PRIME sub-networks,

a secure multiservice telecommunication infrastructure

Many utilities all over Europe rely on PRIME for their advanced metering infrastructure. Massive smart meter rollouts are taking place in Poland, Portugal and Spain. Nearly seven million PRIME smart meters have already been deployed or, to put it another way – close to 100,000 PRIME sub-networks are currently active in Europe.

All these utilities in the end realize that, they are deploying more than a smart metering infrastructure – they are deploying a MULTISERVICE telecommunication network infrastructure. PRIME telecommunication sub-networks are providing a coverage area, linked to the low voltage grid, which supports additional services and applications apart from the main feature of managing smart meters. Low voltage grid monitoring and control and distributed generation integration are new applications, which are starting to use existing PRIME sub-networks.

Fig 1: PRIME Worldwide Pilot and Deployments Map (Meter Numbers as at August 2015)

PRIME as a network infrastructure will transport data of different types. On one hand, customer consumption information is traversing PRIME networks – so data privacy becomes a fundamental issue and also a legal mandate. On the other hand, operational data, which is critical for low voltage grid monitoring and control, needs to be managed so that low voltage assets are kept secure. Application protocols such as DLMS/COSEM have a critical role to play in order to provide cybersecurity mechanisms to ensure data integrity and confidentiality. PRIME v1.4 also provides additional cybersecurity mechanisms so that utilities deploying PRIME telecommunication sub-networks can rely on a secure infrastructure that:

- Prevents intrusion
- Avoids data manipulation/tampering and guarantees data authentication and confidentiality.

PRIME v1.4 supports a set of flexible security features at MAC (medium access control) layer that allows utilities to control which security mechanisms to activate for each PRIME telecommunication sub-network. The base node plays a central role in every PRIME sub-network: every service node willing to access the telecommunication services offered by a PRIME sub-network needs to register with the base node. This registration process is the basis for service node authentication. It also allows for secure negotiation on the appropriate security profile that will be used for all data exchanges through the PRIME sub-network.

PRIME v1.4 supports three security profiles. All security profiles, thanks to its registration process, facilitate mechanisms for service node authentication. Security profiles 1 and 2 are based on AES-128 (following NIST recommendations) and provide secure functionalities for key derivation, key wrapping/unwrapping and authenticated encryption of all data packets. Thus, both profiles guarantee data packets confidentiality, authenticity and integrity. Moreover, replay attacks are prevented through the use of a message counter.

PRIME is a connection-oriented technology so that any data exchange requires a previous connection establishment. Each connection will be closely related to the type of data to be transported. PRIME is designed to transport IPv4 or IPv6 data packets, and it is also optimized for smart metering data transport (e.g. DLMS/COSEM over IEC 61334-4-32). The service node, when establishing a connection, can opt for the security mechanisms it wishes to apply for all the data exchanges linked to that connection.

Key management plays a critical role in any cybersecurity architecture. Each PRIME node will have a unique key – the device unique key (DUK). PRIME follows NIST recommendation NIST SP 800-108 for deriving two additional keys, the registration key (REGK) and the key wrapping key (KWK). The REGK is used during the mutual authentication process (base node and service node) that occurs when a new service node registers with the base node. The KWK is used by the base node to wrap the individual working key (WK) that the base node creates for each specific service node, for authenticated encryption of all data traffic. Additionally the base node uses the KWK to deliver the sub-network working key (SWK), which is used for common messages that the base node needs to share with all registered service nodes.

As a conclusion, PRIME v1.4 MAC layer security has been flexibly designed so that utilities, as telecommunication infrastructure owners, can choose among different options to deploy a secure architecture for their PRIME sub-networks. MI

Fig 2: Main Components of a PRIME Sub-Network

ABOUT THE AUTHOR

Txetxu Arzuaga is ZIV LV products unit manager, at CG Automation (Distribution Automation). Txetxu has been deeply involved in the conceptualization, design and deployment of powerline networking solutions for Advanced Metering Infrastructure.