors. Whilst the communication will be housed in the meter a final decision has yet to be made as to the ultimate configuration for the full rollout.

7 Protocols for the WAN

Whilst it has been previously stated in this document that ESB Networks will not be specifying a WAN technology for the full rollout, there are, however key protocols which merit special consideration. It is believed that incorporation of these protocols will facilitate openness, interoperability and management of whichever solution is proposed. To understand the relevance of the standard we need to use the OSI reference model which is considered to be the most appropriate means to compare technologies from a protocol and standards perspective.

The OSI Reference Model, as proposed by the Open Standards Institute, describes a set of seven layers that define the different stages that data must go through to travel from one device to another over a network

Although ESB Networks does not intend to specify all layers of the model in advance, it is proposed that IP is specified as the protocol for the Data Network Layer and that DLMS/COSEM is specified as the protocol for the Application Layer. The reasons for this are outlined below.

The reference model describes seven layers but for ease of use this can be simplified, to four layers, as outlined in the example below.

Layer	***Standard/Specification***
Application	DLMS/COSEM
Network/Transport	IP
MAC	To be Determined
Physical	To be Determined

Table 1: Possible Mandated Standards for SMI

7.1 Internet Protocol (IP)

This section briefly outlines the reasons why Internet Protocol (IP) should be considered to be mandatory for the SMI Networks.

IP stands for Internet Protocol and is the key protocol of the Internet. IP has been in use for over 30 years and has evolved into a highly secure, effective communications protocol. Using IP can deliver the following benefits:

- **IP provides easy transfer of data between applications residing on different networks** IP provides a single Network Protocol for use over many different Transmission Media and almost any lower level Link Layer
- **IP allows Applications to improve without reference to the Networks they use.** Applications running over IP networks can change and grow by modifying existing capabilities or adding new capabilities without any impact on the underlying networks or the devices connected to them.
- **IP provides a Standard Addressing Mechanism for all devices in the infrastructure** IPv6 can uniquely address extremely large numbers of devices and is particularly suited to SMI networks which typically contain many millions of devices.

- **IP supports highly scalable, highly flexible and highly available networks** IP is used in the largest public and private networks in the world and has been proven to be highly scalable, flexible and reliable.
- **IP is a mature, standardised and well documented protocol** IP has been available for 30 years and is fully standardised.
- **Lightweight IP Stacks are readily available for constrained devices** There are new IP integration protocols such as 6LowPan allow IPv6 networking to operate effectively over small packet size communications technologies, ideal for SMI.
- **IP Networks are Manageable and Secure** One of the benefits of 30 years of operational IP networks is its set of well-understood network management and security protocols, mechanisms, and toolsets that are widely available

In summary, IP is mature and has been proven on the most demanding network in the world, the Internet. Thirty years of use, development and refinement have presented a robust, reliable, scalable, cost effective and well understood networking protocol capable of being deployed in any scenario. It is therefore proposed that IP be mandated as the networking protocol of choice for the SMI.

7.2 DLMS/COSEM

The IEC 62056 DLMS/COSEM series of standards developed by IEC TC 13 and supported by the DLMS User Association provides a consistent standardization framework for smart metering. DLOMS/COSEM has the following benefits;

- It facilitates the use of a single, communication media independent, object-oriented data model that can be used over a wide range of communication media and facilitates interoperability on the end device level.

- DLMS/COSEM, as managed by the DLMS UA provides a framework for conformance testing and a test tool set for execution of conformance testing and certification. As a consequence of this there is a broad ecosystem built up around the standard.

- For this reason it has gained wide acceptance and as of April 2012 the DLMS UA had some 250 members. The standard has been implemented by 70 manufacturers and there were 230 compliant implementations. There are also support tools and services available from independent sources.

- The DLMS UA, in co-operation with the IEC and other bodies is committed to keep the standard up-to-date to meet new requirements and be in line with the latest technology developments.

- The standard maintains a set of core functionality allowing for project specific or country specific customisations to be managed by the development of published companion specifications. This has been the case for Linky (ERDF / France), DSMR (Netherlands), PRIME (Iberdrola, Hidrocantábrico-EDP, Gas Natural Fenosa / Spain, Hidrocantábrico-EDP / Portugal), IDIS (covering several markets) in addition a companion specification is currently being developed for the GB rollout.

- The main benefit of DLMS/COSEM is that it brings interoperability, which is managed and which has a clear path for future development.

ESB Networks proposes designating DLMS/COSEM as the mandatory application standards for smart metering.

8 Technology Risk Management

Technology risk is a key concern for the project; this is especially the case for newer technologies in an immature environment. ESB Networks proposes to use a graded approach to evaluating technology risk, based on the level of maturity and adoption of the technology. This will be a methodology similar to those used in other programs such as GB.

The SMI roll out will require technologies that can be delivered reliably and in the most economic manner. The Programme requirements are likely to require the evaluation of a number of technologies which may include commercial off the shelf(COTS), bespoke or new solutions. As part of the evaluation process, it will be necessary to assess the technical risk inherent in the solutions proposed and it will be necessary for the vendors to provide evidence of their maturity.

