

28th October 2010

Margaret Coaster  
Smart Metering Team, Ofgem E-Serve  
9 Millbank, London SW1P 3GE

## Roke's Response to Smart Metering Prospectus

### About Roke

Roke Manor Research Ltd (Roke) is an independent R&D centre in the UK, specialising in professional consultancy and engineering for the Defence, National Security, Telecoms and related markets. We have been a trusted provider of services, products and advice to the UK government for over 50 years.



## Introduction

Roke welcomes the opportunity to respond to the Smart Metering Prospectus and supporting documents provided by Ofgem and DECC. The UK's Smart Metering Programme represents a significant investment in the nation's energy infrastructure. A successful Smart Metering deployment facilitates and enables a wide range of Low Carbon and Smart Grid technologies, which all play an important role in safeguarding the UK's future energy security.

The recently published HMG National Security Strategy highlights the growing dependence of the UK's national infrastructure on information and communication technology. The Smart Metering Programme is a prime example of this. The Strategy highlights cyber security as one of the highest priorities for UK national security.

Roke welcomes the emphasis placed on privacy and security in the Smart Metering Prospectus and supporting documents. We believe that effective leadership, coordination and consultation are crucial in ensuring the rollout of a secure and resilient Smart Metering system, and ensuring it is capable of evolving to meet future security challenges.

Specific comments with respect to the security-related questions posed in the Prospectus and Data Privacy and Security document are presented below.

## Prospectus

### **Question 15: Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?**

Roke supports the risk-based approach being used in the Smart Metering Programme to define security requirements. We believe that a detailed risk-assessment provides the basis for defining appropriate security requirements which target real (vs perceived) threats in a cost-effective manner.

The prospectus states that the Government wishes to accelerate significantly the rollout of Smart Meters. Roke believes that efforts to accelerate the rollout should be contingent on the ability to accelerate the risk assessment, the definition of comprehensive security requirements and the ability of equipment and service providers to provide products and solutions which satisfy these security requirements.

Public trust is essential to the acceptance and ease of deployment of smart metering and the DCC service, and as such Roke encourages the reuse of established open standards and the publishing of an open security specification in the development of a trusted, secure system. Existing standards and experience in cryptographic key management, communication security and tamper evidence can be applied in the new domain of smart metering with relatively few modifications.

Roke recognises the need to support early movers and the deployment of interim metering systems prior to the establishment of the DCC service. Indeed, such interim systems could provide valuable experience which will benefit the rollout of the DCC service (and help maintain momentum in the event of any slippage in the DCC rollout). We believe that the security of such interim solutions is every bit as important as that of the DCC service.

Significant changes and advances in security threats and solutions can be expected over the lifetime of the smart

metering system. Technologies in the early stages of research today could have a profound impact on the system in 10 years time. On the other hand, the cost of Smart Meters and their deployment prevents frequent replacement. Therefore, the smart metering system will need to evolve to accommodate a mixture of new and legacy devices with varying security capabilities. The design of these devices needs to ensure that the system as a whole exhibits and maintains strong emergent security characteristics.

Finally, the UK's Smart Metering Programme represents an opportunity for industry and academia to develop innovative security solutions and expertise with consequent benefits to the UK's competitiveness in the security arena.

### **Recommendations:**

1. We recommend that the Programme should actively support the rollout of secure interim metering systems, aligning them with the evolving security framework being developed for the DCC service. This will reduce the issues related to the switchover of domestic energy consumers to the DCC service. In addition, elements of these interim metering systems may persist for non-domestic energy users. Roke considers it vital that all metering systems, not just those served by the DCC service, be brought under a common security framework.
2. We recommend that the Programme should include horizon scanning activities. Consideration should be given to how future technical advances in security may impact Smart Meters, DCC service, etc.
3. We recommend that the Programme make the (appropriate) security requirements available to UK industry and academia, with a view to stimulating innovation and enhancing the UK's competitiveness in the security arena.

