Empowering DSOs to secure the Smart Grid

Gemalto smart energy cybersecurity solution
Our evolving energy ecosystem

3 powerful agents of change: digitalization, decarbonization and decentralization

As the world’s growing need for energy meets the power of the Internet of Things, the traditional energy marketplace is rapidly transforming. Millions of meters and energy assets are connected and digitized each year, providing enormous benefits to the entire ecosystem: real time tracking of energy production and consumption data, optimized load balancing systems, streamlined operations and billing systems to name a few.

As connectivity expands and the landscape is digitalizing, new distributed energy resources (DERs) and stakeholders are able to integrate into and expand the grid. DERs offer non-carbon resources that improve the energy sector’s overall carbon footprint, a key benefit for everyone.

The convenience and benefits of a 24/7 connected infrastructure bring new challenges as well. For instance, divergent hardware and software systems from multi-vendors need to be harmonized and integrated in order to securely communicate with one another. Connected devices should be updatable, to ensure that they’ll be able to cope with new regulations and updates required over long lifecycles. And as the number of connected meters expands, the increased volume of real time digital data creates many new vulnerabilities, with a critically growing cyber attack surface. The trustworthiness of data generated and exchanged is crucial to grid management, billing and safety of the communities.

As the smart energy ecosystem rapidly transforms into a massive and complex IoT network, connected meters, assets, backends and the data they exchange must be secured.

As the main actors for coordinating and managing the smart grid, Distribution System Operators (DSOs) are central to driving the evolution of the new ecosystem. They must consider built-in security at the very beginning of smart metering deployments to ensure data trustworthiness throughout the ecosystem and the success of this new digitalized world.
Considering that smart grids are a critical national asset, governments and national entities have been actively working on defining a set of new standards and regulations.

Mitigating risk with standards and regulation
As the energy sector goes digital and decentralizes power generation sources, new players enter the market and new cyber threats emerge. Governments, energy authorities and industry coalitions around the world are scrutinizing security best practices and working to protect the reliability of power as well as the integrity of smart grids while supporting energy actors to adopt the right attitude. Non-compliance with emerging regulations could prevent access to the marketplace or lead to costly fines.

Cybersecurity agencies in the European Union and the US are leading the way forward by driving the adoption of new standards and legislation to protect the IoT and smart grids. For instance, the European Union Agency for Network Information Security, ENISA, published one of the first IoT security directives specifying the use of strong cryptography to protect the confidentiality, authenticity and integrity of data at rest or in transit on IoT networks. Other ENISA directives stipulate IoT device software and firmware must have the ability to be securely updated Over-The-Air (OTA) and access to connected devices should only be done through hard-to-crack, device-individual passwords.

To allow smart grids to evolve while maintaining steadfast security, updatability is essential to sturdy security architecture. In agreement with ENISA, the US National Institute of Standards and Technology (NIST) recommends that systems must be in place to regularly and securely revoke and generate new access credentials every 1 to 3 years. This is only a fraction of the lifespan of smart meters.

The U.S. IoT Cybersecurity Improvement Act of 2017 further refined updatability recommendations stipulating that OTA updates to fix or remove vulnerabilities or defects should be done in a properly authenticated and secure manner, without using fixed or hardcoded credentials.

New regulations will continue to appear and there can be no compromise on data confidentiality and integrity. DSOs currently deploying Advanced Metering Infrastructures need to prepare for the future, allowing the ability to securely react and easily adapt to changes. In this context, deploying scalable security solutions at the beginning of a project - that enable secure remote updates - is an essential component of any security architecture. Each and every connected point in the ecosystem should be carefully examined because the growing base of digitalized assets creates a larger attack surface, including system layers which were not previously considered.

Understanding evolving vulnerabilities
Vulnerability and attack points are ubiquitous throughout the smart grid ecosystem. Every sensor, smart meter, data concentrator or Head End System (HES) is a potential point of vulnerability that hackers could attack. Without proper security mechanisms, data generated in devices and flowing from asset-to-asset, over powerlines and wireless networks is vulnerable to manipulation. And the incentives for meddling with data are clear.

