End-to-End Cybersecurity Solution **for Advanced Metering Infrastructures**

In the burgeoning age of the Internet of Things, the energy infrastructure has become increasingly complex. 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.

There has never been a more urgent need to secure Advanced Metering Infrastructures.

Smart meters are becoming the industry standard and data is a mission critical asset. Unprotected meters, implemented for long periods exceeding 10 years, can easily be hacked to alter consumption information, to gain access to sensitive data, or even to damage critical governmental infrastructures.

According to Forbes, 4.1 billion records were exposed by data breaches in the first half of 2019 alone. The consequences of cyber-attacks can be devastating: black outs across entire countries, access to nuclear plants and personal data breaches. For device makers and utilities, loss of customers, reputation and revenue can be difficult to recover.

Uninterrupted security is paramount to the success of smart energy systems

Governments led by Germany, and followed by France, the United Kingdom and the United States are responding by launching initiatives that mandate specific protection protocols for smart grid deployments. Non-compliance with emerging regulations could prevent access to the market place or lead to costly fines.

For example, the USA´s National Institute of Standards and Technology (NIST) recommends that device keys and certificates stored in connected devices be renewed at least every five years. In most of the cases, these are renewed every two years.

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

The first step metering device manufacturers should take is identifying the risk of threats for their specific environment, and engage in a security-by-design approach when manufacturing devices.

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

Designing a built-in security architecture that is updatable for the device lifetime prevents unnecessary and costly risk to all ecosystem stakeholders.

Mitigating Risk in Advanced Metering Infrastructures

As smart grids expand, vulnerability and attack points multiply at every touchpoint:

- **Metering Devices:** unprotected points of connectivity can become digital doorways to the entire ecosystem, allowing metering device cloning, data manipulation, or alteration of a device's global performance.
- **Communication Layer:** As data transitions through a data concentrator (DC) or directly to an Head End System (HES), protection is crucial against distributed denial of service (DDoS) attacks, spoofing, or data breaches that could disrupt service and compromise confidentiality and integrity.
- **Application Layer:** HES or Metering Data Management Systems (MDMS) - receiving and analysing data generated by smart meters - must leverage strong authentication, digital signature and encryption mechanisms. This ensures the applications are legitimate and the data can be trusted.

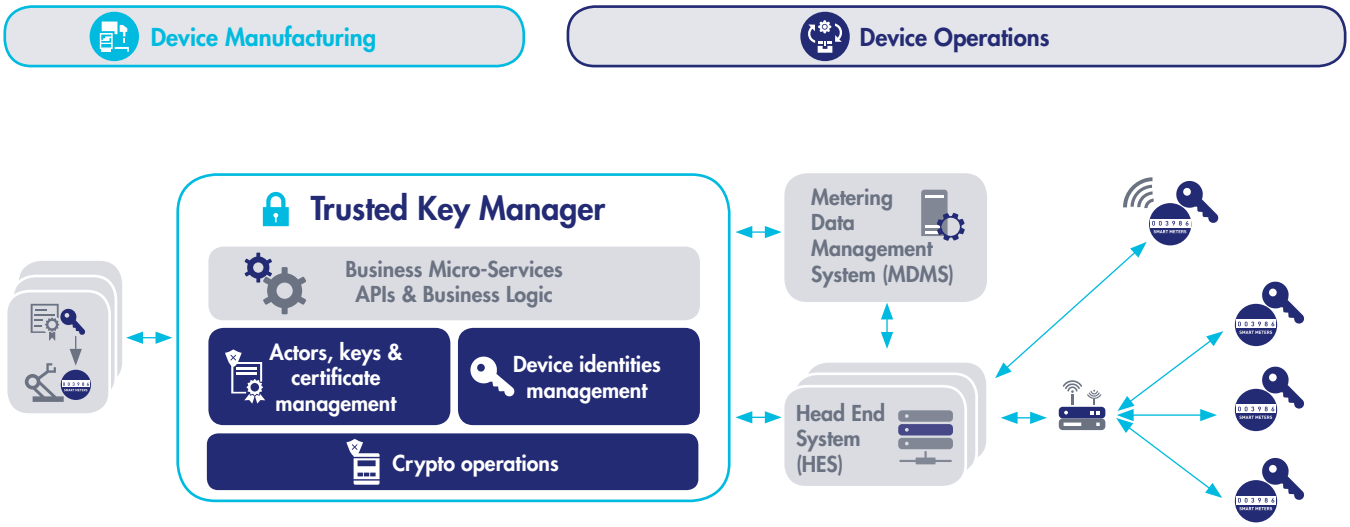
Advanced Metering Infrastructures require seamless built-in security at all these layers to ensure complete system integrity.

Thales Trusted Key Manager: Ensuring End-to-End Security for the Smart Grid

Leveraging decades of digital security expertise, Thales offers an advanced cybersecurity solution: the **Trusted Key Manager for Smart Energy.** The dedicated solution protects massive smart metering deployments and ensures integrity and reliability for the entire lifecycle of connected devices and their data.

The Device Language Message Specification (DLMS) represents a powerful asset for Advanced Metering Infrastructures, enabling interoperability, efficiency and security for metering data exchange. To pave the way for long-lasting security and upgradability, Thales Trusted Key Manager supports DLMS suites 0 and 1.

Thales Trusted Key Manager for Smart Energy:
Securing Device Deployment and Operations



The Thales solution is comprised of the world-leading Safenet Hardware Security Module (HSM), a dedicated Key Management System (KMS) and best-in-class Public Key Infrastructure (PKI). The solution facilitates dynamic credential and security updates, without costly service in the field. The Thales Trusted Key Manager sits at the heart of AMI security. It gives DSOs full flexibility to work with a variety of meter vendors and Head End Systems, ensuring independence for private DSOs (multi-sourcing) and state-owned utilities (sovereignty).

3 pillars of security to ensure smart metering protection:

Smart Meter Key Provisioning

The Thales solution expertly manages key and credentials provisioning, allowing smart meter makers and utilities to focus on their core competencies. It securely provisions highly diversified, encrypted keys in smart meters at the time of manufacturing. This eliminates the need to send keys over the air, which greatly reduces the cyber-attack surface of the ecosystem. Once smart meters are in the field, their keys can be automatically updated at first power-on, to ensure a full change of ownership.

Mutual Authentication and Encryption

Before a device or application is allowed to send or access data, the Thales solution remotely authenticates and activates key credentials for authorized meters and applications that can prove their legitimacy. The process leverages standardized cryptographic algorithms and a highly reliable digital authentication handshake, between data sender and data receiver. The mutual authentication mechanism ensures that data transferred over the network has not been altered, is coming from a legitimate source, and is undecipherable to eavesdroppers.

Security Lifecycle Management

The smart energy ecosystem is dynamic: new players come and go, new cyber threats emerge and keys depreciate. Thales solves this challenge and provides continuous protection through remote credentials management and secure embedded software updates over the lifetime of devices.

Designed for maximum convenience, the future-proof solution is ready-to-use and requires minimal micro-service configuration to integrate with any back-end.

The Thales Trusted Key Manager for Smart Energy solution acts as a safe certificate authority to guard keys and credentials, keeping utilities protected against ever-evolving cyber threats. Smart meter manufacturers and grid managers can keep security at its highest level, while decreasing operational time and cost.

To discover our **Seamless Metering Connectivity** offer, including IoT modules and eSIM, please visit **thalesgroup.com/iot**