White Paper
AMM Data Security

Advanced Metering Management Data Security

Advanced Metering Management Data Security

Advanced Metering Management Data Security

Introdouction

An Advanced Metering Management (AMM) system is a powerful energy management service based on two-way data communication. It enables a wide range of applications such as remote meter reading, customer relationship management and demand-side management. In addition, it provides functions to assist utilities with load control, reporting power outages and monitoring power quality. Vast amounts of information flow through an AMM system everyday and security of this data is a top priority. It is vital to protect the system against unauthorised users or 'hackers' and to ensure the integrity and confidentiality of the data.

The data flowing through an AMM system is exposed to various risks such as intrusions in the field network, the data centre or even at system level. There are currently no uniform security standards for AMM systems, however, solution providers should ensure built in security technology to protect the system.

Security architecture for AMM systems should ensure system and network availability, while at the same time meeting critical security objectives such as confidentiality, integrity and authentication of data. By using a system that focuses on these objectives a utility can effectively manage security risks.

Advanced Metering Management Data Security

Overview of AMM security issues

While regulatory entities, industry associations, utilities and suppliers are working on common security standards for advanced metering infrastructure, prudent service providers are assessing and mitigating potential risks. AMM networks typically interface with meters and in-home networks. Security assessments are necessary at the metering endpoint or concentrator level, local-area network level and head-end or data processing level.

Best practices in securing communication networks commonly include standards for ensuring the authentication of network users, integrity of communications and confidentiality of data. These objectives provide a framework for effectively managing security risk.

Security architecture that utilizes advanced encryption techniques at the in-home device, multi-energy metering endpoint, network and head-end level to protect against intrusions should be provided. Network design is also an important security consideration - from how the messages are transmitted, to control of potential network access points – and can provide additional protection against abuse.

Each electric utility faces unique security standards. When deploying an AMM system, a utility should consider the various security standards implemented into the system, as well as the flexibility of the system to suit its unique needs. It should also be considered that security systems, albeit vital, form an extra layer of software which can slow down a utility's system, and require additional communication expenses. This paper focuses on the technical strategies to combat security risks; however, a utility should consider physical and procedural solutions as well.

Advanced Metering Management Data Security

Main areas of concern

Availability

Availability of data is a paramount concern in an AMM system. Utilities must have complete confidence that they will have constant access to their meter and billing data at all times. Therefore, it is vital that an AMM system has the ability to identify and overcome issues such as denial of service (DoS) attacks or equipment tampering that could be used to compromise an AMM network and inhibit the monitoring and control functions the network provides. This concern should be addressed during system integration.

Confidentiality

Confidentiality is a universal concern. Information privacy is of high importance not only to the utility but also to the end customer. A utility must ensure information such as scheduled customer billing data, meter alarm information and home-area network events, is protected against ‘unauthorised accesses’, which includes authenticated users lacking the required permission as well as hackers.

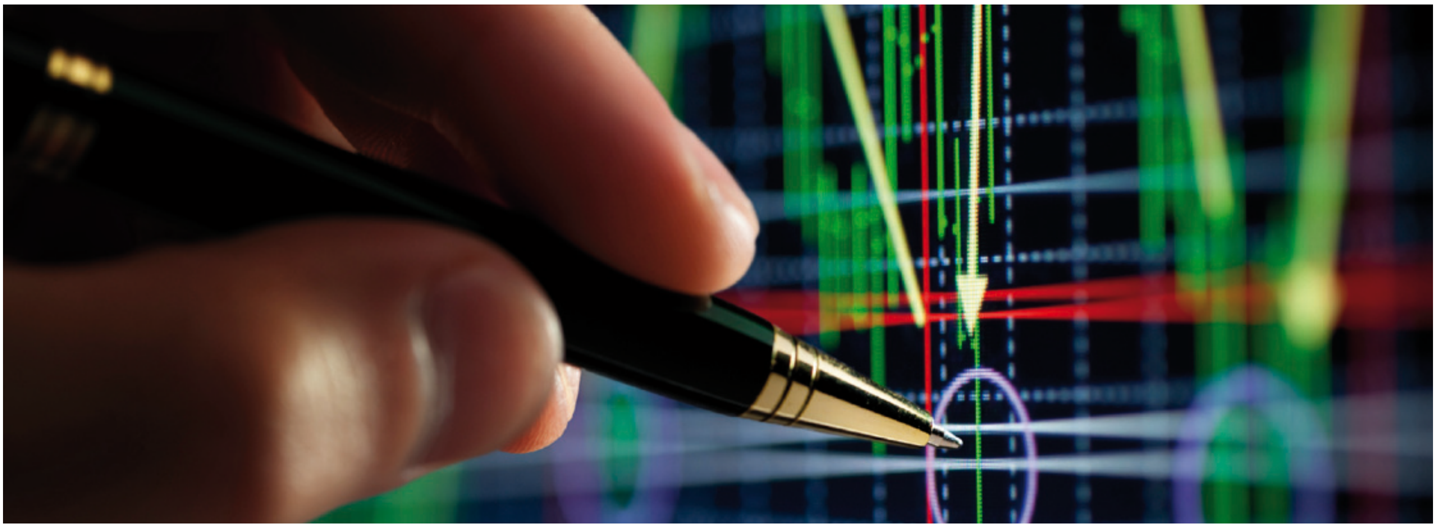
For the customer, the Personal Data Protection Act can ensure their metering data remains confidential. In addition, customer consumption information is sent to the utility in a series of numbers which do not correlate to the customers’ personal details such as name or address. Nevertheless, a utility must ensure that this data is protected.

