



**Secure Electrans Limited**

**Smart Metering Implementation Programme:  
Consultation on Draft Licence Conditions and  
Technical Specifications  
for the Roll-out of  
Gas and Electricity Smart Metering  
Equipment  
(August 2011)**



## **Abstract**

This document provides feedback to the United Kingdom Department of Energy and Climate Change consultation on Draft Licence Conditions and Technical Specifications for the Roll-Out of Gas and Electricity Smart Metering Equipment, Reference Number 11 D/836.

## **Introduction**

Secure Electrans supports the evaluation being undertaken by the Department and welcomes the opportunity to provide responses to this consultation. In the context of Smart Metering Equipment, Secure Electrans develop Enhanced In-Home Display devices; as such, our responses are limited to the topics within our scope.

## **Secure Electrans Responses**

Q1: No response

Q2: No response

Q3: No response

Q4: No response

Q5: No response

Q6: No response

Q7: No response

**Q8: What contribution do you think the interoperability licence condition as drafted could play in ensuring that suppliers work together to ensure Smart Metering Equipment is interoperable?**

The interoperability licence condition requires all suppliers, and therefore presumably their equipment providers, to agree on a common standard or standards, and then ensure that the Smart Metering Equipment is interoperable. This approach encourages the interoperability of equipment, irrespective of the supplier that installed it.

**Q9: Do you think the licence conditions as drafted effectively underpin the policy intention to ensure Smart Metering Equipment is interoperable?**

The condition preventing the replacement of equipment, coupled with the requirement for remote re-configuration, should both encourage interoperability and at the same time ease the change of supplier for the customer. However, although remote upgrading of equipment is beneficial, care must be taken to ensure backward-compatibility wherever possible.

**Q10: What role could a dispute resolution mechanism have a role in ensuring interoperability? What key features should such a mechanism have?**

Secure Electrans believe that a dispute resolution mechanism should be used as a last resort, if at all. It is more important to specify suitable open standards with proven interoperability, then put in place suitable test and certification processes to ensure manufacturers comply with those standards.

Q11: No response

Q12: No response

Q13: No response

Q14: No response

Q15: No response

Q16: No response

**Q17: What period of notice do you think would be appropriate before the obligation to provide an IHD comes into effect?**

In order to speed up development, many manufacturers will have made assumptions on the requirements and technology to be used. If the technology eventually chosen is not the same as that assumed, then significant delay may occur. Until final requirements are frozen, final design cannot be concluded either, and that can have a significant effect where the design of components (e.g. custom displays) is dependent on those requirements/design. Note also that, for interoperability, the SMETS is probably not the specification against which product is designed; it is likely that the requirements of the SMETS will have to be reflected into the standards of whatever technologies are chosen for the Smart Metering system.

Assuming that IHDs are designed and ready for manufacture ahead of the notice period, component procurement times must be taken into account; although it is assumed that manufacturers will try and avoid long lead-time components, 26-week lead times on critical components are not unheard of. There will also be ramp-up times for a manufacturing plant (say 6-8 weeks).

**Q18: Would the consumer changing their supplier raise any particular issues with regard to the approach set out for the provision of IHDs?**

So long as the programme ensures interoperability between the supplied Smart Metering Equipment, we do not envisage any serious issues if the consumer changes their supplier. It is assumed that the SMETS will ensure provision for reconfiguration of an IHD on Change of Supplier. Changing supplier within the first 12 months following supply of an IHD could result in the device having to be replaced within that period if the original device becomes faulty (the new supplier may not carry the same make of device). Consideration should be given to the case where, following payment for an Enhanced IHD to one supplier, the customer switches supplier to one that does not support the enhanced features provided by the purchased device.

**Q19: Do you think the licence conditions as drafted effectively underpin the policy intentions set out for the provision of IHDs to domestic consumers?**

Other than the points made above, Secure Electrans believe that the licence conditions as drafted effectively underpin the policy intentions set out for the provision of IHDs to domestic customers.

Q20: No response

Q21: No response

Q22: No response

Q23: No response

**Q24: Do you think that there are other requirements that the Government should adopt in the SMETS?**

In general, Secure Electrans believe that the IDTS satisfies the requirements for the UK Smart Metering system. However, we believe further review of the document is required to remove the inconsistencies that inevitably result from the combined output of various bodies.