A range of types of evidence will be used to evaluate the risk associated with the proposed solutions, these may include:

- Field trial results;
- Site visits to field trials / current working installation;
- Laboratory test results (verified);
- Demonstrations;
- Scientific papers;
- Independent research;
- Expert opinions;
- References from existing customers
- Outputs of network planning in selected geographic areas;
- Performance metrics from existing installations (whether trials or working installations).

Within the evaluation process, ESB Networks will assess the technical risk of the solutions proposed by vendors at all levels. WAN sub-systems include the primary wide area network technologies (by geography, rural or urban), in-fill communication technologies and the communications module in the meter. The approach that the Programme will adopt to assess technical risk outlined in the table below.

Technology Risk Level	*Maturity of System*	*Evidence of Maturity*	*Level of Confidence*
1. Very low	Technology in Use in similar deployments	Vendor credibility/Scale Evidence from deployment Field visit Operator references Documentation	High . Evidence should give high level of confidence that technology can meet requirements.
2. Low	Technology in use in different deployment	Vendor Credibility/Scale Evidence from deployment Field Visit Operator references Documentation	High . Evidence should give high level of confidence that technology can meet requirements.
3. Medium	Technology deployed in trials	Vendor Credibility Field visit References Documentation	Evidence should give confidence of vendors capability, but evidence of technology capability is required
4. High	Technology available for trial	Vendor Credibility Documentation Site visit to vendor labs	Little evidence of ability to deliver
5. Very High	Technology tested in lab	Vendor Credibility/Scale Documentation/Papers	No evidence of capability of technology to deliver

Table 2: Suggested approach to Technical Risk Assessment

9 Technology Trials

ESB Networks will continue to carry out some small scale technology trials on emerging technologies. The purpose of these trials is to;

- Inform ESB Networks as to the readiness of emerging technologies for deployment
- Inform ESB Networks as to the capability of these emerging technologies
- Test the emerging technologies in the Irish environment and on Irish Networks
- The trials will assist in the risk assessment process

10 Pre-deployment

ESB Networks intends to carry out a larger scale Pre-deployment exercise utilising the preferred technology to emerge from the procurement process.

The objective of the pre – deployment is;

- End to end testing of the implemented system of systems
- Integration testing (with back end systems);
- Sub-system testing for the components comprising the WAN solution.
- WAN performance
- Understand the deployment requirements of the technology
- Evaluate the performance of the technology in a large scale deployment prior to final sign off

11 Conclusion

Based on the outcome of the technology trials, the ongoing technology developments internationally and uncertainty over the final functional and performance requirements for smart metering, ESB Networks will not specify a specific technology or technologies at this stage in the process.

The objective of this document is to outline a strategy for how ESB Networks will select a suitable WAN technology or combination of technologies to accommodate the Irish SMI roll out.

The strategy will involve a number of steps:

Before commencing procurement:

- Develop the volumetric, performance and latency requirements of the WAN based on business processes and performance requirements emerging from the industry workshops
- Develop the security requirements including security related payload impact
- Conduct some small scale technology trials on emerging technologies as required
- Confirm the suitability of IP as the networking standard
- Confirm the suitability of DLMS/COSEM as the application standard
- Develop meter communications module technical requirements
- Identify other network parameters in terms of coverage and availability
- Develop technology risk management framework for WAN and acceptable risk profiles for WAN technology and vendor
- Development of Data Room
- Finalise WAN requirements document for procurement.

Technology selection process (during procurement):

- Overall approach is to select WAN solution with the lowest total cost of ownership which meets the WAN requirements.
- Important factors to be considered will include areas such as : Technical Risk Assessment and evaluation / pre-deployment stage.

Glossary

3G	Third Generation Mobile Communications
4G	Fourth Generation Mobile Communications
CENELEC	European Committee for Electrotechnical Standardization
CER	Commission for Energy Regulation
CIA	Confidentiality, Integrity and Availability
COSEM	COmpanion Specification for Energy Metering
DAO	Distribution Asset Owner
DLMS	Device Language Message Specification
DNO	Distribution Network Operator
DSO	Distribution System Operator
DST	Daylight Saving Time
DUoS	Distribution Use of System Charges
ENCS	European Network for Cyber Security
ESB	Electricity Supply Board
EU	European Union
G3	Third Generation PLC (ERDF Technology)
GPRS	General Packet Radio Service
HAN	Home Area Network
IHD	In-home Display
ISO	International Standards Organisation
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MDMS	Meter Data Management System
MW	MegaWatts
OSI	Open Systems Interface
PLC	Power Line Carrier
PRIME	**P**owe**R**line **I**ntelligent **M**etering **E**volution
RF	Radio Frequency
RFI	Request For Information
RFP	Request for Proposal
SLA	Service Level Agreement
SMI	Smart Metering Infrastructure
WAN	Wide Area Network