Case study

Silver Spring Networks—Securing the Smart Grid with Utimaco's Hardware Security Module

Motivation: protect high value assets in the smart grid

Silver Spring Networks is a leading provider of IoT networking solutions for connecting critical infrastructure. With a track record of more than a decade, Silver Spring has worked with some of the largest utilities around the world, leveraging its proven multi-application platform to enhance operational efficiency and quality of service for energy, water and smart city systems.

Increasingly, utilities are faced with the challenge to modernize their distribution systems to deliver ubiquitous intelligence and control across multiple critical devices and software applications. Enabling the smart grid requires an advanced IP-based network designed around the same communication model as the Internet. Every energy meter, every communication node in the smart grid distribution chain is equipped with an IP address to be able to not only receive commands (on/off, less/more), but also to send responses (OK/not OK) to the system and/or other participants in the network.

The challenge: securing the connected grid

As with the financial sector, energy companies are faced with an imminent threat of attack due to the high-value assets they hold, and the potential impact of a security breach on critical physical infrastructure. As grids become increasingly connected, utility systems will be exposed to the same attack surface as the Internet. Securing these critical connections against the threat of malicious attack or intrusion requires proven, multi-layer protection across multiple device and application layers.

A typical attack scenario: mass-disconnection of users

One example of a typical command and attack scenario in a smart grid environment is by issuing a "remote disconnect" of smart meters. With traditional one-way distribution networks, a disconnect of an electric meter would always require a truck roll – i.e. a utility truck physically driving to the meter and disconnecting it from the power supply. This could happen for various reasons, such as unpaid bills, moving to a different location or maintenance. Modern, intelligent distribution systems enable smart meters to remotely disconnect, which enables the utility to send a disconnect command to a specific smart meter for instantaneous execution. But what would happen if a third party hacked into the system, hijacked the communication and repeated the same command ("disconnect from grid") to 50,000 meters at the same time? The answer is that the whole power grid would be out of sync, substations would go offline, potentially even causing a rolling black-out that could shut down an entire portion of the grid in a city, state or country.

The solution: digital permits from a FIPS-certified HSM from Utimaco

Silver Spring provides secure communications for nearly 23 million smart devices in its networks. To protect the data between those smart devices, Silver Spring opted for Utimaco's hardware root of trust. Utimaco's FIPS-certified hardware security module (HSM) generates and stores secure digital permits that are required for executing communication commands between the Silver Spring smart devices. Each permit contains a cryptographic signature, generated via true random number generation, so that devices such as meters can verify the authenticity and integrity of the permit before executing the command.

The technical solution: Key for preventing abuse by third parties

An HSM enables a hardware-based solution to check the authenticity of every command received by a smart meter, preventing abuse by third parties. This system leverages asymmetrical cryptography, in which a public encryption key held by every meter deciphers the command sent by the central authority. Only the central authority has the private key to encrypt the messages, and only messages using the private key are recognized by the smart meters as genuine. This method prevents commands from being executed by anybody other than the central authority. The authenticity of every command is secured, and abuse is not possible.

Unprecedented security even in the most hostile environments

Compared to software solutions, hardware security modules offer unprecedented security, even in the most hostile environments. The module will detect when the attack is happening and delete any keys the attackers left behind. True random number generation, as provided by HSMs, enables cryptographic keys that cannot be cloned. In comparison, software-based cryptographic keys can be captured in the moment of unlocking – offering attackers the ability to take over the software, exploit vulnerabilities and run attacks remotely.

The HSM will protect the keys from being hacked through any attack, including drilling, heat, power blackouts and chemical attacks. If the HSM senses that the device is being tampered with, the HSM will automatically delete the keys immediately.

About Silver Spring Networks

Silver Spring Networks is a leading networking platform and solutions provider for smart energy networks. Silver Spring's pioneering IPv6 networking platform, with 22.9 million Silver Spring enabled devices delivered, is connecting utilities to homes and business throughout the world with the goal of achieving greater energy efficiency for the planet. Silver Spring's innovative solutions enable utilities to gain operational efficiencies, improve grid reliability, and empower consumers to monitor and manage energy consumption. Silver Spring Networks' customers include major utilities around the globe such as Baltimore Gas & Electric, CitiPower & Powercor, Commonwealth Edison, Consolidated Edison, CPS Energy, Florida Power & Light, Jemena Electricity Networks Limited, Pacific Gas & Electric, Pepco Holdings, Progress Energy, and Singapore Power, among others. To learn more, please visit www.silverspringnet.com.

About Utimaco

Utimaco is a leading manufacturer of hardware based security solutions that provide the root of trust to keep cryptographic keys safe, secure critical digital infrastructures and protect high value data assets. Only Utimaco delivers a general-purpose hardware security module (HSM) as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications. With German precision engineering, tamperproof Utimaco HSM offers scalable performance with the highest level of physical security and self-defense for hostile environments.