By altering consumption data directly at a smart meter level, hackers can artificially reduce bills, resulting in large revenue loss for utilities. Devices not manufactured in a secure facility are vulnerable to credential hacking that can wreak havoc on the grid. Illegitimate devices with cloned credentials can send false data and disrupt the whole grid balance.

By monitoring power consumption, would-be thieves can “see” when buildings are empty and vulnerable to burglary. Users´ personal identity information is also an attractive target for identity thieves. And breaches to interconnected elements like data concentrators or Head End Systems (HESs) can open the door to grid wide tampering allowing black outs and threats to national security. A hacked backend could indeed send commands to multiple meters that would paralyze the grid with system overloads that would irrevocably damage delivery channels.
**Defense against MadIoT attacks**

The success of modern energy grids depends on a persistent balance between energy supply and demand. When demand outpaces supply, or vice versa, system controllers are quick to react with load shifting or turning off the power supply to portions of the grid in order to protect critical infrastructure against damage.

Researchers at Princeton University have demonstrated how the majority of the grid could be brought down by a hack that causes just a 1% sudden change in electricity demand. This is a tempting vulnerability for malicious hackers. Without steadfast digital security, a simple botnet attack could take command of smart home solutions such as connected HVAC systems and facilitate coordinated attacks that overload the system by requesting more or less power. These so called “MadIoT” botnet attacks can also impact a post-blackout restart. The attacker can stop the grid from restarting by suddenly increasing energy demand using the same IoT botnet format.

Strong device authentication technology is essential from the very beginning of smart meter design and manufacturing and in all edge devices. This tried and true digital security best practice can defend against MadIoT attacks by ensuring that the entities sending data are legitimate and that the data is trustworthy.

**3 main areas of vulnerability in smart grids**

Based on current hacking threats, three main points of vulnerability have emerged in the smart grid:

- **Smart Meters**
  - Insight into building occupancy and household habits
  - Energy consumption data alteration, resulting in bill tampering
  - Private data theft
  - Outside commands of endpoints if access is not correctly protected

- **Data Concentrators**
  - Smart meter hack transferring to all meters attached to same concentrator
  - Crippling DDOS attacks compromising energy service availability
  - Meter data alteration
  - Private data breach

- **HES / Backend Systems**
  - Data integrity tampering
  - Private data theft
  - Unexpected, malicious increase in electricity demand causing widespread outages
  - National security threat, Pressure on governments

To defend against attack all layers must be protected at each point of vulnerability. This ensures that data arriving at the backend has not been manipulated or intercepted by malicious actors on the way. Securing edge devices will also ensure that attacks cannot be initiated at the backend to command a fleet of meters that could wreak havoc on the grid infrastructure.
Smart grid security: it all starts from edge devices!

Traditional security measures, such as Data Management Systems with firewalls, are simply not enough to protect complex modern smart grids at multiple levels. To ensure complete system integrity and trust, DSOs must consider the system as a whole, realizing that a breach at one level could potentially lead to damaging consequences on the other levels as well. To prevent this, smart grid security must start with protecting meters at the edge of the ecosystem.

The success of the grid depends on the trustworthiness of the data that is generated and communicated by millions of smart meters at the edge. A smart meter must be able to securely identify itself to the rest of the ecosystem to ensure its legitimacy to send and receive data. It also must be able to protect the data it generates when it’s resting in the device, and when it’s shared with another authenticated asset in the system. Encryption mechanisms implemented at the core of an edge device are essential to prevent data interception and tampering along the way, which would alter system validity or even endanger the grid.

Safeguarding the system takes expertise and a deep understanding of the principles of securing IoT devices and data flowing throughout the smart grid.

