THALES

gemalto
a Thales company

Securing Devices in Advanced Metering Infrastructures:

Recommendations for Smart Meter and HES Vendors

CHAPTER 1:

Trustworthy data: The essence of a successful smart grid

In the energy marketplace, data is the new oil

Smart grid managers and Head End System (HES) vendors depend on data to drive their business. Receiving and analyzing accurate data from grid endpoints - the smart meters - is the main element that determines business success. Their customers, Distribution System Operators (DSOs) and Advanced Metering Infrastructures (AMI) managers, then use this data for crucial processes: monitoring energy demand and production, load shifting to maintain a persistent grid balance at all times and billing customers. Each tiny bit of data is the starting point for monetization and asset management and it must be accurate and trusted in order to keep power flowing.

Ensuring data trustworthiness requires the implementation of a strong AMI security strategy, to protect devices generating data as well as the data itself, as it flows throughout the ecosystem.

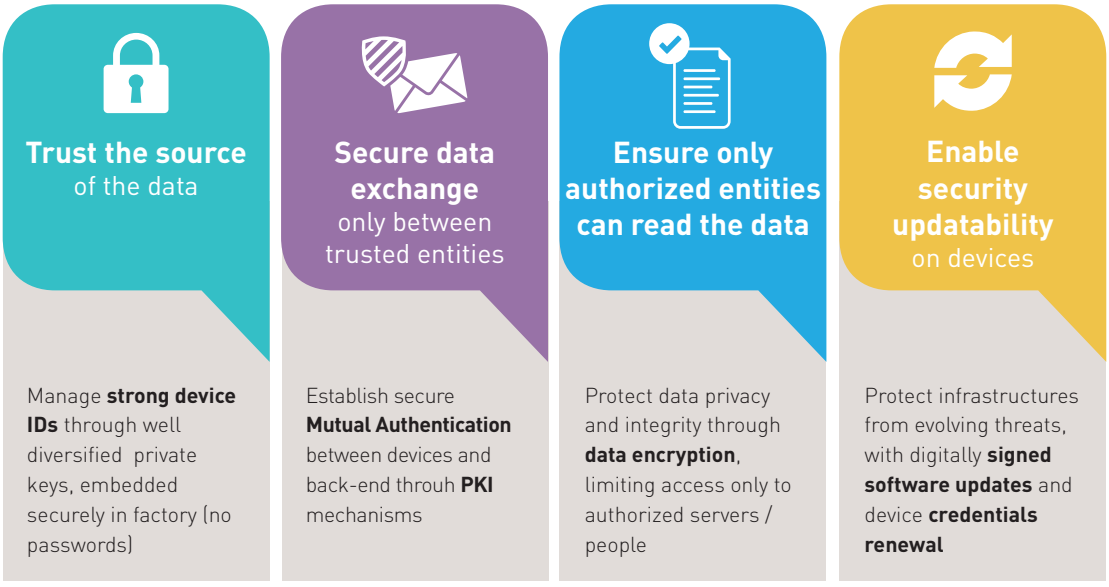
The principles of data security

Data in a smart grid is generated by hundreds of thousands, sometimes even millions of physically accessible yet unattended devices. When smart grid managers receive data, they must ensure that:

1. data is accurately associated to a legitimate endpoint or smart meter
2. data has not been tampered with or altered
3. data cannot be accessed by unauthorized entities

In order to achieve these requirements, **4 security principles** must be considered to ensure device security, legitimate ownership, data confidentiality and integrity throughout the infrastructure.

SECURITY: It´s all about 4 core principles



The importance of lifecycle management

Of these four principles, updatability is arguably the most important principle to ensure device and data security, as well as the one most often overlooked. Cybercriminal efforts move fast, rendering cutting-edge defenses obsolete in a matter of moments. In addition, zero-day exploits, social engineering attacks and insider threats have the potential to negate any benefits derived from encrypting traffic and data in the first place.

