HSM for Securing the Smart Grid

SOLUTION BRIEF

Benefits of PKI

- Protect customers private data
- Protect power grid from manipulation
- Prevent large scale attacks on the grid
- Eliminate deployment of fraudulent meters

Building trust in the smart grid with hardware security modules for meter attestation, PKI and EKM management, and compliance with security mandates

Overview

The smart grid is the first major effort to modernize an energy infrastructure that has remained largely unchanged over the past several decades. The smart grid creates a network of links between customers and utility companies that provides increased insight into energy consumption, cost, and workload across the energy grid.

At a time when energy utilities play an increasingly important role in our everyday lives, smart grid technologies introduce new security challenges that must be addressed. Implementing a smart grid without proper security could result in grid instability, loss of private information, utility fraud, and unauthorized access to energy consumption data. Building a trusted smart grid will require robust security solutions that can be easily deployed at the communication and application layers of the smart grid infrastructure.

In the first phase of smart grid deployments, traditional meters will be replaced with smart meters that can be read remotely, called smart meters. The Advance Metering Infrastructure (AMI) is the second phase of the smart grid and uses smart meters to enable a two-way channel of communication between meters and the utility company. Securing this two-way line of communication is imperative, and will require a solution for authentication and device attestation to ensure the integrity of the grid.

HSMs Role in the Smart Grid

Smart grid security solutions must be able to deploy on a large scale, with minimal effect on application performance. Securing the smart grid at the communication layer will require a system to identify connected meters, to verify that these meters are configured correctly, and to validate thm for network access. The recommended solution for this authentication process is a Public Key Infrastructure (PKI). PKIs are ideal for large scale security deployments that require a high level of security with minimal impact on performance. In a PKI environment, it is essential that private keys and certificates are guarded with a reliable key management solution that protects against ever-evolving data threats.

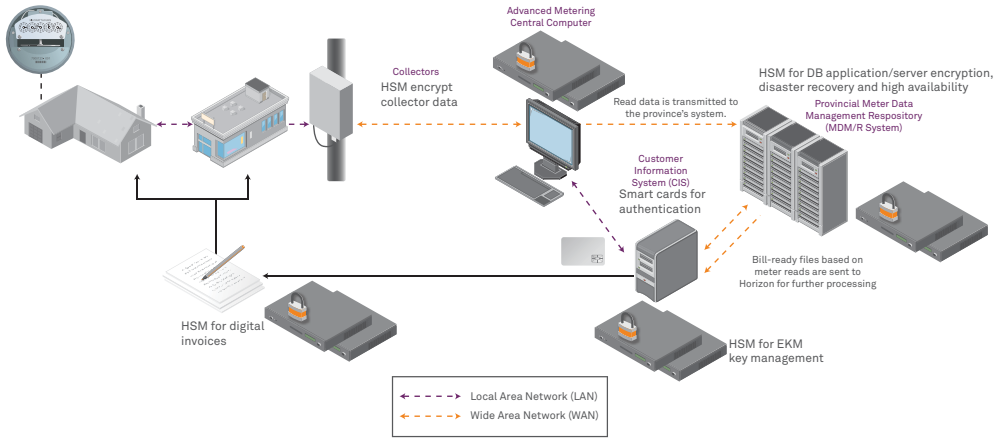
SafeNet HSMs offer a cost-effective PKI solution for easy deployment in smart grid infrastructures. With the SafeNet PKI Bundle, product and maintenance costs are dramatically reduced by combining HSM functionality that usually requires two or more HSMs into a single HSM “bundle” of modular functions. For CAs with certificates and root keys, for example, rather than requiring separate HSMs for key generation and key export for offline and online root CAs, the requirements can be fulfilled by only one SafeNet HSM that stores keys in hardware to achieve FIPS 140-2 L3 security. In addition, with processing speeds of up to 6,000 1024-bit RSA and 400 384-bit ECC transactions per second, SafeNet HSMs can keep up with the performance requirements of even the most complex smart meter deployments.

Why SafeNet HSMs?

- FIPS 140-2 Level 3-validated hardware
- Common Criteria EAL 4+ certified
- Ideal for disaster recovery readiness
- Scalable, easy installation and management
- High-availability mode

HSMs provide the following security functions:

- **Device Attestation.** Using device attestation certificates, the HSM confirms the device manufacturer, model, and serial number, and that the device has not been tampered. These certificates, coupled with the appropriate authentication protocol, can be used by the energy service provider to ensure that the device is exactly what it claims to be.
- **PKI and EKM Key Management.** HSMs provide significant cost savings, as HSM functionality (key generation/offline root/online root/key export) is made available with one device.
- **Trust Anchor.** A local policy database is a set of rules that define how the device can use its certificate, and what types of certificates it should accept when acting as a relying party. The LPD would be a signed object, signed and stored within the HSM.
- **Encryption and Decryption of Information.** AES 256 & ECC 256/384-bit. ECIES key management and ECDSA signing performance (256-bit curves).
- **Transaction processing of usage and billing to customers.** Provide a trusted path for energy usage for accurate and secure electronic billing.
- **Compliance.** Compliant with PII, NIST, FIPS, and NERC audits
- **Remote Management of Meters.** Securely update the metering settings, configuration, security credentials, and firmware of all devices in the AMI System.



About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet. For more information, visit www.safenet-inc.com.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected