Comments to the document: "A call for evidence on data access and privacy"

Author:

[redacted]

STMicroelectronics

Via Olivetti 2, Agrate B.za

20041 Milano

Italy

[redacted]

[redacted]

Question 18

What current and future technical options exist for energy consumption data minimisation / privacy enhancing technologies? How might aggregated or anonymised data be provided in practice? Would this imply additional services to be provided by DCC?

There are new schemes making use of homomorphic encryption or similar techniques for improving privacy in the process of elaborating the bill of energy consumption for the final customer.

These techniques are very interesting and are opening a new research chapter. Right now these are not mature and needs some time for reviews and acceptance by the research community. In sight of this possible evolution of security primitives and considering that the expected life cycle of a meter is expected to be 10+ years, it is recommended that the security should be upgradable, via software upgrade or with the possibility to replace the secure element (like the SIM card used in mobile phones)

Questions

21. What practical options for authentication would provide the right balance between allowing easy access to consumer data in the home while providing the necessary privacy protection? Are there any other issues or options that the programme should be considering in developing the approach in this area?

22. Are there other issues that need to be considered to make using the HAN a viable route for access to data in the home, from either a process or consumer perspective?

Unified comment for the two questions

The key management infrastructure should consider the possibility of accessing data with different privilege levels.

In home data visualization could be done via utility network for simplicity. It might be easier to access data with a smart phone via internet compared to create a link between a smart phone and the meter via power line communication or radio frequency link (zigbee for instance). These connectivity links are very common for meters but are not supported by most consumer devices, like smart phones, tablet or personal computers. Otherwise a dedicated device for displaying information has to be adopted (supporting the direct link with the meter).

The possibility of accessing data via a standard device has to be careful studied. It can be seen as an exception of the end-to-end security paradigm, where the new end is now a consumer device that might not be able to guarantee an acceptable level of security.