The ability to manage the security lifecycle of connected devices as well as to automatically and remotely control device and data access, is critical for steadfast cybersecurity of any IoT deployment. This is particularly true for devices such as smart meters that are expected to operate in the field for many years, up to 15 years for most. The key to a robust cybersecurity solution is flexibility. Credential and access policies should be adaptable and remotely managed across the whole network to quickly react in the case of a suspected breach, or to cope with new security threats or regulation.

Standards and regulations for secure lifecycle management

Essentially, lifecycle management ensures that a device's identity remains as secure as possible for as long as the device is in operation. Regularly renewing digital certificates, access credentials and rights is a must do practice. Similarly, ensuring that firmware is kept up-to-date and genuine remains a crucial aspect of minimizing the risk of devices being compromised.

Recognized security principles and prerequisites are becoming a key focus for DSOs and AMI managers, as well as for governments and national agencies, which are actively developing standards and regulations. Following is an overview of current or emerging regulations, standards and specifications around the world.

UNITED STATES

The IoT Cybersecurity Improvement Act of 2017 obliges government agencies to include specific clauses in their contracts that require digital security features for any Internet connected device acquired by the US government. Among the security features recommended, the Act requires secure updatability, stipulating that over-the-air (OTA) updates to fix or remove vulnerabilities should be done in a properly authenticated and secure manner, without using fixed or hardcoded credentials.

In addition, The National Institute of Standards and Technology (NIST), further refined recommendations for cryptographic key updates stipulating an exchange between one and five years depending on the key type and usage (see beside extract chart).

NIST SP 800-57 Pt. 1 Rev. 4

Table 1: Suggested cryptoperiods for key types

	Crytoperiod	
Key Type	**Originator-Usage Period (OUP)**	**Recipient-Usage Period**
Private Signature Key	1 to 3 years	–
Public Signature-Verification Key	Several years (depends on key size)	
Symmetric Authentication Key	≤ 2 years	≤ OUP + 3 years
Private Authentication Key	1 to 2 years	
Public Authentication Key	1 to 2 years	
Symmetric Data Encryption Keys	≤ 2 years	≤ OUP + 3 years
Symmetric Key Wrapping Key	≤ 2 years	≤ OUP + 3 years
Symmetric Master Key	About 1 year	–
Symmetric Key Agreement Key	1 to 2 years	

EUROPE

The Council of the European Union proposed an EU Cybersecurity Act to create a common cybersecurity certification framework to build cyber resilience and response capabilities. The Act strengthens the power of the European Union Agency for Network and Information Security (ENISA) making it the permanent agency for cybersecurity for the EU.

> Germany

The BSI, Germany's Federal Office for Information Security, requires BSI-certified smart meter gateways with encryption capabilities and digital keys rotation. The BSI also recommends the use of embedded Secure Elements (eSE) in gateways to serve as a tamper-proof storage for cryptographic keys.

> United Kingdom

The Department of Energy and Climate Change has defined security and confidentiality guidelines within the Smart Metering Implementation Programme.

> France

The National Council on Informatics and Liberty (CNIL), the national data protection authority for France, has mandated data encryption with best of class algorithms as well as specifications for encryption keys and device identity protection.

The National Agency for Security of Information Systems (ANSSI) has defined a security referential – with a set of guidelines, recommendations and best practices – that applies for smart metering dealing with personal information.

DLMS: Securing secret key exchange and metering data

Industry leaders collaborated on a standard to define and deliver a standard language for connected devices in the smart metering field – the **Device Language Message Specification or DLMS**. This language or communication protocol is designed to ensure interoperability, efficiency and security throughout energy infrastructures.

The DLMS provides different 'suites' that define sets of algorithms and security mechanisms suited to specific use cases. From there, security policies and devices capabilities determine which security elements must be used.

