13th October 2011

Smart Metering Implementation Programme – RollOut Team
Department of Energy & Climate Change
3 Whitehall Place
London
SW1A 2AW

Dear Sir,

Consultation on draft licence conditions and technical specifications for the rollout of gas and electricity smart metering equipment (Ref URN 11D/836):

Gemserv welcomes the opportunity to respond to this consultation relating to draft licence conditions and technical specifications for the roll-out of smart meters.

Gemserv specialises in the development and management of efficient and effective industry-wide governance arrangements. We are the leading specialist UK consultancy in market architecture design and trusted market assurance, with expertise in developing interoperability and creating frameworks for building consensus between market participants to ensure that critical processes work to the benefit of the GB market. Red Island Consulting, a subsidiary of Gemserv is Europe's most experienced provider of information security solutions and has led more than 120 organisations through to full ISO27001 certification.

This consultation is focussed on licence conditions and obligations which, in general, Gemserv supports as a key enabler for the roll-out of gas and electricity smart metering equipment. Underpinning the legal and regulatory arrangements robust governance must be established through either the Smart Energy Code (SEC) or the existing codes, as appropriate. Gemserv has focussed this response on those questions that relate to directly to our areas of expertise in energy and data security, where we can offer the most value and insight. For this reason we have provided a response to the following questions 10, 23, 28, 54, 55, 56, 57, 58, 59, 60, 61 and 62.

Furthermore in this document we have commented on DECC" s proposals, and include additional considerations that we believe are important for the roll-out of gas and electricity smart metering equipment and make specific reference to interoperability, dispute resolution and data security.

Question 10. What role could a dispute resolution mechanism have a role in ensuring interoperability? What key features should such a mechanism have?

Gemserv notes that the Prospectus included a reference to dispute resolution being a section of the Smart Energy Code (SEC), and this aspect of governance is a feature of existing codes in the electricity and gas sectors.

Gemserv believe that a dispute resolution mechanism is a fundamental requirement of contractual governance to enable a material issue to be appropriately progressed. However, formalising a dispute is not always the most effective means of progressing essentially operational issues. There are many examples of interoperability issues that have arisen over time in the energy sector, which have been resolved through collaborative and expert debate to drive towards a common solution. For example, a facility for open discussion of issues within the market arrangements is a useful means by which to create debate and obtain views from the community of industry participants in order to inform the most appropriate resolution.

Gemserv are of the view that any dispute and issue resolution mechanisms should be managed through the SEC and under the powers of the Panel, albeit not a function of the Panel itself. In this regard, a degree of self-governance is an important feature, since this provides for peer consideration of the issue in order to assess the implications. That is not to say that it may ultimately become a dispute between two parties, however it is important that matters of disagreement can be considered in an open way, to enable cases to be progressed in a holistic and consensual manner, since this approach ensures interoperability for the market as a whole.

In our experience of administering the Master Registration Agreement (MRA), a formal dispute between two or more parties is a necessary provision of a multi-lateral code, however it is not an ideal „ first call" and could be detrimental to „ market health" since disputes by their very nature introduce contention and conflict. Good governance should provide for a range of mechanisms to facilitate SEC parties having a means to debate issues and contribute to solutions, whilst at the same time ensuring that any party has recourse to arbitration and law if required.

Another factor to consider is the affect on performance on any one participant, and in this regard it should not be overlooked that the Data Communications Company (DCC) itself could be compromised by a DCC User" s interoperability issue. As the Consultation Document notes, there is a customer impact which may need to be resolved without undue delay.

Taking the above into account, the range of features that a dispute resolution mechanism should offer includes:

- Access to non-partisan advice through a helpdesk in order to gather more information or previous examples of perceived interoperability;
- A forum to raise issues for discussion and to seek wider views as to the remedy required;
- A responsive remedy process that recognises both licensee and customer outcomes; and
- An escalation route, which includes a staged reconciliation process, an independent nominated arbitration body, a defined decision-making process and a delegated expert group who can convene to consider technical and commercial matters.