Main principles to protect connected devices and the data they generate

As the energy market has evolved, DSOs have stepped into a more active role of facilitating and managing the smart grid ecosystem. They are now responsible for guaranteeing distribution system stability, reliability of consumer data and cost-effectiveness, and they should achieve all this through the intelligent use of technology. Although all stakeholders have a role in securing the smart grid, DSOs are at the center of it all, ensuring that each player has done its part and that the system can be trusted. Ultimately, it is the DSO’s responsibility to safeguard data integrity and privacy and to secure global system availability. To this end, DSOs must enforce the tried and true principles of digital security.

The 4 principles of IoT devices security

To ensure trust across the sensitive smart grid landscape, four key principles guide security best practices to help DSOs mitigate risk at every potential attack point. These principles have been market tested for decades in government, banking and financial services industries and they have stood the test of time for success in ensuring digital security.

**Principles of IoT Devices Security**

1. **Trust the source of the data:** Integrate strong and diversified device IDs in all smart energy meters and end points at the time of manufacturing. This enable strong authentication of legitimate devices to trust in the source sending energy data.

2. **Ensure data is exchanged among trusted entities:** Leverage strong mutual authentication technology based on encryption mechanisms using a Private Key Infrastructure (PKI). This ensures that data exchanged between meters, gateways and backend systems is done among trusted entities.

3. **Certify data privacy and integrity:** Encrypt and sign all data exchanged and make certain only authorized entities can decrypt messages.

4. **Manage security updates for the lifecycle of devices:** Leverage a PKI solution to renew device access keys and to cope with evolving threats and new regulations. Digitally sign all software updates to ensure these come from legitimate sources.
End-to-end system security is best achieved with strong authentication technology based on market proven Public Key Infrastructure (PKI) schemes that leverage Hardware Security Modules (HSMs). The PKI mechanism allows clear identification of the owner of a connected device ID, to make certain the owner is legitimate and the device can receive and send data. The system works with root certificate authorities (CAs), which are supreme authorities who “notarize” a legitimate device ownership.

The PKI technology generates well-diversified device IDs [extremely difficult to guess] for authorized ecosystem entities, along with data encryption keys. These enable a secure digital handshake between devices and platforms authorized to exchange data, and ensures that data has not been tampered with during the exchange.

At the core of a PKI infrastructure, the HSM serves as a tamper-resistant digital vault used for generating, storing and distributing diversified digital IDs, encryption keys and credentials. The HSMs maintain the integrity of private keys in the PKI, securing data exchange and enabling secure over-the-air device updates and credential lifecycle management.

Independence strengthens security and flexibility
A strong cybersecurity strategy is a DSO’s long term insurance policy to mitigate risk and protect the smart grid. DSOs need total confidence that steadfast security will protect and defend all layers of the grid for its entire lifespan. To achieve this, they need to segregate security lifecycle management from the rest of the grid management. This allows DSOs to tightly control day-to-day security updates either on their own or with a trusted third party. This provides significant benefits:

1. Secure device ID generation and provisioning eliminates vulnerabilities in manufacturing:
Creating and provisioning secure, unique device IDs for connected assets is a complex process that requires a highly specialized environment and secure mechanisms. It requires the ability to generate a cryptographic key, map the key to a device’s public identity such as a serial number, and securely store the identity scheme maps all along the logistics chain without any breach. This secure process protects DSOs from weak key generation [too easy to guess] and from potential manufacturing flaws that could compromise the provisioning of devices and lead to device cloning or ID interception. Furthermore, a secure identity scheme serves as the cornerstone of automated operational processes including device provisioning, device onboarding to external platforms and alert management throughout the device lifecycle.

2. Streamlined management of meters from multiple Smart Meter Vendors (SMV):
Managing connected device credentials and updates from one independent security platform allows DSOs to integrate multiple SMV partners into their global grid deployments while managing all meters via one unique platform. This simplifies and speeds the integration of added meters and vendors. It also allows credential management and updates seamlessly across the entire fleet of devices.