DLMS Suites and associated elements

SECURITY SUITE ID	SECURITY SUITE NAME	AUTHENTICATION ALGORITHM	ENCRYPTION ALGORITHM	DIGITAL SIGNATURE	KEY TRANSPORT METHOD	KEY AGREEMENT METHOD
Suite 0	AES-GCM-128	AES-GCM-128	AES-GCM-128	-	AES-128 key wrap	-
Suite 1	ECDH-ECDSA-AES-GCM-128-SHA-256	AES-GCM-128	AES-GCM-128	ECDSA P-256 (with SHA-256)	AES-128 key wrap	ECDH P-256
Suite 2	ECDH-ECDSA-AES-GCM-256-SHA-384	AES-GCM-256	AES-GCM-256	ECDSA P-384 (with SHA-384)	AES-256 key wrap	ECDH P-384

Source: DLMS User Association – Smart Metering Standardization

Suites 1 and 2 (as shown in the graphic) introduce asymmetric encryption algorithms (based on the use of a pair of keys - private and public) for digital signature and key agreement methods. Thanks to asymmetric encryption, the latest DLMS suites 1 & 2 bring data integrity among the tangible use cases. This is key to ensure energy consumption data has not been tampered with, for example, and that data securely flows from edge devices to the HES.

SYMMETRIC AND ASYMMETRIC ENCRYPTION: ONE COMPLEMENTS THE OTHER

Symmetric encryption (e.g. AES) occurs when the same key is used to encrypt and decrypt a message.
It is fast, but the main challenge is that the key must be known by each party before making use of it. Thus, the sharing of this key among several parties weakens the key.
On the other hand, asymmetric encryption (e.g. RSA) involves a key pair, both a private and public key for each party. The difficulty here lies in getting or provisioning the keys, which requires expert knowledge and the operation of a Public Key Infrastructure (PKI). PKI-based encryption is highly scalable and allows the secure exchange of information between millions of parts. In fact, it is quietly at work behind the scenes to enable web browsing.

In a pair of private/public keys:

- The **Private key** is used to generate signatures that anyone can verify with the corresponding public key. It is also used to decrypt data sent by anyone using the related public key.
- The **Public key** (or a certificate) is used to verify a signature and authenticate the entity owing the private key. It is also used to encrypt data that only the owner of the corresponding private key will be able to decrypt.

Quite often, such is the case for datagram Transport Layer Security (dTLS), once all the key pairs are in place with public keys stored within public certificates, then some ephemeral symmetric keys are exchanged using asymmetric encryption. This means that the symmetric keys are exchanged in a secure way, can be used for quicker data exchanges, and then later on discarded.

Although setting and operating a PKI requires some resource and knowledge, the benefits are real and tangible:

- All tools and facilities (through standardized interfaces) are in place to renew and even revoke certificates
- Digitally signed firmware updates are allowed, notably for Data Concentrators (DCs) and smart meters
- Maintenance operations personnel can access devices in a secure manner

More specifically for the smart metering use case, asymmetric encryption allows the secure exchange of energy asset ownership, switching from factory configuration to deployed production ownership.

Once the credentials from the various smart meters and DCs have been identified by a central security entity - managed by grid managers under DSO mandate - it is then possible for them to securely operate the freshly delivered and installed meters or DCs. The HES and the DC can securely exchange new credentials that are now solely known by the DSO, and no longer by the smart meter vendor or DC manufacturer.

When PKI-based solutions are used in conjunction with a central Certificate Authority (CA), DSOs are free to work with a variety of different smart meters and data concentrator manufacturers. The CA creates and delivers certificates and credentials for different ecosystem stakeholders including maintenance personnel, manufacturers and firmware developers. At the same time, DSOs can maintain tight control of security lifecycle management.

CHAPTER 2:
The limits of the ´first line of defense´

Smart grid managers today are aware of the vital importance of mitigating the risk of cyber-attacks. Many have begun implementing "first line of defense" security architectures that focus on 2 of the 4 main security principles. They make certain that smart meters are given a **personal digital ID**, in the best case using diversified cryptographic keys, and they ensure that **data is encrypted** in all devices.

Establishing diversified devices IDs was set to limit Mirai-type attacks by eliminating common credentials including similar and easy-to-guess hardcoded passwords for a whole fleet. To prevent this, unique keys are injected into smart meters and used for 2 purposes: identity validation and encryption.

Though these principles are advancing industry best practices for security, they are not enough to protect the grid for the long lifespan of smart meters. Usual implementations do not solve the requirements of end-to-end security, regular device updates and keeping operational processes simple.