Question 23. Do you think there are any consequential changes to existing codes needed in order to make the proposed roll-out obligations work correctly? Please explain your reasoning.

The roll-out obligations will chiefly be a compliance matter for Suppliers. However, it is to be expected that existing core industry documents, and particularly the supporting procedures and data catalogues, will require consequential modification at least to be able to recognise a smart meter is in place.

A rationale for such changes is that the portfolio of meter points that a Supplier holds is subject to losses and gains through normal market switching and customer acquisition activities. The Programme is keen to ensure that the customer" s switching ability is not compromised through the introduction of smart metering systems. Thus it is reasonable that the obligation to install a smart meter and the associated devices to complete the system are efficiently transferred as part of the Change of Supplier (CoS) process.

Visibility of whether a smart meter has already been installed at a metering point will be a crucial piece of information in the customer" s experience of a switch. This applies to an incoming Supplier being aware that either no smart meter is in place, in which case it needs to be included within that Suppliers roll-out plans; or that a smart meter is in place and whether the DCC is servicing that meter.

Indeed there are emerging requirements from within the Smart Metering Implementation Programme (SMIP) Workgroups that Suppliers wish current market processes and data sets to be modified to enable new smart meter data to be updated and exchanged at relevant market events. In particular, there is growing support for gas and electricity registration systems to be updated to

include new registration data. In the case of the electricity registration system, this would necessitate revisions to the MRA and, whilst the changes themselves can be developed and agreed under the MRA change procedures, Authority consent would be required to give effect to them.

It is anticipated that some Suppliers will begin deployment of smart meters prior to the roll-out being mandated to start. In this case, it is highly desirable that an incoming Supplier has early visibility of the type of metering at a premises, especially if this occurs during the period when the SMIP anticipates „ Smart CoS" being in force. The existing Electricity Central Online Enquiry Service (ECOES) is flexible enough to allow a rapid deployment of a cost effective solution to address the new data requirements for CoS.

Question 28. Do you think that the SMETS should ultimately be governed as part of the Smart Energy Code? What alternative arrangements could be adopted for the ongoing governance of the SMETS? Please explain your reasoning.

The SEC is the appropriate vehicle to manage the Smart Metering Equipment Technical Specification (SMETS), and could be incorporated as a schedule to the SEC. This arrangement provides the optimal governance and due change process for managing the evolution of the SMETS.

We believe that there may be a need for appropriate expert participation in managing the evolution of the SMETS and in this regard the principles from the Codes Governance Review will be applied to the SEC and it is expected that changes would be put to the widest consultation. Gemserv considers that an effective route to collate the views is a delegated expert group, constituted by the SEC Panel, who would provide an effectively and appropriate rigorous assessment and input to technical assessments and operational factors.

An example of this community approach to governance is the Meter Operation Code of Practice Agreement (MOCoPA) in the electricity sector, which comprises a balance of Meter Operators, Distribution Networks and Suppliers overseeing the successful operation of the MOCoPA. This could serve as a useful model when considering the constitution and terms of reference for a SMETS expert group. We also believe that there may be merit in establishing such an expert group even whilst the SMETS remains under the control of the Secretary of State, since any decision to amend the SMETS in this critical period needs to be fully informed by all relevant expertise.

Gemserv would observe that management of the SMETS was an early consideration of the Smart Meter Design Group (SMDG), whose recommendations included the establishment of a technical expert group as an initial matter for the SEC Panel at foundation. We consider their findings to be a sound basis upon which to develop a terms of reference for an expert group with delegated responsibility for evaluation and recommendation of revisions to the SMETS.

Question 54: 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.

Gemserv believes that it is vital that arrangements are in place to avoid disruption to the smart meter programme, and therefore that it is paramount that equipment is subject to assurance prior to roll-out.

The Government decision documents to date have given a strong direction that assurance and accreditation are likely to be features of the smart arrangements. These arrangements should be proportionate and not unduly burdensome but nevertheless effective and obligatory i.e. underpinned by regulatory obligations.

