© Thales Group

Protecting Smart Metering infrastructures with Thales Trusted Key Manager

THALES

Building a future we can all trust

Thales Trusted Key Manager – the smart grid security pillar:

- **Diversified Meter IDs**
  The solution expertly manages key provisioning in energy assets, allowing meter manufacturers and utilities to focus on their core competencies. It securely provisions encrypted keys in smart meters at the time of manufacturing, which eliminates the need to send keys over the air and reduces the ecosystem's cyber attack surface.
- **Digital Authentication**
  Before a device or application is allowed to send or access data, the solution remotely authenticates and activates key credentials for authorised meters and applications that can prove their legitimacy. The process leverages standardised cryptographic algorithms and a highly reliable digital authentication handshake, between data sender and data receiver.
- **Data Encryption**
  The Public Key Infrastructure (PKI)-based solution automates encryption and decryption mechanisms to ensure data confidentiality and integrity between smart meters, gateways and back-ends. Implemented at the core of edge devices, these mechanisms prevent data interception and tampering along the way, which would alter system validity or even endanger the grid.
- **Security Lifecycle Management**
  The smart energy ecosystem is dynamic with new players coming and going, with new cyber threats or regulations emerging. Thales provides continuous protection through remote device credential management enabling secure software updates and revocation/renewal of cryptographic keys when needed.

The smart energy ecosystem is an interconnected framework that leverages IoT and automation to optimize energy usage, enhance grid stability and facilitate renewable integration. This advanced system is revolutionizing the way we produce, distribute, and consume energy, contributing to sustainability and operational efficiency.

New players and private citizens are joining the ecosystem, deploying assets that tie into evolving grid infrastructures.

As the smart energy ecosystem expands, so does the opportunity for cyber-attacks and there has never been a more urgent need to secure Advanced Metering Infrastructure (AMI).

The bad news?

Unprotected smart meters, implemented for long periods exceeding 10 years, can easily be hacked to alter consumption data, to gain access to sensitive data, or even to cause physical damage to the global grid.

The consequences of such cyber attacks to the grid can be devastating: blackouts across entire countries, access to nuclear plants, and personal data breaches.

There’s more.

For device makers, DSOs (Distribution System Operators), and Utilities, the loss of customers, reputation, and revenue can be difficult to recover.

Uninterrupted security is key for smart energy systems

Governments, led by Germany and the BSI, in Europe, are launching initiatives that mandate specific protection protocols for smart grid deployments.

In addition, other regulators as the National Institute of Standards and Technology (NIST) recommend a policy whereby encryption keys and certificates stored in connected devices should be renewed every 5 years or sooner.

As smart meters have a lifecycle of 10 to 15 years, an advanced security mechanism to replace aging keys and to enable remote credential management is paramount.

Strong encryption and authentication tools must be considered and implemented before meters are deployed.

Without built-in security architecture that is reliable for the entire device lifetime, ecosystem partners are exposed to unnecessary and costly risk.

That's where the Thales Trusted Key Manager solution fits in.

Ensuring end-to-end security for the smart grid

Leveraging decades of digital security expertise and its Trusted Key Manager solution, Thales offers an advanced security solution, dedicated to grid management and to Utilities.

The Thales metering security solution protects massive smart metering deployments and ensures integrity and reliability for the entire lifecycle of energy devices and the data they exchange.

The solution is comprised of cryptographic hardware products (Hardware Security Modules (HSM)), which protect sensitive data in the smart grid.

It also leverages leading-edge authentication and encryption technology with digital code signing certificates.

The result?

Metering data is received from a legitimate source while safeguarding against data tampering and fraud at all points.

The solution facilitates dynamic credential updates and authorizations, without costly service in the field.

THALES

Building a future we can all trust

thalesgroup.com