Identified limitations of current efforts

1. Challenge: Creating, provisioning and storing diversified device keys, in a secure way

SMART METER MANUFACTURING PROCESS

Generating and injecting unique and diversified device IDs into smart meters is not a simple process. It requires specialized software, secure servers and expertise, to avoid key interception or "leakage" during the device provisioning. Furthermore, when device IDs and secret keys are inserted at the time of meter manufacturing, smart grid operators and DSOs need assurance that the factory itself is a secure environment protected against potential cyber-attack and dishonest employees. Devices not manufactured in a secure facility are vulnerable to credential hacking that could wreak havoc on the grid. Illegitimate devices with cloned credentials can send false data and disrupt the whole grid balance. Furthermore, poorly protected devices could enable hackers to access private data and artificially reduce bills, resulting in large revenue loss for utilities.
To stay on the safe side, the root key (also called master key) used for symmetric keys derivation, or the Certificate Authority private key used to sign device certificates, must be carefully and securely stored, preferably in an independent Hardware Security Module (HSM). This is the core asset of a solid security system, which ensures that secret keys are never exposed to the external, IP world.

KEY EXCHANGE BETWEEN ECOSYSTEM PARTNERS

Whatever the mode chosen for generating and provisioning device IDs in the meter factory, there is a need for a secure mechanism to exchange device keys with the DSO and back-end systems. These device keys should then be renewed by DSOs and grid operators for them to securely manage devices remotely. This is a crucial element of smart grid security, which should rely on a Public Key Infrastructure (PKI), clearly separating stakeholders and responsibilities.

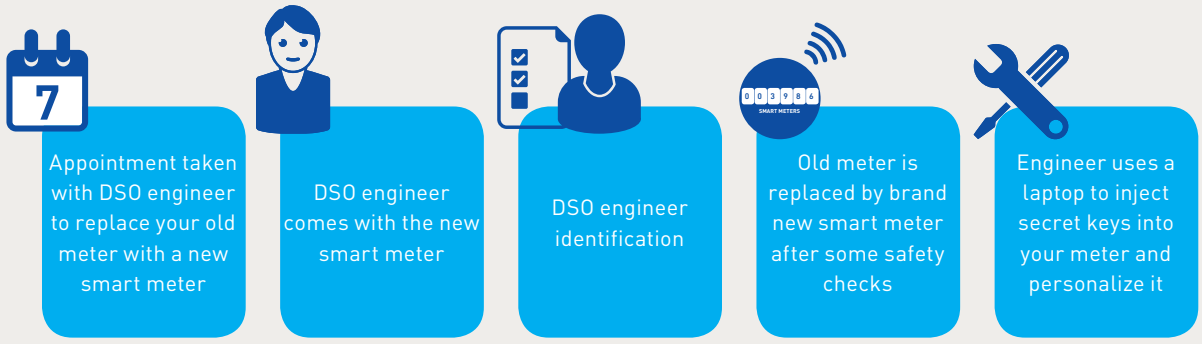
METER INSTALLATION

In some scenarios, a technician is in charge of the key injection during meter installation. In this case, either the technician has access to the keys that are populated in his hand held unit, or the keys are transmitted in real time by the IT team. This requires connectivity, which can be tricky when meters are installed deep in building basements, for example.

When keys are pre-provisioned on smart meters, the smart grid manager typically links them in the inventory database to the device's serial number. When a technician installs a meter, he reads the serial number and provides it to the back-end system. This human information retrieval process allows the back-end to provision the meter to the network and to its corresponding gateway. This system is fraught with vulnerability. A simple mistake in serial number retrieval would lead to impossible commissioning, leading to meters that are not readable.

Allowing a technician or even an engineer to enter into a private space to install an important asset like a smart meter also requires a great deal of trust. How can one be certain that the laptop used for installation is free of viruses that could infect the smart meter? And what guarantees does one have that the injected secret key won't be spread through malicious software in the laptop?

Usual smart meter installation



It is thus highly recommended that automated processes be implemented prior to meter installation, to ensure automatic authentication of legitimate providers and genuine devices as well as direct onboarding to the gateway and network at installation and first use.

