



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

Infineon Technologies UK Ltd  
Infineon House,  
Great Western Court,  
Hunts Ground Road,  
Stoke Gifford,  
BRISTOL BS34 8HP

[REDACTED]  
[REDACTED]  
[REDACTED]  
28 October 2010

**Subject: Smart Metering implementation programme: prospectus**

Dear Madam

With reference to the prospectus documents published on the 27<sup>th</sup> of July 2010, we would like offer some response to those specific questions as we feel we are qualified to answer.

Infineon Technologies AG based in Germany, offers semiconductor and system solutions addressing three central challenges to modern society: energy efficiency, mobility, and security. In the 2009 fiscal year (ending September), the company reported sales of Euro 3.03 billion with approximately 25,650 employees worldwide.

In the field of smart meters Infineon offers products for the metrology, controllers, communications, and power management. Infineon supplies products to many of the world's metering companies.

As key partner of the security industry, Infineon contributes a quarter-century of security expertise gained in the development and production of chip card ICs and security ICs to the effort to increase the security of today's solutions in reliable identification of persons and goods, payment and banking, communications, access protection for data and networks, and digital home entertainment electronics. Infineon has been the world market leader in chip card ICs for twelve consecutive years.

It is with this focus of the need for security in smart metering we have focussed our response, as we believe that security has to be specified and designed in at the very beginning of a programme if security measures are to be effective throughout the lifetime of the system.

Infineon has worked with several UK government agencies to provide security advice and support on various different programmes. We gladly extend our offer of such open advice to the various Ofgem advisory working groups or Committee of Experts if requested.

In the following submission we have used your document references and question numbers to help with assessment. If there are any queries or concerns please do not hesitate to contact me.

Yours Faithfully

[REDACTED]

[REDACTED]

# Smart Metering Implementation Programme: Prospectus

## Chapter 2 Customer Experience

<b>Q1</b>	<b>Helping consumers understand their energy use:</b> Do you have any comments on the proposed minimum functional requirements and arrangements for provision of the in-home display device?
	The IHD requires a secure data communication because it may be physically separated from the meter and or the HAN module. If the IHD become an input device for entering prepayment token data, during WAN network outage, then there is even a great need for data security. In either case the IHD should be equipped with a dedicated hardware security module to enforce protection against attacks. The hardware security module should be certified according to an appropriate international standard.

<b>Q2</b>	<b>Data Privacy and Security:</b> Do you have any comments on our overall approach to data privacy?
	A dedicated security profile has to be created and according which the devices can be accredited to from various suppliers. This will help enable interoperability of data communication, and ensure that private data is protected at all times

<b>Q4</b>	<b>A new approach to debt management and prepayment:</b> Have we identified the full range of consumer protection issues related to remote disconnection and switching to prepayment?
	The ability for remote disconnect may make the system vulnerable to attacks and misuse. Remote disconnect requires strong data security means to avoid misuse. It is advisable that security evaluations and certification according ISO/IEC 15408 should be applied and at least EAL4_+ High is chosen that assures tamperproof components on the printed circuit board level for all smart meters components and communication units involved in data handling of remote disconnect commands.

## Chapter 3 Industry Roles and Experience

<b>Q9</b>	<b>Scope of activities:</b> Do you have any comments on the proposal that the scope of activities of the central data and communications function should be limited initially to those functions that are essential for the effective transfer of smart metering data, such as data access and scheduled data retrieval?

<b>Q15</b>	<b>System security:</b> Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?
	A dedicated security profile has to be created and according which the devices can be accredited to from various suppliers to ensure data integrity.  It is advisable that security evaluations and certification according ISO/IEC 15408 should be applied and EAL4+ high is chosen for the tamperproof/tamper-indicating components on the printed circuit board level for smart meters and concentrators.

## CONSUMER PROTECTION Ref: 94a/10

### Chapter 3. Prepayment and remote disconnection

<b>Q6</b>	<b>Do you consider that existing protections in the licence are sufficient to ensure that consumers are not remotely switched to prepayment mode inappropriately?</b>
	The consumer must have the final authority, therefore the supplier authentication stored in the meter, should include a digital signature of the consumer: this signature could be invoked by use of web based transaction authenticated by use of a One Time Password (OTP) or by telephone using dial up options and again input of (OTP). The OTP could be sent to the consumer via letter or SMS when the supplier confirms the switching of supplier.

<b>Q7</b>	<b>Could provision of an appropriate IHD help overcome meter accessibility issues to facilitate prepayment usage?</b>
	If the IHD become an input device for entering prepayment token data then there is even a great need for data security. The HAN software radio protocol may not satisfy payment industry security requirements. The IHD then needs a security certification function which should be enforced by a dedicated hardware security module.

<b>Q15</b>	<b>Have we identified the full range of consumer protection issues associated with the capability to conduct remote disconnection or switching from credit to prepayment terms? If not, please identify any additional such issues.</b>
	The ability for remote disconnects and payment updates make the system vulnerable to attacks and misuse. Data traffic levels may be subject to eavesdropping or other analysis from which consumer presence or behaviour can be determined. As stated above it is advisable that security evaluations and certification according ISO/IEC 15408 should be applied and EAL4+ high is chosen for tamperproof/tamper-indicating components on the printed circuit board level for smart meters and concentrators, and that the software is encrypted and managed so that consumer information is not transported in clear or a low security software enciphered text.