Integrity

Ensuring data integrity can be achieved by implementing strategies to detect any changes which have been made to the data. Changes can be made during data transmission and retrieval. Such changes can be malicious, due to hacking, or accidental due to equipment failure. An advanced metering network must ensure that actions performed against a device can be traced back. Common forms of maintaining data integrity include data encryption, digital signatures, logging, tracking and auditing actions.

Authentication

A utility must be aware of who is accessing its data. This is achieved through authentication which is enabled by an identity management system. The system assigns access permission to identities. This prevents hackers from attempting to access an AMM network through the physical network in the field or at the head-end application server and data centre. Modern authentication strategies are difficult to breach and must be implemented at each level of the system



Advanced Metering Management Data Security

Best Practices

An AMM system must have the capability of delivering data through all components of the system with a high degree of availability while also ensuring that the receipt of the data has been delivered in a highly confidential manner. It is also important that a utility has the confidence to know that the data has not been tampered with or altered and that the various AMM components have the ability to authenticate that messages originate from a reliable and trusted source. In addition, appropriate processes and procedures must be followed to ensure that proper access controls are implemented such that only authorized entities or personnel have access to sensitive data or the ability to perform various high-risk functions.

Ensuring confidentiality

AMM systems should protect confidential information through the use of security standards for interoperable solutions, as well as various encryption techniques at the multi-energy endpoint and network levels. Correspondingly, by using the AMM system a utility can manage different types of controlling functions such as contract management tasks to be carried out in the multi-energy device level.

Advanced security standard

State of the art security practices are imperative for data transfer between multi energy metering points and the next system instance, such as a data concentrator or an advanced meter reading (AMR) system. The valued DLMS/COSEM protocol provides several security features for accessing and transporting data. Data transport security provides privacy and authentication of data as it travels from a multi energy meter point to the next system instance.

This international standard for electricity metering allows energy solution providers to offer fully interoperable solutions. In addition, the security features of DLMS/COSEM are scalable according to the unique needs of the system user.

Encrytion techniques

Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing 'key'. To ensure confidentiality in meter data transfer the following encryption techniques should be used:

- Advanced Encryption Standard (AES) encryption using unique keys at the endpoint to protect home or premises information from interception that could lead to potential privacy and operational exploits.
- AES encryption uses segment keys to conceal broadcast command and control messages from interception that could be used to develop operational exploits.
- Eliptic Curve Cryptography (ECC) in ZigBee enabled endpoints
- Secure Sockets Layer (SSL) protocol to protect data transported over IP based networks, as well as securing sockets for http and web services.

Advanced Metering Management Data Security

Privacy of In home display information

In home displays (IHD) are uniquely bound to its multi-energy electricity meters. Data from the IHD is stored in the electricity meter and not the IHD. Therefore, the data is protected by the meters security technologies such as encryption techniques and the DLMS/COSEM protocol. Data on the IHD is reset as soon as the unit looses power.

Authentication and integrity of data

The authentication and integrity of system software and hardware, billing and operational data, and command control message functions are paramount to network security. Authentication takes place when a user logs on to the systems interface. AMM systems should be protected using strict, hierarchical access control mechanisms. The internal network should be protected from external access using firewalls and multiple levels of network level access control mechanisms.

User authentication

An AMM system should allocate access permits to users. As different users, such as supplier staff, utility staff, the grid operator, or the multi energy utility, have different interests, they also have different rights to the data on the system and metering point. Access permits can ensure that users have rights only to their required information.

In addition, all users of external connections should be authenticated inside a secure data connection protocol. This is especially necessary for protecting against signals from an unauthorised meter or a PC that emulates a meter.

