

external electromagnetic interference. Failure to ensure compliance could lead to equipment being adversely affected by emissions from other in home technology and in particular disruption of HAN and WAN communications.

**Q53.12 WAN**

A53.12 The WAN is a vital element of the solution, and it is critical that despite the potential for multiple technology choices across GB, interoperability is ensured. The choice of WAN has an impact on communications hub hardware, which will impact all the procurement aspects for suppliers. Minimising the number of supported technologies will benefit the suppliers and reduce overall costs.

WAN selection needs to embrace both the functionality and performance required to deliver against the relevant business processes, but also the non-functional requirements that form part of the End-to-End coherence of the entire Smart Metering Infrastructure. These include diagnostics, security, network administration, message/function priorities, ability to self-heal, reporting, taxonomy and transaction management. WAN should be selected as part of the overall System design considering 'best fit' and suitability for anticipated future requirements, e.g. HH, Smart Grid, EV's etc.

<b>Question 54</b>	<b>Do you think that an assurance framework, underpinned by regulatory obligations, is needed to support the delivery of the required functionality, interconnectivity, interoperability, and security of Smart Metering Equipment? Please explain your reasoning.</b>
--------------------	--

An assurance framework is crucial to ensure delivery of the required functionality, interconnectivity, interoperability and security of Smart Metering Equipment. This must have an independent central body with the powers to define and manage the framework and ensure that it is adhered to.

The Smart Energy code (SEC) should be the choice to oversee appointment for this independent body especially as they will have responsibility for the DCC governance, which will have direct links to define the SMHAN requirements in the future.

Regulatory support from Ofgem to enable enforcement to comply with the framework is required. It should be noted that definition of Smart metering products in this context are: Items at an individual component level such as 'Meter' or 'Communications hub', rather than the complete SME installation i.e. if one product with the SMHAN is not on the DCC certified list the whole SMHAN fails the DCC acceptance process.

<b>Question 55</b>	<b>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</b>
<p>Yes such a test regime that has central independent governance is imperative to ensure that the testing itself is carried out in a uniform way that provides assurance. This also provides a commercial assurance framework for all concerned parties. For example if there were two test houses each declaring their own defined test regime they could be carrying out completely different tests which they each see as conforming to their interpretation of the SMETS compliance. In such circumstances how could the industry decide liabilities when two manufacturer's components following different test regimes are not secure or interoperable?</p> <p>A Smart Energy Code (SEC) defined framework would also be in a position to provide an investigation leading to a resolution dispute process. Any judicial review resulting from litigation between parties who decide not to abide by the SEC appointed dispute outcomes, would take into account said findings in their decision process. This regime would again provide a degree of confidence by investors.</p>	

<b>Question 56</b>	<b>What are your views on the options outlined for a testing regime? Are there other options that should be considered?</b>
<p>It should be noted that although suppliers (the Licensee) will be subject to some form of test regime, in reality this is expected to be on the basis that a Meter Asset Provider (MAP) would look to purchase components that have already been through a compliance regime in terms of 'functionality, interoperability and security' as part of the manufacturing process. This may not always be the case, for example a supplier may attempt post-installation SME compliance accreditation via the test regime.</p> <p>The following points in are taken from page 69, with answers below:</p> <p>Option: A market led approach</p> <p>Response: We do not believe a 'market led' approach should be adopted.</p> <p>As well as the points mentioned, this creates the issue that those testing have a commercial incentive to 'pass at any cost'. Such circumstances could lead to costly mistakes and impact on any workable disputes process.</p> <p>Option: A mandatory industry code and body to deliver and govern a testing regime and: A certification and accreditation scheme</p> <p>Response: A mixture of both would be essential to have a mandatory industry scheme which oversees the licensing and agreed process with the test houses who would be authorised to provide relevant accreditation 'stamps'.</p>	

