Comments to:

"A consultation on draft licence conditions and technical specifications for the roll-out of gas and electricity smart metering equipment."

55. Do you agree that as part of any assurance framework adopted, there should be a testing regime in place to support the delivery of the required functionality, interoperability and security? Please explain your reasoning

A certification regime, especially for security compliance should be mandatory. Our recommendation is to use the Common Criteria framework, well deployed in different applications.

If level of security is left as a degree of freedom to the implementers, there might be a jeopardize smart grid where the security of the network will be equal to the weakest link of the chain.

It is on the responsibility of the government to set high security standard in order of having a reliable smart grid.

56. What are your views on the options outlined for a testing regime? Are there other options that should be considered?

There should be requirements for the use of certified meters only. Meters tested by authorized laboratories.

Define the tests that a meter should be able to pass is a long and costly work that should start as soon as possible. Our recommendation is to adopt the Common Criteria approach (for a quick overview it is possible to read http://en.wikipedia.org/wiki/Common_criteria).

For a successful process it is necessary to involve stakeholder as: meter manufacturers and silicon provider, among the others.

58. Do you think that the activities outlined above are a suitable way for achieving interoperability across Smart Metering Equipment cryptographic functionality? How else could this be achieved?

Yes, specify a trust hierarchy and a cryptographic key management is a mandatory action for achieving interoperability.

59. Do you agree that cryptographic/ key management is necessary to secure the End-to-end Smart Metering System? Please explain your reasoning

Yes, key management is a fundamental building block of a complex system composed by many devices.

All the communications will be done on physical media that require protections using

cryptographic functions. Smart grid communication can be seen as a digital network, and any digital network today adopt cryptographic function for protecting privacy, data integrity and authentication of data communicated over the network.

If the system has to be open and interoperable it is necessary to define the key management scheme and the cryptographic primitive used for it, and give the possibility to different actor to implement devices compatible to these specifications.

60. Do you agree with the Government's assessment of the advantages and disadvantages of the cryptographic solutions identified above? What other options should the Government consider? Please explain your reasoning

Most of the security protocols use a hybrid scheme for convenience; it is not very common to have an application based only on public key primitive.

Overall the discussion on which type of cryptographic primitive should be used seems a bit premature. It would be preferable to have a more detailed description of the security requirements of the different communications executed on the smart grid. From the security requirements it is generally easier to derive which cryptographic primitive should be used.