



Ofgem Smart Metering Implementation Programme:

Data Privacy & Security consultation: Renesas Electronics Europe response

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

The approach itself looks right. The point we would make is that, in order for any provider to claim his ability to meet the security requirements, it would be necessary to go further into the expression of these requirements. Let us clarify this statement as follows:

Going through the process of implementing a secure information system, there are 4 necessary step :

- 1/ Identify the assets to be protected
- 2/ Identify threats (possible attacks) and vulnerabilities
- 3/ Decide the list of attacks the system MUST resist against (and eliminate, or make optional, those which seem to be un-realistic, or only “nice to have”).
- 4/ Define appropriate countermeasure.

The document covers mainly the first 2 items and leaves open the item 3/ and 4/.

The assets to be protected onto a secure platform are usually:

- cryptographic keys
- platform issuer data
- IPs: algorithm, code,...
- Private data

At platform level (chip/terminal) there are so many types of attacks :

- Invasive attacks
 - o Reverse engineering
 - o Probing
 - o FIB (Focused Ion beam)
- Passive attacks
 - o Timing attacks
 - o Side-channel analysis (Power, EM,...)
- Active attacks
 - o Fault attacks
- Others...

For « appropriately » securing a smart meter and the end to end communication, what is the relevant list of attacks the system must resist against? What are the ways to specify this, and then to check that each solution complies –or does not- to these detailed security requirement ?

One simple answer to the above question would be to refer to what the smart card industry has done, especially regarding the security features and certification schemes.



Ofgem Smart Metering Implementation Programme:

Implementing a piece of silicon similar to a smart card chip in term of security features into a smart meter would allow :

- 1- To bring a decisive contribution in term of security by ensuring :
 - a. Strong (mutual) authentication between the smart meter and the head end computer
 - b. Data confidentiality (encryption)
 - c. Data integrity (hashing)
 - d. Non-repudiation of any transaction or information transmission (digital signature)
 - e. Secure storage of platform assets into a tamper resistant area
- 2- To bring a high degree of security that can be **measured and evaluated** against existing security schemes.

The above call for more detailed discussions and Renesas would like to keep in contact with the Smart Grid stakeholders in order to contribute building a safe and secure Smart Grid.