URN 12D/234 – Smart Metering Implementation Programme – Request for comments on a draft licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters

---

Response from REDACTED

General Observations

1. The risk assessment appears to have been performed assuming that the smart metering system is working correctly. The meters contain interruption devices (switch/valve) that controls the energy supply to the home. There is a risk that a fault (accidental or induced) can cause the supply to be interrupted in a population of meters. Such a scenario could arise through a number of sources:
    a. Unintended operation of the meter firmware – a set of circumstances that lead to the malfunction of the firmware
    b. Malicious manipulation of the firmware at any stage of the design or manufacturing process.
    c. Insider attack at the head end system

    The result of large population of electricity meters permanently interrupting the supply and so requiring meter swap out will lead to a national emergency situation. (Thousands of meters cannot be changed in a short period of time.)

2. The onus is on the Energy Supplier to assure the security of the smart metering system. This requires them to audit the whole supply chain or rely on assurances from equipment manufacturers and service providers that they have security under control. This may be an issue for some suppliers who may not have expertise in this area.

3. The license conditions appear to reiterate the contents of ISO 27001 rather than simply specify that companies in the supply chain must be ISO 27001 certified. There is no mention of standards for the metering system. The supplier cannot be expected to test or judge the security of the meter but they could ask to see the compliance certificate to FIPS140-2 for example.

Z4 - The licensee must take such steps and do such things as are within its power to provide that the Supplier End-to-End System is at all times Secure.

In order to meet this requirement, the supplier must ensure that all combinations of all devices have been tested with all combinations of messages, valid and invalid with the head end to ensure no combination in the present or future can ever give rise to a security issue.
(Note past experience with Keymeters that were in the field for a number of years and succumbed to a major failure when a new token vending machine was introduced or the population of radio telemeters that cut off all South Wales when a new message type that sent weather forecast data was trialled.)

It would be advisable to require that the licensee must implement security measures and procedures in accordance with ISO27001 to ensure a high level of security in the end-to-end system.

Z5 – Supplier End-to-End Definition

One end is the meter (c) – that is obvious but what is the other end? Is it the head end system operated by the data collector or is it the supply company's billing system?

Is it expected that messages arriving at the meter are checked to ensure they came from the Supplier or from the Data Collector? If the latter, how is it envisaged that data flows between head end system and energy supplier are to be authenticated and encrypted?

Is it expected that the equipment described in paragraphs b and c is secure in itself or that it is considered insecure (eg similar to the internet)?

Has consideration been given to the DNO requiring access to the meter? If so where does such an organisation fit in Foundation? The DNO end-to-end security may be a requirement.

Z6 – Security of Component Parts

The definition is lacking. The clause calls for an 'Appropriate Standard' which is open to interpretation. It would be better to specify what that standard would be (eg FIPS 140-2 level 2) for the metering rather than trying summarise what is contained in such a standard. Manufacturers cannot design to undefined requirements and certification bodies (Competent Independent Organisation) cannot test against them either.

The definition of interference or misuse is not precise – this could range from a simple physical attack (hammer) to a tazer. Threats must be defined, which is difficult, or more practically the defence mechanism prescribed – for example FIPS 140-2 Level 2 specifies how a cryptographic device should be protected in precise terms that can be certified against.

Z8 – Compliance with Standards

The words 'take all reasonable steps to ensure that it is able to comply' is a subjective statement. This would be more precise if it were worded 'The licensee must be certified to ISO 27001:2005.' This can be verified and is not open to interpretation.

Z9 to Z16 – Information Security Policy

These sections effectively reiterate the requirements contained in ISO 27001 and therefore do not need to appear in this document. If the licensee is ISO 27001 certified then Z9-Z16 will be covered already.

Z17 – Compliance with Directions

This section is presumably included to address issues that may arise resulting in a security issue. This therefore must include a requirement to remove and replace a population of meters in the event of threat to critical national infrastructure. Who would bear the cost of such an exercise – the government or the supplier?

The section refers to the 'Authority' – it is not defined who this is. Do they take financial responsibility for the actions they prescribe?

CONCLUSIONS

Question 1

The document is imprecisely worded. It is open to interpretation and therefore may be applied differently between suppliers and therefore the security measures may vary between licensees. There may be a difference of opinion between suppliers. A new supplier may consider a meter fitted by a previous supplier to be a security risk and to require its removal on gaining a customer. Most suppliers may lack the resources to properly audit the supply chain as required and may choose not to enter the market at Foundation at all and thereby miss a valuable opportunity to gain early experience with smart metering roll out which could later prove detrimental to their competativeness .

Question 2

The document should simply state the standards to which suppliers and equipment manufacturers must comply:

ISO 27001 for data handling and control
FIPS140-2 Level 2 for meters

This would produce a level playing field without ambiguity or doubt and would be auditable.

Question 3

A big risk to small suppliers would be that of the possibility that all meters would have to be removed following an instruction by the 'Authority'.
The biggest risk of all is that of a population of meters malfunctioning accidentally or maliciously causing mass blackouts that are impossible to fix quickly. Such an issue during Foundation would not only be a huge logistical issue but would have serious implications for the viability of the smart metering programme.