Meter authentication

- The authenticity of a meter which is sending data should be ensured. This is done by checking the meter's serial number before the actual data connection is established between the meter and the system.
- The DLMS/COSEM protocol ensures data access security to the electricity meter data. Data access security is based on assigning different access rights. The next system component must be properly authenticated to access data.
- Multi-energy meters should ensure that access to the meter's software is adequately protected by access keys. Consequently, the system can automatically confirm that the data is coming from an authentic meter device.

Data integrity

Data integrity should be ensured while data is stored on the meter, and also as data is transmitted to the next system component.

An AMM system should protect access to stored data against unauthorised access, modification, removal or destruction. This is typically done using check sums which ensure the data is valid.

The system should recognise accidental and unintentionally transmitted data changes as well as required data retransmission using encryption techniques and protocols such as M-Bus and DLMS.

Further authentication and integrity features should include:

- Role Based Access Controls (RBAC) within the head-end system enabling the utility to restrict operational and data access on a granular basis to both individuals and systems with an explicit need
- Native and Lightweight Directory Access Protocol (LDAP) with user authentication mechanisms at the head-end. The native authentication mechanism is based on User ID and hashed passwords. LDAP support enables the utility to implement extremely elaborate multifactor and even multi-person access controls using standard third-party systems
- Hash Message Authentication Codes (HMACs) to guarantee the authenticity of a message
- Mobile administration software makes use of digital certificates issued by the head-end to authenticate field tools

Advanced Metering Management Data Security

Ensuring availability

AMM systems should use, and be highly compatible with, standard IT infrastructure so that utilities can employ traditional data centre technologies to solve availability challenges. The unique challenge is that many network systems being deployed today use PLC communications, which are inherently susceptible to interference. AMM systems can reduce jamming and interference issues through the design and function of the network.

Other security measures

The network must be controlled and monitored appropriately to protect against threats and to maintain the security of systems and applications that use the network, including transferred information.

The party responsible for the network must implement controls to ensure the security of information in the network and to protect associated services against unauthorised access.

Other security measures to be considered include:

- Strategies to quickly identify security breaches, to localise the areas affected, and to react in a timely manner.
- Train all utility and third-party employees who have access to AMM data or controls.
- Perform ongoing third-party penetration testing to identify potential system vulnerabilities

Advanced Metering Management Data Security

A leading AMM solution provider

Landis+Gyr is the leading global provider of secure AMM systems. With a reputation for providing high quality solutions and with energy management experience across the globe, the company ensures that its AMM systems meet the highest security standards and practices.

Landis+Gyr AMM solutions are scalable to meet the unique security needs of utilities. The company follows best security practices throughout the entire metering value chain and incorporates standards and software to ensure all security concerns are addressed. Confidentiality, availability, authentication and integrity of data are of top priority for Landis+Gyr. It employs standards such as the DLMS/COSEM protocol and encryption techniques such as AES, EEC and SSL. The highest authentication and integrity practices are also provided using RBAC, LDAP, HMACs along with other applications. It ensures that proper access controls are implemented in its systems and that utilities feel safe in the knowledge that the confidential data of the utility and its customers is handled safely.

Paving the way for the future

In its pursuit of improving energy efficiency, Landis+Gyr is paving the way for the next generation of smart grid and supports an interoperable, open standard environment. Smart grid technology enables enhanced reliability in energy distribution systems, while providing tools to improve response times to events that disrupt power delivery. These benefits do not come without risk. As smart grid and advanced metering technology continue to evolve, system security must evolve with it. Advanced metering networks are already playing a larger role in managing demand response, distribution automation and personal energy management, making security a top priority. Landis+Gyr is confronting potential risks through the development of advanced security features within the architecture and design of Gridstream solutions, while taking an active role in industry efforts to establish security standards. In the future, Landis+Gyr will continue to make security an essential part of its product and network development strategy.

About Landis+Gyr

A trusted name in energy management solutions, Landis+Gyr operates in 30 countries across five continents. Landis+Gyr ranks as the worldwide leader in electricity metering with a preeminent position in Advanced Metering Management. Its meters and solutions empower utilities and end-customers to improve their energy efficiency, reduce their energy costs and contribute to a sustainable use of resources. With a proven track record for more than a century, it's Landis+Gyr's primary goal to help utilities manage energy better.

For more information on how you can manage energy better please contact:
Landis+Gyr AG
Feldstrasse 1
6301 Zug
Switzerland
Tel: +41 (0)41 935 6000
Fax: +41 (0)41 935 6501
Email: info@landisgyr.com
Website: www.landisgyr.com/europe