**Q25: Do you agree that all the requirements recommended in the IDTS should be adopted by the Government in the SMETS?**

There is evidence of the same information or similar information which could be derived from other data, being requirements of the system; this could have a detrimental effect of both memory requirements of the various elements and bandwidth on the various communications links required within the system. Whilst the minimum requirements for the various aspects of the system must be defined, care must be taken to avoid stifling innovation of more advanced offerings (as an example, power limitations on an IHD may prevent the inclusion of features that a customer would be willing to support on a separate device providing similar functionality).

**Q26: Do you agree that the security requirements recommended in the IDTS are proportionate to the level of risk that the End-to-end Smart Metering System faces?**

We believe that the security requirements are proportionate to the level of risk that the end-to-end system faces, protecting the critical elements and providing limited access to customer's personal data.

Q27: No response

Q28: No response

Q29: No response

**Q30: Do you agree that the Government should include a requirement for a Communications Hub in the SMETS?**

The provision of a Communications Hub would eliminate the dependency of gas-first installations on a smart electricity meter, and would provide a logical boundary between the HAN and WAN technologies. However, Secure Electrans do not have a strong view on this matter, but believe that any related technologies should not be reliant on particular system architecture.

Q31: No response

Q32: No response

Q33: No response

Q34: No response

Q35: No response

**Q36: Do you agree there should be no restrictions on the HAN standards adopted by suppliers, provided they are available as a European (CEN, CENELEC or ETSI) or International (IEC or ISO) standard?**

By not specifying a HAN standard, Secure Electrants believe that there will be a dilution of resources in an environment of increasingly challenging timescales; standardising on a particular main HAN standard at this stage would provide focus and will increase the chances of successful interoperability (it is recognised that other technologies will have to be considered for problem sites).

**Q37: The IDTS has recommended that all standards should be recognised or be in the process of being recognised by 31 December 2014; do you agree with this recommendation?**

We do not believe that any existing or proposed European or International standard will currently satisfy the GB requirements, and therefore consideration should be given to those technologies willing to accommodate the required changes.

**Q38: Do you think that regulatory obligations are needed to underpin a systematic approach to testing of HAN standards during the Foundation phase?**

Rather than creating new regulation, it is recommended that standards are chosen that already provide their own, proven, testing and certification process.

**Q39: Do you agree with industry's recommendation that DLMS should be adopted as the application layer for communications with the DCC? Do you believe there are any consumer, economic or technical issues with this solution which could be circumvented by an alternative approach?**

Secure Electrants has no particular opinion on the application layer to be used for the WAN connection to the DCC, so long as the chosen protocol does not have a detrimental effect on the SM HAN.

**Q40: Do you agree with industry's recommendation that DLMS and Zigbee SEP 1.x should be adopted as the application layer for communications within the consumer premises, provided they install the necessary translation equipment? Do you believe there are any consumer, economic or technical issues with this solution which could be resolved by an alternative approach?**

Secure Electrants believe that ZigBee SEP1.x offers the best solution as the application layer to be used for the SM HAN; it has already been proven in similar Smart Metering implementations and the structure of its two-way communication techniques, coupled

with fundamental security, allow it to make efficient use of the available bandwidth whilst maintaining the confidentiality and protection of critical elements of the system. Recent experience suggests that it could be readily adapted to suit the particular requirement of the UK market. ZigBee SEP 1.x is capable of 'tunnelling' a number of other protocols.

Q41: No response

Q42: No response

Q43: No response

Q44: No response

Q45: No response

**Q46: Do you agree with the proposed approach for consumers to access data and transfer it from the HAN via a separate "bridging" device?**

We believe that the approach proposed allows consumer access to data in a manner controlled by a device trusted by the SM HAN, whilst not interfering with the core functionality of the SM HAN. Depending on the HAN technology selected, there are already devices in existence capable of performing the 'bridge' functionality.

Q47: No response

Q48: No response

Q49: No response

**Q50: Do you agree that the IHD should only be required to display ambient feedback based on energy usage?**

Whilst the limitation of ambient feedback to energy usage only, in the minimum requirements for a compliant IHD, makes sense, the ability for more complex devices to provide additional information should not be suppressed; such functionality provides a differentiator between products.