# STATEMENT OF DESIGN REQUIREMENTS ref 94b/10

## Chapter 3. Overview of the design requirements

<b>Q1</b>	<b>Should the HAN hardware be exchangeable without the need to exchange the meter?</b>
	Yes: to allow long term interoperability and security the HAN should be exchangeable without the expense of changing the meter, if this the most cost effective approach. A few installations may have issues with the RF spectrum /protocol used by an HAN, so exchangeable HAN module maybe a useful option for some installers. For Gas meters power consumption is crucial so upgradeable HAN interface may reduce the need for battery replacement visits

<b>Q2</b>	<b>Are suitable HAN technologies available that meet the functional requirements?</b>
	Yes, but care should taken to allow appropriate security: The HAN hardware may be used as a tool to attack the meter and the overall networks. HAN hardware can be easily proliferated and can be used as tools to distribute criminal services as happened in the past with fake pay-tv cards and TV set top boxes We advise that HAN hardware should have appropriate security in place and should be part of the security evaluation according to ISO/IEC 15408. To control the ability critical authentication and communication stacks should be protected by a dedicated security controller mandated and approved by the appropriate information assurance authorities e.g. CESG

## Chapter 5. Achieving Technical Operability

<b>Q7</b>	<b>Do you agree that the proposed approach to developing technical specifications will deliver the necessary technical certainty and interoperability?</b>
	Yes the approach seems correct, but a dedicated security profile has to be created and according to which devices can be accredited to from various suppliers to help deliver the necessary level of technical certainty

## **IN HOME DISPLAY (IHD) ref 94c/10**

### **2. Functional Requirements of the IHD**

<b>Q6</b>	<b>Do you agree with the proposed minimum functional requirements for the IHD?</b>
	The minimum functional requirements need to be changed to reflect the needs for security.

### **3. Nature of the Mandate on Suppliers in relation to the IHD**

<b>Q8</b>	<b>Do you agree with the proposals covering the roles of and obligations on suppliers in relation to the IHD?</b>
	There are suggestions within the supplier community to allow the IHD to have a two way function, i.e. to be able to input data to the meter in case of WAN failure to allow pre-payment updates. This would then require the IHD to be included in the security protection profile to ensure it cannot be misused.

# COMMUNICATIONS BUSINESS MODEL ref 94d/10

## Chapter 2. The Scope of DCC

<b>Q1</b>	<b>Do you agree that access control to secure centrally-coordinated communications, translation services and scheduled data retrieval are essential as part of the initial scope of DCC?</b>
	Yes, the DCC services should be accredited to a security standard such as BS1799/ISOIEC 17799

<b>Q4</b>	<b>Do any measures need to be put in place to facilitate rollout in the period before DCC service availability and the transition to provision of services by DCC, for example requiring DCC to take on communications contracts meeting certain pre-defined criteria?</b>
	<p>DCC must assure that all appropriate means are in place to assure that proper security measures are in place to protect the service against criminals and cyber terrorists.</p> <p>Special care must be taken with respect to smart grid network nodes that are easily accessible and where access cannot be protected by physical means. This applies to smart meters and concentrators. It is advisable that security evaluations and certification according ISO/IEC 15408 should be applied and EAL4+ high is chosen for tamperproof/tamper-indicating components on the printed circuit board level.</p>

## 3. The Structure and Realisation of DCC

<b>Q7</b>	<b>Do you have any comments on the steps DCC would need to take to be in a position to provide its services and the likely timescales involved?</b>
	To fulfil the requirements stated previously the DCC should assure that respective security protection profiles are available and the regulatory obligation is passed.

## DATA PRIVACY AND SECURITY ref 94e/10

### Chapter 4. Smart Metering System Security

<b>Q5</b>	<b>Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?</b>
	<p>The approach is clear, but there is no security profile (or at least publically available). There is a need within e-commerce legislation in the UK and EU to ensure that transactions are protected using security standard ISO/IEC 15408 to be at least Common Criteria EAL4+ High.</p> <p>The smart metering system must protect the personal and payment data using technology which meets these requirements. It is unlikely that a meter or its standard components could meet this need economically. The inclusion of a Hardware Security Module (HSM) in the form of a dedicated certified security controller is the most cost effective solution. The same concept has been successfully used in GSM systems by use of a SIM, PC trusted networking with the use of TPM, and several other consumer equipments. In this way the Smart Metering Systems components can be built cost effectively and the security focused on a single device in each unit i.e. a certified HSM that will meet the need for end-to-end security.</p>

## REGULATORY AND COMMERCIAL FRAMEWORK ref 94h/10

<b>Q1</b>	<b>Have we identified all of the key elements that you would expect to see as part of the Smart Metering Regulatory Regime?</b>
	<p>There is no guidance on the independent security certification of the equipment. There is a need within Ecommerce legislation in the UK and EU to ensure that transactions are protected using security standard ISO/IEC 15408 to be at least Common Criteria EAL4+ High.</p> <p>The smart metering system must protect the personal and payment data using technology which meets these requirements. It is unlikely that a meter or its standard components could meet this need economically. The inclusion of a Hardware Security Module (HSM) in the form of a dedicated certified security controller is the most cost effective solution. The same concept has been successfully used in GSM systems by use of a SIM, PC trusted networking with the use of TPM, and several other consumer equipments. Smart Metering Systems with a certified HSM will meet the need for end-to-end security.</p>



## NON-DOMESTIC SECTOR ref 94i/10

<b>Q10</b>	<b>Do you agree with our approach to data privacy and security for non-domestic customers?</b>
	<p>There is a need within Ecommerce legislation in the UK and EU to ensure that transactions are protected using security standard ISO/IEC 15408 to be at least Common Criteria EAL4. The smart metering system must protect the personal and payment data using technology which meets these requirements. It is unlikely that a meter or its standard components could meet this need economically. The inclusion of a Hardware Security Module (HSM) in the form of a dedicated certified security controller is the most cost effective solution. The same concept has been successfully used in GSM systems by use of a SIM, PC trusted networking with the use of TPM, and several other consumer equipments. Smart Metering Systems with a certified HSM will meet the need for end-to-end security.</p>