End-to-End Security Solution for Advanced Metering Infrastructure

Complete credential lifecycle management for smart utilities

> 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 Infrastructure.**

Smart meters are becoming the industry standard and data is a mission critic asset. Unprotected 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 energy assets. The consequences of such attacks, such as the recent Stuxnet attack, can be devastating: black outs across entire countries, access to nuclear plants and personal data breeches. 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 marketplace or lead to costly fines.

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

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.

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.

Ecosystem partners are getting serious about security planning and the first step is identifying the risk of threat from end-to-end.

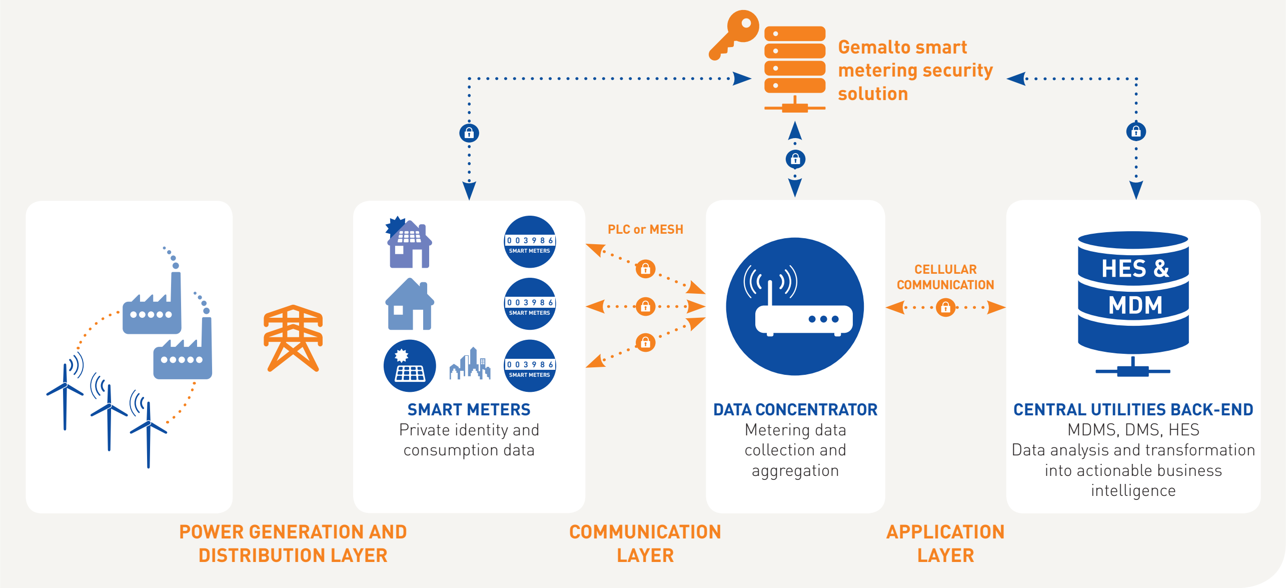
Mitigating Risk in Advanced Metering Infrastructure

As smart grids expand, vulnerability and attack points multiply on every layer of the system:

- **Power generation and distribution layer:** unprotected points of connectivity and data exchange can become digital doorways to the ecosystem, allowing attacks that alter energy distribution or even cut it off altogether.
- **Communication layer:** gateways and smart meters need protection against distributed denial of service (DDoS) attacks, spoofing and data breaches that disrupt service and compromise confidentiality and integrity.

- **Application layer:** platforms such as Meter Data Management Systems (MDMS) and Distribution Management Systems (DMS) need strong authentication and encryption to ensure that applications are legitimate and that data can be trusted.

Advanced Metering Infrastructures require seamless security at all these layers to ensure complete system integrity. **The image below shows where strong authentication is needed throughout the system:**


Gemalto smart metering security solution
PLC or MESH
CELLULAR COMMUNICATION
HES & MDM
SMART METERS
Private identity and consumption data
DATA CONCENTRATOR
Metering data collection and aggregation
CENTRAL UTILITIES BACK-END
MDMS, DMS, HES
Data analysis and transformation into actionable business intelligence
POWER GENERATION AND DISTRIBUTION LAYER
COMMUNICATION LAYER
APPLICATION LAYER

Ensuring End-to-End Security of the Smart Energy Ecosystem

Leveraging decades of digital security expertise, Gemalto offers an advanced security solution, which protects massive smart metering deployments and ensures integrity and reliability for the entire lifecycle of devices.

The Gemalto **smart metering security solution** is comprised of hardened cryptographic hardware products (Hardware Security Modules and Secure Elements), which protect the smart metering ecosystem. The solution leverages leading-edge authentication and encryption technology with digital code signing certificates. This ensures metering data is received from a legitimate source while safeguarding against data tampering and fraud at all points. The solution facilitates dynamic key and credential updates and authorizations, without costly service in the field.

The solution provides 3 pillars of security to ensure smart metering protection:

> Smart Meter Key Provisioning

The Gemalto solution expertly manages key provisioning, allowing device makers 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. The keys can be stored in different security container frameworks, such as the Cinterion Secure Element, which offers a tamper-resistant environment to guard sensitive keys.

GEMALTO.COM/IOT

> Strong Authentication

Before a device or application is allowed to send or access data, the Gemalto 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, algorithms depreciate, new cyber threats emerge. Gemalto solves this challenge and provides continuous ongoing protection through remote credential management enabling secure updates and revocation of crypto keys over the lifetime of devices.
The solution can be deployed externally or on customer premises, where it easily integrates with existing architectures.

The Gemalto smart metering security solution acts as a safe certificate authority to guard keys and credentials, keeping utilities protected against ever-evolving cyber threats. Unfaltering security ensures stakeholders can trust in the evolving smart energy landscape.

gemalto
security to be free