For the testing of technical and hardware components of the Smart metering equipment the consequences of delivery of components or complete installations that fail to provide the required functionality, interconnectivity, interoperability or security are the key consideration. Of course there will be hardware failures in such a large programme but these should be discrete and not the result of a failure to meet design criteria. Given the very large scale and intensity of the roll-out any systematic failure could result in similarly large scale disruption to the programme and high costs for correction.

Gemserv believe that the benefits of smart metering cannot be achieved simply by the installation of equipment. All participants in the smart market will have to deploy systems that support the infrastructure and fulfil more general market-level interoperability requirements. Assurance and performance monitoring are key facets of any interoperational market from start up to a managed handover in the case of a participant exiting the market. This has been, and continues to be, an important feature of the complex competitive markets as demonstrated by the electricity markets in Great Britain and Ireland.

It is important to de-risk impacts on the DCC arising from a performance failure by a DCC user. This can be achieved through up-front assurance to demonstrate that a participant" s systems and

business solutions are fit for purpose, including delivering the required interoperability functions, and pose no threats to the stability of market interoperation or fundamental security protections. Key to the integrity of this assurance is that it should be an independent function delivered under the market code and managed by the code administrator rather than, say, the DCC who is embedded within the performance regime.

It should not be overlooked that there will be overlaps with aspects of the market governed by existing instruments. There may be efficiencies in co-operation and collaboration between the other assurance bodies and the SEC, with perhaps a phased transition of key testing activities to the SEC as the smart metering population grows.

In either case, the Panel should be enabled to operate the appropriate assurance model independently, with accountability to the SEC parties, including the DCC. Gemserv believes that assurance should be managed under the SEC Panel in order to administer the appropriate controls and development of the overall performance and assurance regime. It may well be that the Code Administrator duties could encompass elements of these activities, or they may be provided by technical experts appointed by the Panel.

Question 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.

Gemserv believes that any assurance framework adopted should include a testing regime. The smart meter equipment to be installed by suppliers comprises a number of separate components that must conform to a defined specification (SMETS) so that they will interoperate according to smart requirements. The SMETS define the requirements for the individual components and not for the smart installation as a whole. This provides a number of important benefits:

- Components can be designed and manufactured by different companies and yet interoperate when connected at installation, thus creating a competitive market for components and thereby driving down costs;
- Components can be switched individually in the event of failure; and

- An improved component can be introduced into the installation without affecting other components or the installation as a whole.

Without a testing regime there would be uncertainty whether these benefits would accrue, since a complete installation may well function according to requirements, in spite of the fact that one or more components does not meet those requirements. This failure would become apparent only when some change is needed to the installation, for example if a supplier wanted to provide enhanced functions in one component to a customer who was switching to them, only to find that other components did not interoperate according to the requirement. By this stage, many thousands of invalid installations may have been completed.

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

Given the scale of the smart installation roll-out there will be great interest from manufacturers in supplying equipment. Naturally they will wish to supply whole installations rather than components in order to maximise sales revenue and profit. This may well also provide the most cost-effective procurement option for suppliers. Given this, a market-led approach to testing could well be ineffective in providing compliance at the component level since it will always be tempting for a manufacturer to make a cost saving in this area, whilst remaining able to demonstrate compliance at the installation level, especially when this is unlikely to be discovered for some time. For this reason a market-led approach is not favoured by Gemserv.

Either of the other two options would deliver the required assurance however Gemserv believes that the second option (.i.e. mandatory industry code to deliver and govern a testing regime) does have some advantages in the short term. The detailed work required to specify testing requirements/plans and design laboratory test equipment would undoubtedly reveal ambiguities, omissions or errors in the SMETS. This will result in revisions to the SMETS and thereafter the testing regime i.e. a feedback loop. It may be that this feedback loop would be much less responsive if independent test houses were involved since this would necessarily involve an arm" s-length commercial relationship, whereas if all testing-related activities fell under one industry body the commercial element would be less prevalent. In the longer term specifications should be more stable and it may be more cost-beneficial to employ independent expert test houses.