**Q51: Do you agree that Smart Metering Equipment should be designed to support the calculation and/or display of account balances as described above, even though suppliers may not initially be mandated to invoke such functionality for credit customers?**

Assuming that the same (or compatible) tariff 'table' is used for both Prepayment and Credit accounts, Secure Electrans believe that there should be little increased functionality required by the applicable algorithm(s) to handle accrued credit (for credit customers) as well as remaining credit (for prepayment customers). The transfer of account balance from supplier to IHD could be as simple as a text/display message; however care must be taken in the design of IHDs to clearly differentiate between real-time consumption information and supplier-provided account information.

**Q52: What do you think the costs and benefits are of mandating suppliers to display an account balance (over-and-above those arising from display of information on cumulative cost of consumption) for credit customers on their IHD?**

As stated in the commentary, the benefits of providing an actual account balance/bill via the Smart Metering system is questionable when this information is already provided via other means (and is likely to continue to be). We do not believe that there would be a significant increase in cost within the SM HAN to handle this additional information; cost within the DCC and supplier systems may be more significant.

**Q53: Do you agree with or have any comments on the Government's proposals for the outstanding issues from the Response?**

It is assumed that the current draft data catalogue has been complied without regard to any particular protocol. There will therefore be an opportunity to improve the efficiency of these data structures if they are tailored to the particular technologies chosen to be used with the Smart Metering system.

**Q54: 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?**

Rather than creating new frameworks, it is recommended that standards are chosen that already provide the required functionality, interconnectivity, interoperability and security. Several standards already provide their own, proven, testing and certification process.



**Q55: 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?**

Equipment should be required to pass a testing and certification process. This is commonly administered by certified test laboratories. Only equipment certified by this process should be allowed to be used.

**Q56: What are your views on the options outlined for a testing regime? Are there other options that should be considered?**

Secure Electrans would favour a certification scheme whereby equipment has to pass a testing and certification process administered by certified testing laboratories. This approach has already been successfully implemented by a number of communications standards.

**Q57: Do you think that a different approach to assurance is necessary for the Foundation and enduring phases?**

We believe that the same approach should be applied to the Foundation phase as used for the enduring phase. Equipment developed for the Foundation phase may have to interoperate with equipment installed for the later stages. Earlier deployment of the assurance framework at the Foundation phase will provide a proving ground for the later phase.

**Q58: Do you think that the activities outlined above are a suitable way for achieving interoperability across Smart Metering Equipment cryptographic functionality?**

Secure Electrans believe that the development of an end-to-end trust hierarchy and cryptographic key management, together with the use of common cryptographic interfaces, are needed to protect against unauthorised modification, injection and disclosure of sensitive data and critical commands. Due to the variety of WAN technologies that could be employed, there may need to be different schemes employed for the HAN and WAN networks, however care must be taken at the point where the two domains meet.

**Q59: Do you agree that cryptographic/ key management is necessary to secure the End-to-end Smart Metering System?**

Cryptographic key management is necessary to secure the end-to-end Smart Metering System; this is typically performed using asymmetric cryptography and PKI.

**Q60: 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?**

Although the categories identified in Table 7 appear correct, some of the stated advantages and disadvantages are not. Digital certificates themselves do not protect against repudiation, although signing using the associated private key will. In the hybrid case, shared keys are typically created using key agreement (although the mechanism can also be used for secure transportation)

**Q61: 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?**

From the options stated in Table 7, Secure Electrans believe that the Hybrid option would be the best approach; use an asymmetric method to create or share symmetric keys, then use the resultant symmetric key for more efficient general command/data transfer. Although the use of a CA does incur cost, the proposed structure of the Smart Metering System does favour a centralised trust model rather than de-centralised solution such as a 'Web of Trust'. The DCC would be an obvious candidate to manage this trust model, or another, associated central body.

**Q62: How do you believe the security approach should be applied to opted out non-domestic consumers? Do you see any issues with the approach?**

Assuming that 'opted out' refers to the lack of an In-Home Display, Secure Electrans believes that there will still be a need to secure the transfer of fiscal meter data from meter to DCC, and therefore the same security approach will be required.

-- END OF DOCUMENT --