DISASTER RECOVERY SITE CASE

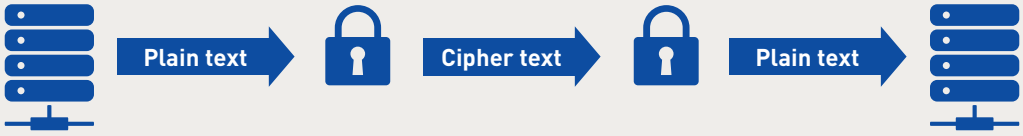
To ensure resilience and availability, DSOs should consider a disaster recovery site implementation. Hence the same sensitive keys are located in 2 different places, creating multiple points of vulnerabilities. It is then crucial that an advanced security solution is replicated in the recovery site, to have the same level of security as in the primary site.

USING ASYMMETRIC CRYPTOGRAPHY TO SECURELY EXCHANGE SYMMETRIC KEYS

When symmetric cryptography is used, several entities share the same access key to a device (contrary to the asymmetric method, where entities don´t share common keys), which makes this key weaker over time. This is one of the reasons for the existence of the DLMS suites 1 and 2 – it pushes the use of asymmetric encryption to ease and secure the key exchange process as well as key renewal between stakeholders, while ensuring keys are under the sole control of its owner.

It is far more efficient and faster to encrypt applicative data with symmetric algorithms. However, it is recommended to use asymmetric encryption for the initial key generation between partners: keys are then wrapped in a secure way, to prevent from key interception. Then, once keys have been generated, a symmetric encryption method for data exchange can be further used.

Secure session key generation



Sender	Encryption	Decryption	Recipient
The sender generates a session key	The recipient´s public key is used to encrypt the session key	The recipient´s private key is used to decrypt the session key	The session key has been securely exchanged. It can now be used for faster symmetric exchange

The reality is that various data concentrators and smart meters vendors implement and work with different DLMS suites (some using only DLMS suite 0, unlike others implementing suites 1 or even 2). Grid managers could thus be facing the simultaneous management of different suites, which increases complexity. For this reason, the security system in place should be one that is able to accommodate any kind of device using any DLMS suite, in order to process data coming from various vendors, in one unique platform.

2. The importance of isolating secret keys from the external world

Storing secret keys in an HSM under direct control of a Meter Data Management System (MDMS) or any internet facing system such as an HES is risky and should be avoided. Indeed, even if a firewall is in place in the vicinity of the HSM (to validate or block inbound/outbound connections according to ruleset) as well as a reverse proxy, the HSM will still be reachable and exposed to the possibly compromised IP world. It is then crucial that the HSM operates independently from the MDMS or HES, with its own access control rules, even if both are positioned at a same physical location.

Dedicating the management of your secrets to a specialized system (also called Key Management System or KMS) ensures the non-disclosure of any of them and guarantees to limit the access to your sensitive business data to only strongly authenticated, authorized and identified entities. No keys should be left uncontrolled in secondary systems where security policies may be overlooked.

Primary security initiatives are a good start and show that energy actors understand the importance of cybersecurity. Too often though, these initial measures are incomplete to truly protect the energy infrastructure end-to-end during the long life of connected energy assets. The next section goes through a list of best practices and recommendations to make sure all layers of the ecosystem are truly protected. One should never forget that cybersecurity infrastructure is only as strong as its weakest link.

CHAPTER 3:

Improving cybersecurity with best practices, while simplifying metering roll-outs

AMIs and smart grid devices possess specific features inherent to energy that are not common in other IoT verticals. This includes the large number of deployed devices, their longevity, the sensitive nature of generated data, the need for highly secure key generation and provisioning along with the necessity of regular credentials revocation and exchange. All of these elements necessitate a tailored-made solution that takes all involved actors into account, from smart meter manufacturers up to DSOs managing the grid.

