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)

Introduction

This document is written to respond to queries raised by DECC in relation to Smart Metering Implementation Programme as listed in published document "2546-smip-consultation-rollout-180811.pdf".

About Authors

We have over 15 years of experience in metering, communication and security domains. We are currently working for GB AMI solution.

We have expressed our personal views while responding to questions raised by DECC. It does not represent the views of our organisation.

Questions

39.	**Do you agree with industry's recommendation that DLMS should be adopted as the application layer for communications with the DCC? Do you believe there are any consumer, economic or technical issues with this solution which could be circumvented by an alternative approach? Do you have any economic, technical or consumer evidence to assist Government in evaluating industry's proposal?**

DLMS is a "session oriented" "point to point" communication protocol which was originally designed to communicate with metering devices. Using DLMS on WAN is likely to introduce many functional and security problems, some of which are described below:

No Object Model Defined for Gateway Devices

While DLMS itself is a well defined IEC standard, various companion standards exist to define the COSEM object model. These popular object models are defined for electricity meters and practically nothing is defined for gateway devices. Though it is easy to define this object model but defining a mature, technically sound and widely accepted companion standard itself is a challenge. So it might seem like using an established standard such as DLMS might be easier, but in reality it leaves a lot to be defined. So using DLMS has no particular advantage over other WAN protocols.

Not Suitable for All WAN Technologies

It is established (Page 46, Point 134) that no single WAN technology can cater to all installation sites. So final solution is likely to have a mix of GPRS, long range radio, RF mesh etc. Any technology based on radio is likely to have higher latency and lower bandwidth. This results in a fragile communication mechanism susceptible to session time-out problems.

Since DLMS is a session oriented protocol, it relies on session sign-on and state-full commands to be reliably delivered to target device. It may not be possible to use session oriented protocol like DLMS.

40.	**Do you agree with industry's recommendation that DLMS and Zigbee SEP 1.x should be adopted as the application layer for communications within the consumer premises, provided they install the necessary translation equipment? Do you believe there are any consumer, economic or technical issues with this solution which could be resolved by an alternative approach? Do you have any economic, technical or consumer evidence to assist Government in evaluating industry's proposal?**

It remains unclear why someone would want to use different protocols to communicate with electricity and gas meter. But if electricity meters use DLMS and gas meters use Zigbee to communicate within consumer premise, following issues need to be examined:

Not Suitable for All WAN Technologies

This mechanism assumes DCC sends the commands to Hub which will in turn tunnel them to E-Meter over Zigbee. Since DLMS is session oriented protocol, communication with E-Meter will be susceptible to higher latency and delays. It is difficult to imagine such a protocol running over slow RF networks and over Zigbee tunnel.

Inefficient Data Encoding

DLMS was designed for point to point AMR application as well as direct reading via serial port and DLMS meters used to be read on a small scale. Extending it to a large scale such as GB AMI is not suitable because of its inefficient encoding of various meter data such as profile data.

Example (considering only information data):

1 day consumption data = 48 * 2 (48 interval, each having 2 byte value) + 4 (4 byte time value) = **100** bytes

When this data is encoded in DLMS format, it becomes around **912** bytes.

Above example clearly indicates that sending data of millions of smart meters will have higher operation cost due to large bandwidth and higher air time requirements. This will become even more difficult in case of slow networks such as long range radio.

Data Authentication

If Hub collects the data from E-Meter locally and then sends it to DCC, there is no way for DCC to make sure that this data really originated from E-Meter. This is because DLMS data doesn't contain any authenticate code or signature. This clearly violates the DECC security requirements.

Command Authentication

If Hub is expected to take actions on behalf of DCC, it means Hub has to have E-Meter's key. This is necessary for a successful sign-on operation over DLMS. Since Hub is installed in consumer premises, it is vulnerable to various attacks. This makes it very risky to save meter's cryptography keys on Hub.

Key Exposure

In case of local support in event of WAN failure, meter's cryptographic material (keys and passwords) has to be transferred to hand-held terminal to perform various operations like meter configuration, prepayment adjustment, debt adjustment etc. This makes key management more difficult and increases the security threats.

Key Distribution

DLMS uses symmetric key cryptography and it is well known that managing and distributing the cryptographic keys is a difficult task in symmetric key cryptography. DLMS has no support of modern public key infrastructure to handle key management effectively.

Increased Complexity on Hub

This scheme means Hub has to use Zigbee to communicate with gas meter and other HAN devices such as IPD but it has to use DLMS to communicate with electricity meter. This essentially means Hub has to implement 2 different protocols making it more complex and less reliable. Any future change in either DLMS or Zigbee is likely to trigger a firmware upgrade in Hub making it highly unstable.

Issues with Zigbee

While it is possible to use Zigbee to communicate with both electricity and gas meters, there are several issues with that as well. Zigbee specification was originally designed for communication within HAN. Extending it for GB AMI require significant utility specific extensions such as tariff updates, meter reading data, configuration reads etc. SSWG has tried to define these extensions but still various functional and security issues have not been addressed as per DECC requirements. Current specification fails to meet DECC security requirements like authentication of data origin. If Hub is compromised, then false data can be communicated to HAN as well as WAN.