3. Isolate secret keys to support system integrity and data trustworthiness
Hardware Security Modules (HSMs) use advanced encryption-based mechanisms to create sturdy access credentials and secret keys. These are the core elements of trusted data exchange, secure device updates and remote credential management. To maintain the integrity of these private keys, it is vital to keep the HSM independent from the HES and to isolate secret keys from the external IP world. The two entities (HSM/HES) should work independently, even if they are both positioned at the HES back end.
Leveraging decades of digital security expertise, Gemalto offers an advanced smart energy cybersecurity solution that protects massive smart meter deployments. The solution ensures the secure exchange of data between legitimate energy actors for the entire lifecycle of devices. It empowers DSOs to take ownership and control of their smart grid security policy while leveraging a proven solution from the global leader in digital security.

**Meeting new security requirements while reducing operational costs**

Combining an advanced HSM, strong PKI-based authentication and the most recent encryption technologies, the Gemalto Trusted Key Manager (TKM) meets evolving security requirements from both regulators and DSOs. Deployed at all points of risk, it protects, defends and ensures the integrity of the entire smart grid ecosystem.

Built on cloud and micro-services based architecture, the solution perfectly integrates into existing back end environments, either on customer premises or through a hosted mode. All Gemalto solution use cases are mapped to existing business processes via APIs (device installation, maintenance, removal, etc.), optimizing overall grid management operational expenses (OPEX).

**A platform that merges into any existing configuration**

The Gemalto solution was purpose built for smart grids to smoothly integrate with any system configuration and operation mode:

- Integration with existing installed meter deployments
- Supports any communication protocol: PLC, cellular, LoRa, mesh, etc.
- Supports any DLMS protocol: suite 0, 1 and 2
- Micro-services based: automated security operations tightly integrated into business-driven APIs to simplify meter lifecycle management (activation, maintenance, deactivation)
- Flexible integration: deployed on premises or in hybrid mode (public/private) according to customer need
- Management of any device, whatever encryption model (symmetric/asymmetric) or secure container (embedded Secure Element [eSE], Trusted Execution Environment [TEE], Software keystore) is used

**Simplified device identity management from a central platform**

The Gemalto solution allows DSOs to manage the security of large fleets of devices through one central entity. It leverages built-in hardware to enable:

- Diversified and random device identity (ID) generation
- Secure meter and gateway ID key provisioning facilitated at the time of manufacturing in a trusted environment
- Automatic key exchange as devices are deployed, ensuring crucial change of ownership from meter manufacturer to DSO as well as enabling automated device discovery and onboarding (5 times faster than traditional deployment time)
- Secure key wrapping: trusted exchange of symmetric keys between back end servers and operating meter gateways

**Secure credentials and software lifecycle management**

The Gemalto solution enables device IDs and security updatability for each step of a device’s lifecycle: installation, maintenance, software and security updates all the way through to deactivation and removal.

- Certificate management: credential updates, revocations and renewals
- Symmetric key renewal
- Temporary access credential for remote technical maintenance
- Secure firmware and software updates through digital signature schemes
Automatic data encryption and decryption

The PKI-based solution automates encryption and decryption mechanisms to ensure data confidentiality and integrity between meters, gateways and back-ends:

- Use of market proven, standardized AES cryptographic algorithms protect the data at rest in gateways or Head-End-Systems, and when it moves between ecosystem layers
- Strong PKI-based authentication defines who is allowed to access the data
- Message signature protects against data tampering and enables non repudiation

Award-winning Gemalto SafeNet HSM

The Gemalto solution relies on the award-winning SafeNet Hardware Security Module (HSM), which acts as an anchor of trust:

- Secure generation, processing and storage of cryptographic keys inside a hardened, tamper resistant entity
- Dedicated processor specifically designed for the crypto key lifecycle protection

Gemalto’s proven suite of security solutions - PKI-based authentication, encryption technology, world leading HSMs and advanced security lifecycle management - provides DSOs with everything they need to protect the smart energy ecosystem while removing complexity in smart grid management. The Gemalto Trusted Key Manager protects massive global deployments and ensures integrity and reliability for the entire lifecycle of solutions.

To learn more about the Gemalto solution, download the Gemalto End-to-End Security Solution for Advanced Metering Infrastructure overview