Simplifying processes through a central key management platform

SIMPLIFIED KEY PROVISIONING FOR HETEROGENEOUS DEVICES

Meter manufacturers deliver their devices to DSOs together with provisioning data using their own preferred file formats. In most cases, provisioning digital keys to these specific file formats can prove difficult. It involves a lot of back and forth activities between manufacturers and back end systems providers to adapt the device format for key provisioning.
This can be greatly simplified when a central key management system supports an easy mapping between the factories´ device file formats and their security attributes as used in the security solution. In this configuration, DSOs and AMI managers can easily handle a variety of heterogeneous devices, meter vendors and Head End Systems. Any device or new vendor can be simply and quickly integrated in the platform, whatever key file format or DLMS protocol is used (suite 0, 1 or 2).

REDUCED GLOBAL TCO

Managing devices identities and access credentials from one unique platform, with a single HSM cluster, results in better process efficiency and reduced Total Cost of Ownership (TCO), as all security operations are run from one unique location:

- **Certificates and key generation**
- **Key storage**
- **Encryption/decryption** between all ecosystem elements: meters, data concentrators and back-end systems
- **Secure key provisioning** with symmetric key wrapping for secure credential exchanges between back-end servers and edge devices
- **Secure credentials and software updates** run simultaneously towards a whole fleet of connected devices, to act quickly and widely (crucial in the case of a breach suspicion, for ex.)
- **Integration of security operations into traditional operational processes:** meter installation, maintenance, firmware and software updates, access grant and renewal, meter removal

A centralized security solution architecture that is able to manage both asymmetric and symmetric encryption mechanisms strongly simplifies the management of all operations. This significantly increases operational efficiency and reduces the perimeter where secrets are kept.

Claiming device ownership to limit metering data access

In addition to meeting emerging standards and regulations that govern device lifecycle management, DSOs and AMI managers are increasingly becoming aware of the importance of being able to protect the ownership of a device identity (keys), a critical element of the overall system integrity.

To control onboarding of new meters and gateways, DSOs need to rely on strong initial credentials built in the devices by device makers, to ensure only genuine devices are enrolled into their network. But they also need to take ownership of the devices by replacing these initial credentials with their own on the first use of the device, while disabling device manufacturers´ potential access over their assets.

The initial credentials may be factory device certificates, issued by the smart meter manufacturer´s Public Key Infrastructure (PKI), which will then be replaced by operation certificates, issued by the DSO PKI.

DSOs, though, often build and operate their own PKI using self-signed digital certificates. However, it is highly recommended to work with an independent and expert Certificate Authority (CA) that is capable of issuing root certificates and device certificates with the right level of protection for critical ecosystems. Partnering with expert PKI providers, using CA expertise, brings the guarantee for DSOs to work with the most-advanced security encryption mechanisms, which have been specifically built for credential management of energy assets.

Ultimately responsible for the grid´s stability, DSOs and AMI managers benefit from such ownership schemes, which guaranty a high level of security as they fully own all access credentials. Such schemes also enable grid managers to monitor and control their energy assets efficiently, from a unique credential lifecycle management platform, even if meters have been acquired from several device manufacturers. This is crucial, as multi-sourcing is a reality in large grid deployments.

Securely storing device master keys and CA root private keys in a tamper proof environment

As seen in chapter 2, isolation is a well-known rule when it comes to security. Indeed, the more barriers you put between your most precious assets and the external world (and potential source of attacks) the better. This leads to network segregation, firewall and reverse proxies for instance.

When using a Public Key Infrastructure to manage credentials generation, storage and provisioning, Certificate Authority private keys or root keys are a high value asset. They need to be protected by a Hardware Security Module that is not part of the HES so there is no way to reach it from the ´external´ world. This respects the isolation rule of thumb for security.