<b>Question 57</b>	<b>Do you think that a different approach to assurance is necessary for the Foundation and enduring phases? Please explain your answer.</b>
<p>EDF Energy does not believe that the distinction between Foundation and Enduring phases is correct for assurance purposes.</p> <p>Any SME installed for the purposes of testing and trialling, during the 'Current Arrangements' or 'Initial Arrangements' (part of the Foundation phase) are installed at the suppliers liability and should not be required to undergo the compliance test regime.</p> <p>However, any Smart Metering Equipment that is determined to be compliant with the SMETS (and thus applicable for Smart Change of Supplier and requiring ongoing smart rental payments) should be subject to an identical compliance test regime regardless of whether this is during the Smart Change of Supplier stage (within Foundation) or during the Enduring phase. (In reality, this testing regime needs to be in place and operating ahead of Smart Change of Supplier to enable the supply chain to provide compliant Smart Metering Equipment.)</p> <p>If there are no compliancy criteria in place that ensures an SME installation will comply with the enduring DCC solution at individual component level, then it should not be accepted as 'Smart' and commercially / technically interoperable at milestones such as 'Smart Change of Supplier'. In such circumstances what would be the point of applying any testing to ensure 'Interoperability' before we can confirm it is interoperable with the DCC and relevant undefined industry processes?</p> <p>Under current DECC programme milestones; we believe that there should be one compliance test regime in place that ensures compliance to the enduring end to end processes. Delivery of this regime should be aligned to the DCC development lifecycle and any other supporting or linked process change developments.</p>	

<b>Question 58</b>	<b>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?</b>
<p>We agree that interoperability cannot be achieved <b>without</b> "common cryptographic interfaces". (Para 244).</p> <p>This will enable all parties to build equipment and software that behaves in a consistent fashion.</p> <p>We believe a technical document is under development for security requirements that will tell all parties how the more general requirements so far published must be addressed. We await this document as a matter of some urgency and would like to understand how this document will be communicated.</p>	

<b>Question 59</b>	<b>Do you agree that cryptographic/ key management is necessary to secure the End-to-end Smart Metering System? Please explain your reasoning</b>
Yes Key management is essential. The ability to cancel compromised certificates if necessary must also be catered for and a process created for this.	

<b>Question 60</b>	<b>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</b>
We agree with the assessments. The Hybrid solution is the best practice mix (as used in the IPSEC standard). We still need to agree technical details such as key durations.	

<b>Question 61</b>	<b>Do you think that it would be appropriate for the DCC to be responsible for cryptographic key management for the End-to-end Smart Metering System? What other options should the Government consider? Please explain your reasoning.</b>
<p>It is appropriate for there to be a smart meter solution to have a Certificate Authority, where and who hosts this is not as important as understanding the risks of the primary key being compromised.</p> <p>It may be advised to use a supplier who understands how to manage these keys, such as VeriSign for example.</p> <p>We believe that a solution for opted out non-domestic suppliers must also be looked at since it appears that the DCC will not be handling communications or access control in these cases.</p>	

<b>Question 62</b>	<b>How do you believe the security approach should be applied to opted out non-domestic consumers? Do you see any issues with the approach? Please explain your reasoning.</b>
<p>The ability of non-domestic suppliers to “opt out” of DCC usage has seriously complicated all aspects of the Smart Metering Programme.</p> <p>The phrase “opted out non-domestic consumers” could be taken to mean three things.</p> <ol style="list-style-type: none"> <li>1. Some non-domestic sites will be allowed to use AMR rather than smart metering in which case the AMR security framework should be applied.</li> <li>2. Non-domestic suppliers may be allowed to opt out of DCC usage for smart installations. It is essential that the principles applied to ensuring security of DCC sites are not circumvented for every site that chooses not to use the DCC.</li> </ol> <p>Very careful thought needs to be given to the business and systems rules around which</p>	

these sites operate. As an example, a series of security requirements are proposed for the DCC. These need to be reviewed and the question asked around what the equivalent requirement would be for those sites not using the DCC and who is mandated to fulfil that requirement. It is our opinion that many of these requirements need to be allocated to the opting out supplier for an equivalent level of security to apply to these sites.

3. Some meter service providers may also be allowed to opt out of DCC usage for a site. How "access control" is provided for such a site is not clear.

The opt out has very obvious security risks and these risks need to be mitigated through the development of a security requirements document for companies wishing to opt out. Once again STEG and others need to ensure that such a site does not simply by-pass all of the security requirements that apply to everyone else.

Special consideration needs to be given to the rules around which a premise that has **both** opted in Suppliers and opted out suppliers and/or metering service providers should be operated.

**EDF Energy**  
**October 2011**