

Data security in AMR systems: Safety first!

On 15 February, the Telegraph published an article entitled "Smart meters in homes could be hacked". At least, that was the conclusion reached by an advisor to the British government.

In many countries, data security in smart metering systems has now become a question of national security in the course of introducing smart metering. In this article, links and solution approaches for data protection in these systems will be discussed.

A possible smart metering infrastructure is shown in Fig. 1. In this system, it is important to protect the features of confidentiality, integrity and availability, in order to ensure security. The qualities that distinguish a secure system are detailed below. And specific measures need to be implemented in order to achieve these qualities.

Confidentiality

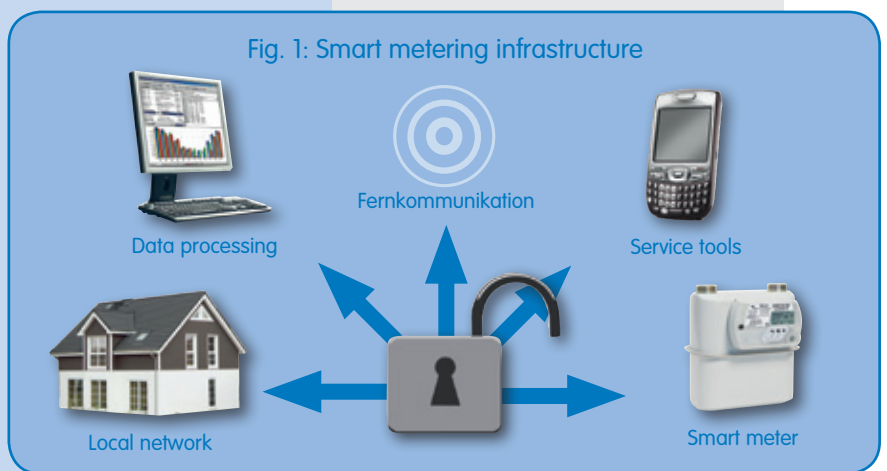
This is the first feature of security. Confidentiality means that information is never conveyed to unauthorized third parties. Everyone expects, for example, that their e-mails are not read by unauthorized persons.

Integrity

This is the second feature of security. Integrity means that the information is never modified in an unauthorized way. A meter with a shut-down facility must therefore be able to ensure that it is switched off only when a switch-off command is given by an authorized party.

Availability

This is the third feature of security. Availability means that a smart metering system always responds to enquiries and commands from authorized parties. A typical hacking scenario is the so-called "denial of service". Here, a system is blocked with so many enquiries that it is no longer able to respond in the required time and, as a result, information needed for network control, for example, is no longer available.



These three features are taken into account in a smart metering system with encryption, authentication and authorization measures.

Encryption

Using an algorithm, encryption transforms the information that is to be protected into a format that third parties cannot read. A current algorithm that may often be found is AES-128. The AES algorithm, for example, is approved in the USA for official documents of the highest secrecy level.

Authentication

Authentication ensures that agents that want access to the smart metering system are in fact who they are supposed to be.

Authorization

Authorization defines what an agent is allowed to do, once they have been authenticated. Mobile phone networks or online banking systems can be seen as analogies for the smart metering system. Here, it is standard practice to set up so-called "end-to-end security". This means that only both agents involved know about codes used and the communication link between them is only used for transferring data. So-called asymmetrical procedures

with a private and a public code respectively for each agent recommend themselves here. This has the advantage that the private code (which must be kept secret) only needs to be saved in once place.

For authorization purposes, appropriate roles need to be defined, for which particular rights are then granted. To give an example, a service engineer performing a battery change on site must activate the authorization for his role on the meter using suitable codes. The same applies for carrying out a firmware update on the installed communication module. In this way, the possibility of a saboteur gaining access and manipulating the meter readings is avoided.

It is becoming apparent that purchasing of a smart meter is not the only thing to do. When introducing smart metering, the whole system must always be checked with respect to the security aspects. The meter and the supply industries in particular must work together to reach a high level of security that is geared towards national demands.