## Data Privacy and Security

### Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

Ofgem has highlighted how the Programme is engaging with international expert groups and standards bodies. Roke strongly supports this approach. International coordination and standardisation in the area of Smart Meter security brings many benefits – sharing of threat intelligence and experience; technical innovation; economies of scale for meter manufacturers and solution providers.

As mentioned in the introduction, Roke believes that leadership, coordination and consultation are vital in developing and maintaining an effective, risk-based security framework. Ofgem is providing this leadership and coordination during the implementation phase. The threat landscape is continually evolving and we believe it is vital that the risk assessment, security requirements and framework be maintained and regularly updated throughout the full lifecycle of the Smart Metering system. We believe that the Programme would benefit from clarification regarding leadership and coordination beyond the implementation phase.

As mentioned earlier, we believe it is important for all metering systems, whether served by DCC or not, to be brought under a common security umbrella. Providing active support to the rollout of secure interim metering systems raises issues about focus and resource. Will the Programme have the bandwidth to simultaneously develop the security framework whilst supporting the rollout and enhancement of interim systems? We believe it is important that stakeholders and trusted third-parties are empowered to use and contribute to the evolving security framework.

Roke strongly supports the principal of security by design and its use in all aspects of the Smart Metering Programme. We believe it is important to consider security by design at both the device level (e.g. Smart Meter) and at the system level. It is important that devices react in ways which support overall system security. For example, in the event of reduced WAN service (e.g. DoS attack), Smart Meters should make use of verifiable local storage in order to reduce their WAN utilisation until full service is resumed. All too often, individual devices in networked systems can act to exacerbate rather than ameliorate downstream problems.

The Data Privacy and Security document rightly highlights the need to include rigorous detection capabilities in the Smart Metering system. This recognises the fact that a

risk-based approach to security is intended to result in a proportionate level of protection (and investment). Therefore, the need to ensure that security events are detectable is paramount, as is the need for rapid and effective incident response. We suggest that the evolution of detection capabilities with the Smart Metering system is just as important as the evolution of protection measures.

Finally, we also agree with the documents emphasis on the need for “stringent security testing”. Roke believes that stringent security testing should be an ongoing requirement and not just limited to the implementation phase. We would welcome clarification from Ofgem on how the Programme will promote and regulate the provision of trusted, independent testing services.

### Recommendations:

1. We recommend that the Programme publish elements of the risk assessment and security framework (at the appropriate classification level) which enables its use by stakeholders and trusted third-parties in the rollout of interim metering systems. We also recommend that a mechanism be included to allow the framework to evolve in response to feedback and experience gained from the rollout and operation of these interim systems.
2. We recommend that the Programme leverages knowledge and experience from other markets, particularly in the area of network-enabled devices deployed in the home. One example is 3G Home NodeBs (femtocells), which are mini base stations deployed in the home to provide enhanced 3G coverage. These devices connect to mobile network operators systems via public fixed-line communications (e.g. DSL) and have a number of security considerations in common with Smart Meters. Use is made of Trusted Environment technologies to provide tamper resistant security measures.
3. We recommend that the Programme considers the specification of Safe Modes and Safe Configurations for Smart Meters which can be activated automatically or remotely in support of overall system stability and security. For example, on detection of physical or electronic tampering (or failed firmware upgrade), the Smart Meter could revert to a minimal Safe Mode. In another example, if the Smart Meter detects problems with the WAN service (e.g. DoS attack), it could enter a preset Safe Configuration which reduces WAN utilisation until full service is restored.

## Conclusion

A proactive approach to securing the UK's smart metering system, as described in the Prospectus, will promote public trust in Smart Meters and act as a catalyst for the adoption of innovative, energy-saving solutions in over 27 million homes. Roke would welcome the opportunity to discuss the comments and recommendations raised in this response with Ofgem and stakeholders in the Smart Metering Programme.

For further information please contact



**Roke Manor Research Ltd**

Roke Manor, Romsey  
Hampshire, SO51 0ZN  
United Kingdom



Part of the Chemring Group

00296