Question 57. Do you think that a different approach to assurance is necessary for the Foundation and enduring phases? Please explain your answer.

Gemserv believes that a different approach to assurance is necessary for the Foundation and enduring phase. In the short term the key objective is to implement smart metering on a wide scale.

In the longer term, however, smart metering will be established and there will be a greater emphasis on component cost and functionality (especially enhanced functionality). It is proven that a competitive environment is best placed to deliver lower costs with greater benefits. In this environment a different and cost-effective approach to assurance can be introduced as any non-compliance is likely to be both limited in scale and discovered quickly.

Question 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?

The activities are certainly a suitable way to achieve interoperability within the Cryptographic requirements. It will be essential that for the integrity of the encrypted data that the implemented controls are consistent across the entire process, between organisations and systems, and not just in the meters. The design of the cryptographic solution must be consistent across all entities. In addition it allows the possibility of more centralised encryption key management processes, possibly by the DCC or SEC to ensure keys are properly controlled and protected.

The solution could alternatively be achieved by development of cryptographic standards rather than a holistic design, allowing each entity to implement the relevant cryptographic solutions within the defined parameters. However, in our view this would lead to much greater risk of poorly implemented systems and controls, and greater effort required to audit and verify implementation and security.

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

It is fair to say that cryptographic / key management is a sensible precaution to protect the security of smart metering systems. Moreover, in the context of smart metering systems being part of the Critical National Infrastructure, any vulnerability might expose it as a target for malicious attack, for both fraudulent purposes to manipulate billing and payment processes, as well as malicious

attacks on individuals, organisations and the GB Infrastructure itself for the purpose of disruption, or theft of personal / sensitive information.

As well as non-authorised attempts to obtain access to and tamper with meter data, the nature of the energy and metering business is that many organisations and therefore individuals will have access to multiple components and touch points of smart metering data, in transmission over networks and devices, processing in applications and systems, and at rest id databases. It should be noted that organised security attacks often focus on authorised employees, or involve the placement of malicious individuals in authorised organisations.

Cryptographic protection of the systems and data across the entire system is essential to reduce the exposure to interception or manipulation of data in all areas of the process, both by non-authorised personnel as well as authorised personnel and organisations. The basic premise should be that access is granted on a " need-to-know" basis. Experience in the Payment Card Industry Data Security Standard has shown that removing the potential to access data, even from those that may be authorised but have no need, greatly reduces the risk of loss or theft of data.

Question 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.

We agree with the assessment of the three main solutions listed. However Gemserv believes that there are additional risks associated with each solution, such as the risk of a breach of a symmetric key, even in a hybrid solution that could cause significant exposure and cost. The use of a Certification Authority (CA) would introduce additional security considerations around the CA itself, however, the risks of securing and transmitting symmetric keys over unsecure networks has its own significant level of risk.

The solutions are certainly the three most suitable options, but additional security risks as well as business advantages and disadvantages should be considered for the three options and factored into the decision making process.

Question 61. 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.

Gemserv believes that there is a need for one organisation to own the cryptographic key management. The DCC is certainly a possible option, however the DCC will also be a user of the

cryptographic solution, and the risks around collusion and internal breach would need to be considered and managed. It would be essential for the DCC to have an independent information security function with sufficient skills and knowledge in cryptography to manage the systems. However, properly managed and proper internal segregation would make this a viable option. We would recommend additional oversight and audit of the key management by an independent entity separate from the DCC, perhaps under the auspices of the SEC Panel.

Alternatively a separate organisation could take responsively for the key management and implementation. This could be an independent expert organisation, or could potentially be a government organisation i.e. the National Technical Authority for Information Assurance, that is already experts in cryptographic management and control.

Question 62. 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.

We believe the same principles and processes should apply to opted-out non-domestic consumers to ensure consistency and integrity. In addition, should such consumers decide to opt-in, the changes would be more easily facilitated if the same security processes are already implemented. Obviously this may add additional cost and overheads to opt out consumers which may affect commercial models.