Federal Ministry
for Economic Affairs
and Energy

Federal Office
for Information Security

Smart Metering – Subject to Stringent Data Protection and Security Rules

Smart metering always means a higher volume of data traffic. The data in question can reveal a great deal about patterns of consumption, which is why smart metering raises issues of data protection. Just like with any other form of digital communication infrastructure, there is also a risk of hacker attacks. In other words, the highest standards of data protection and security must apply.

This is why a very large package (several hundred pages) of technical guidelines and protection profiles developed by the Federal Office for Information Security (BSI) has been included in the draft bill promoting digitisation within the energy transition. The commissioners for data protection appointed by the Federation and by the *Länder* have been involved in the drafting process from the very outset, ensuring that data protection and privacy become part and parcel of the protection profiles and the technical guidelines. Incorporating these BSI documents into the actual legal text will ensure that exceptionally high data protection and security standards apply throughout the development, manufacturing, distribution, and operation of smart-meter gateways.

The result is a standard that follows the approach of data protection, security and interoperability by design, which will enable the smart meter gateways approved by the BSI to be used as communication platforms within smart grids. In this way, they will play a key role in making sure that the energy transition can go digital without this resulting in security being compromised. Under the draft legislation, all smart metering systems would have to be certified by the BSI to guarantee that all parties involved have proved that they comply with all of the data protection and security requirements.

10 data-privacy safeguards

The commissioners for data privacy for the Federation and the Länder have set out specific requirements around smart metering[1]. The draft legislation that is now on the table fully meets all of these requirements:

- **Without explicit approval by the consumer, all data-gathering and use is restricted to the bare minimum required for the energy system to work.**
  Metering data must not be passed on or used other than for the purposes listed in the legislation as necessary for the well-functioning of the energy industry. This ensures that, beyond this, personal metering data cannot be used for any commercial purpose, unless the end user has given their explicit consent.

- **The intervals at which the meter is read have been designed to be long enough to prevent any conclusions being drawn about user habits.**
  For consumers using no more than 10,000 kilowatt-hours of electricity a year, the standard interval at which metering data is to be passed on to third parties under the draft legislation is once a year. The average German household uses some 3,500 kilowatt-hours of electricity per year. Data will only be transmitted more frequently if the end user has opted for a tariff or an additional service for which shorter intervals are necessary. In these

1 Cf. "Datenschutz kompakt" published by the Federal Commissioner for Data Protection and Freedom of Information on 7 October 2015, http://www.bfdi.bund.de/SharedDocs/Publikationen/DatenschutzKompaktBlaetter/Smart%20Metering.pdf;jsessionid=27D145B539E0B-207D0231AC25C15AA75.1_cid329?__blob=publicationFile&v=1. (in German).

cases, the data will also be passed on to grid operators, suppliers and/or other market participants who have the right to access this data. All use of the data will be limited to the purpose for which it is supplied.

Whilst the metering data for those consuming up to 10,000 kilo-watt hours is collected four times an hour in the home, the metering gateway will only make this data accessible to the household in which it has been collected, so as to provide for transparency for consumers. Private consumers can make use of the gateway's visualisation interface to gain a detailed overview over their electricity use, without the need for high-resolution data to be passed on to third parties for visualisation purposes.
Only in cases where end users have given their explicit consent to high-resolution data being passed on to a third party, and only where there is an agreement or contract providing for this, can such data be transferred to the third party. The system used to transmit the data must be secure.

- **No data will be transmitted unless it has been anonymised, pseudonymised, or aggregated.**
  It will be mandatory for encryption to be used whenever data is transmitted by the smart meter gateway to authorised market participants. Depending on the purpose for which the information is used, the data will also be pseudonymised and its integrity protected to ensure that it cannot be accessed or manipulated by 'unauthorised' third parties.

- **Data will be processed in situ, right on the consumer's premises.**
  The smart meter gateway will itself conduct the calculations necessary to determine the household's electricity usage, eliminating the need for detailed user profiles which could be used to snoop on consumers. All data leaving the gateway will therefore be encrypted, aggregated and relevant for billing. There is no need for high-resolution data on electricity usage to be passed on to third parties for pricing purposes. Whenever personal data is processed by smart metering systems, customers' privacy will be fully protected.

- **Energy data will be passed on to as few parties as possible.**
  The transfer of data will be limited to parties explicitly authorised under the legislation to receive such data for a purpose also listed in the legal text. The requirements set out in the documents furnished by the BSI will ensure that the principle of data minimisation applies, and that only aggregated usage data required for billing purposes is allowed to pass through the gateway.

- **It will be mandatory for data to be deleted within specified time periods.**
  Without prejudice to the applicable metering and calibration rules, all personal metering data must be deleted as soon as storage of this data is no longer required for the purpose for which it has been supplied.

- **Consumers will be able to monitor and verify all communications and processing steps at all time.**
  Every end user will be issued by their systems operator with a data sheet detailing what data traffic is necessary and why. Furthermore, end users will be able to access the log kept locally by their gateway about who has received what metering data and when. Safeguards ensuring that smart meters are set to the right configuration and that all data processing is documented will also apply.

- **It will be easy for consumers to enforce their right to object and to data being deleted or corrected.**
  The log will make it easy for any abuses to be detected and proved, allowing for consumer rights to be enforced much more easily.

- **Consumers will still be able to choose the tariff that suits them best.**
  The new law will not limit end consumers' right to select a tariff of their own choice. The smart-metering system is meant to create an incentive for consumers to opt for a tariff that is tailored to their particular needs, without there being any obligation to do so. Whilst bespoke tariffs may require more data to be passed on, all end user data will still be secure. Thanks to the requirements set out in the documents designed by the BSI, all smart-metering systems will in future use encryption when communicating with authorised market participants. Furthermore, the principle of data minimisation applies, meaning that only data required for billing will pass through the gateway. Certification of gateways by the BSI will be mandatory so that end users can be sure that their system meets the requirements imposed by the BSI.

- **Smart meters cannot be accessed freely by outsiders. Access is regulated by means of clearly defined profiles.** For security reasons, all communication will be one-way, i.e. from the gateway to the market participants authorised to receive the data. Communication lines can be established by the gateway on-demand or at pre-defined points in time. The gateway operator, i.e. the consumer, can react instantly to particular incidents and events by using the 'wake-up service', which will instantly establish a communication line. End users have full sovereignty over their data. They can freely access the local log kept by the gateway, check the evaluation profiles used for pricing purposes and the communication profiles for authorised market participants, match these against the provisions agreed in the contract, and take action if there are any discrepancies.