

Diaphragm gas meters used in smart metering

Precise and secure!

By far one of the hottest topics of discussion in European utility companies today is the introduction of "smart" meters. The further the discussions about full-coverage roll-out go, and the more small and medium pilot projects are implemented, the clearer the consequences become. Besides the technical and logistic challenges are requirements for custody transfer of metering data that should not be underestimated, and therefore tasks for the Federal and regional data protection officers or authorities.

A brief review

On 7 April 2009, the Dutch parliament rejected an initiative put forward by its own Ministry of Economic Affairs, which required the compulsory introduction of "smart" meters for all households. Consumers who rejected the installation would have faced a hefty fine or even imprisonment. Consumer protection organisations expressed their concerns, however, claiming that the security of the data to be transferred, and the possibility that personal data could fall into the hands of third parties, would connote an infringement of the European Convention on Human Rights. The initiative for the compulsory introduction of "smart" meters has therefore been rejected for the time being.

The present situation

The topic of data security in smart metering has come to the fore in other countries too, not least in the face of the current scandals concerning data abuse. Utility companies and consumer protection organisations and initiatives are challenged with the task of ensuring personal data protection. The German Federal Association of the Energy and Water Industry (BDEW) has already compiled a draft for a data protection information publication on the topic of smart metering.

In this context, the so-called Big Brother Awards have been distributed each year since 2000. This is a negative award for companies, organisations and individuals threatening people's private sphere, or



making personal data accessible to third parties. The German Big Brother Awards aim to reveal improper use of technology and information.

The effects of such data abuse are enormous. Ultimately, however, the protection of personal data is not the only concern: there is also the vulnerability of critical infrastructure systems and thus of security of supply. The Wall Street Journal, for example, reports that US security experts have established that the US power network is a target of cyber spies abroad time and again. Computer specialists have discovered corresponding software with which parts of the US supply infrastructures can be put out of operation. This

vulnerable infrastructure is critical, whereby any attack by peaceably-minded hackers simply looking for a new challenge appears virtually harmless, especially in direct contrast to the possibilities and intentions of a terrorist organisation.

Security with a capital "S"

The security and encryption of personal data has to be a must when introducing smart metering. Thus corresponding security concepts must be incorporated into existing and new smart metering systems and take new processes into account, such as the exchange of encryption mechanisms between manufacturers

and energy suppliers, for example. In terms of Elster gas meters, communication protocols will in future be transferred encrypted. Thus personal data and critical commands such as the closing and opening of a valve integrated in the meter, can neither be seen by third parties nor intercepted or simulated. The communication protocols will be transferred encrypted in accordance with the Advanced Encryption Standard (AES) 128 (AES encryption is permitted in the USA for state documents of the highest secrecy level).

In the future, the exchange of data between meter and system will be encrypted with a user key. To ensure that it will not be possible for the user key to be illegally

“overheard”, future “smart” meters will be equipped with a so-called default key at the works. This default key is made available to the utility company via a secured file transfer protocol connection, for example, and assist in the encryption of the user key. This way secure data communication can be achieved.

The use of “smart” meters will make the introduction of the above processes for ensuring data protection inevitable. Obviously, the usual ordering and logistic procedures surrounding standard meters will become more complex with the introduction of “smart” meters and careful planning and consultation between the utility companies and the manufacturers is required.

Of course this article should not stir up any fears about cyber attacks and complicated procedures, but similarly we do not want to act as though all the hurdles have been cleared. What is certain is that we at Elster are taking this matter seriously, so that we can competently support our customers with the implementation of smart metering – rest assured!

Carsten Lorenz carsten.lorenz@elster.com