I am responding as an individual who has an interest in the subject of Smart Meters and Smart Grids.

(Data Privacy and Security) Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

I have concerns about some issues relating to the management and operation of smart meters:

Remote Firmware upgrades to smart meters could be their Achilles heal, the biggest issue to watch out for is that by just changing one variable within the firmware a meter could be made to under report the amount of power used.

If care is not taken to control how a valid firmware upgrade is initiated, then it might be possible for the upgrade to be done via the HAN interface.

If a modified firmware were successfully uploaded there would be no externally visible signs of tempering.

As an example the Panasonic GH1 camera firmware was hacked, to provide extra performance, none of the underlying code was changed, but system constants were rewritten within the firmware externally to the camera before the user uploaded it.

As there have been recorded incidents of official firmware upgrades breaking equipment in the past, all meters should have a non upgradeable write once basic version of their firmware, which can be used in an emergency.

A smart meter should be able to examine information contained within a firmware upgrade and reject it, if it is being sent a version of firmware, which is not compatible with it self, because over the lifetime of a smart meter, newer versions will be developed and it only requires a small error to send out the wrong version of a firmware for a meter.

A meter should be able to hold at least two different versions of firmware, so that the live copy is not overwritten during an upgrade.

To improve security of the Firmware it should be encrypted on the chip where it is stored.

To make it harder for the running code to be examined, when the firmware is loaded there should be a mechanism in place to randomise the location of the variables within the memory of the meter and the location of the running code.

When talking over the encrypted WAN link, don’t make the mistake of starting all conversations, with the same piece of information, because doing so makes it easier for the encryption key to be determined as more data is collected, also don’t use numbers which increment with each packet, as this would also weaken the encrypted packets.

The ability to be able to switch the WAN interface could also be a problem as it could open up the option for the insertion of a man in the middle attack, where a bit of hardware was placed in-between the meter and the real WAN interface.

Even if the connections between the WAN interface and the meter was encrypted there would need to be a mechanism for introducing a new WAN interface to a meter, the same mechanism could be used to introduce a man in the middle device.

Ideally the internal operation of the smart meter should be such that the code responsible for the meter reading function should be distinct from the code providing access to the HAN and if this code is running on a single CPU, then each code section should be in its own protected memory area.

All message passing protocols should set an upper limit to the size of a single message, as a common form of attack is a buffer overrun on what looks like a legitimate request.

(Consumer Protection) Question 5: Do you agree that consumers should be able to obtain consumption information free of charge at a useful level of detail and format? How could this be achieved in practice?

Yes I do agree that customers should be able to obtain information free of charge.

12 Months of data is not enough, to be able to compare with last year you need to store at least 13 months, otherwise there is no overlap in data and you are therefore not in a position to be able to do a year on year comparison.

(Prospectus) Question 6: Do you have any comments on the functional requirements for the smart metering system we have set out in the Functional Requirements Catalogue?

(Statement of Design Requirements) Question 1: Should the HAN hardware be exchangeable without the need to exchange the meter?

Taking the reasons as to why the WAN hardware needs to be changeable, then there is no reason as to why the HAN interface should not also be changeable, especially as the signaling system has not yet been fully ratified and you may need to be able to support additional signaling systems in the future.

If the HAN hardware is exchangeable, then it should have its own firmware and embedded processor and be securely located within the smart meter. The main smart meter would then only need to communicate with the HAN and it would be the responsibility of the HAN to take care of the signaling system required to talk to the end device.

(Statement of Design Requirements) Question 2: Are suitable HAN

technologies available that meet the functional requirements?

The way the documents read give the impression that the only HAN signaling system of choice is wireless, however the radio spectrum is getting more and more crowded and the unlicensed band in some places is becoming less reliable as a result of too many households having overlapping WiFi.

Don’t limit the HAN to a WiFi based network as not all domestic properties are suitable for WiFi, any property with thick walls will have a more limited range than they would with an Ethernet over the mains solution.

When you start to move on to demand side management, the devices which are going to take part are going to be connected to the electric wiring of the property anyway, so why use wireless transmission, when you can just as easily send the signal down the mains cabling, it is also easy to prevent mains signalling from exiting the house wiring, this function could be incorporated within the smart meter.

The use of mains based signalling should make it easier for customers to add smart meter aware systems, as there won’t be any possible confusion over which wireless network to attach to.

The distance the system can be placed away from the meter is a function of the cable run and not the local environment.

Ideally there should be an indication on smart meter aware devices that they have successfully registered themselves with the meter.