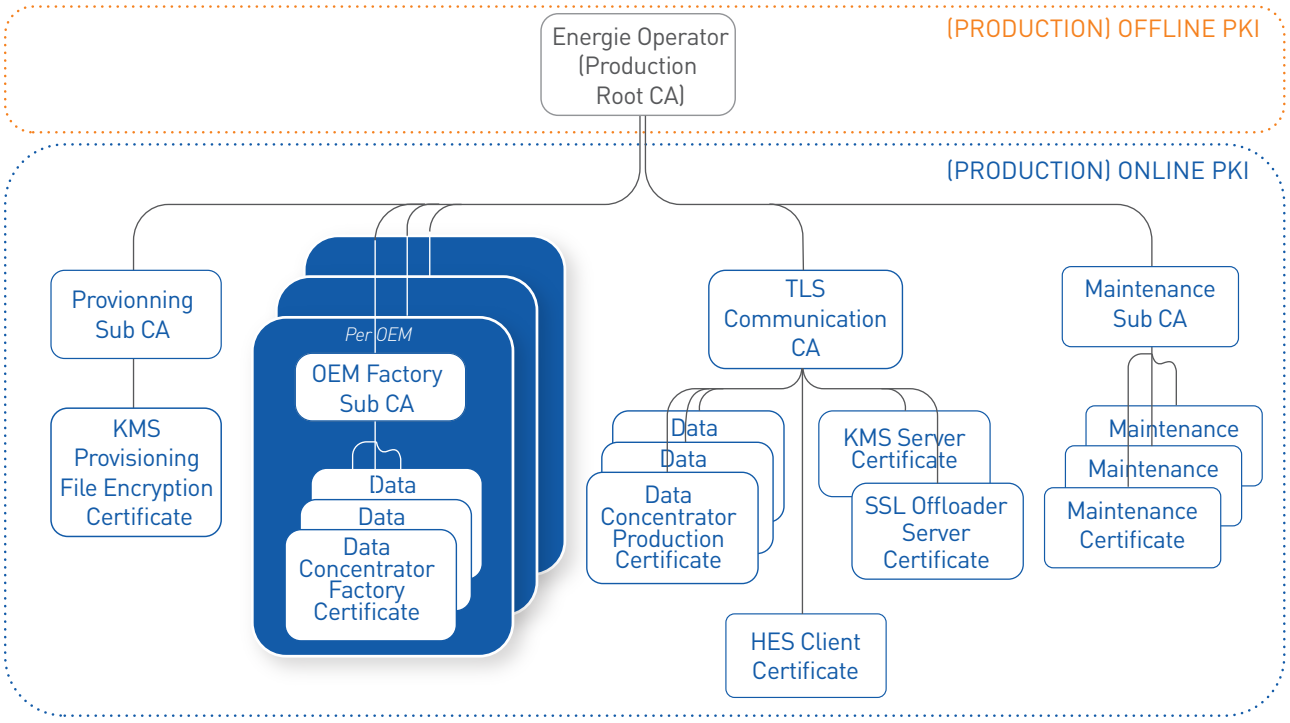
An HSM is definitely the most secure and appropriate method to safeguard encryption keys. Using such a solution, already proven in banking and the most stringent industries, ensures state-of-the-art protection. Regulations such as GDPR demonstrate how severe penalties can be for companies who do not take all possible measures to protect personal identifiable information (PII) and, in the context of smart energy, to also protect the grid from potentially severe hacking. The HSM is seen as a key component of a grid security solution that must be tightly integrated with other subsystems.

Adding an extra layer of isolation, on top, greatly improves the security as well. This can be achieved by having the most critical assets (CA root private key, master key used for derivation of the meter´s symmetric keys, etc.) accessed only through well-defined APIs with stringent role-based access and strong authentication.

Roles and responsibilities are mapped to individual users, making it easy to ensure that each user or system can only do what it is authorized to do. Unique IDs enable auditability at the HSM level making it possible to link any observed activity to a unique requestor.

A production environment is more exposed to risks as it is used for daily operations. This means that the online PKI itself, comprised of various sub CAs used to generate certificates for the different assets, is potentially at risk. An offline PKI secures the Root CA (with a very long lifespan) and reinforce its security. The Root CA is stored on USB HSM connected to a mobile laptop that must be stored in a safe.

Offline versus Online Public Key Infrastructure



Implementing a security lifecycle management

Lifecycle management or updatability capabilities are crucial in an AMI, to cope with secure device updates, regulation or to manage a variety of third parties that might need to access metering devices or data for short periods of time.
There are 3 use cases calling for the implementation of a solid security lifecycle management platform:

1. REGULAR KEY RENEWAL

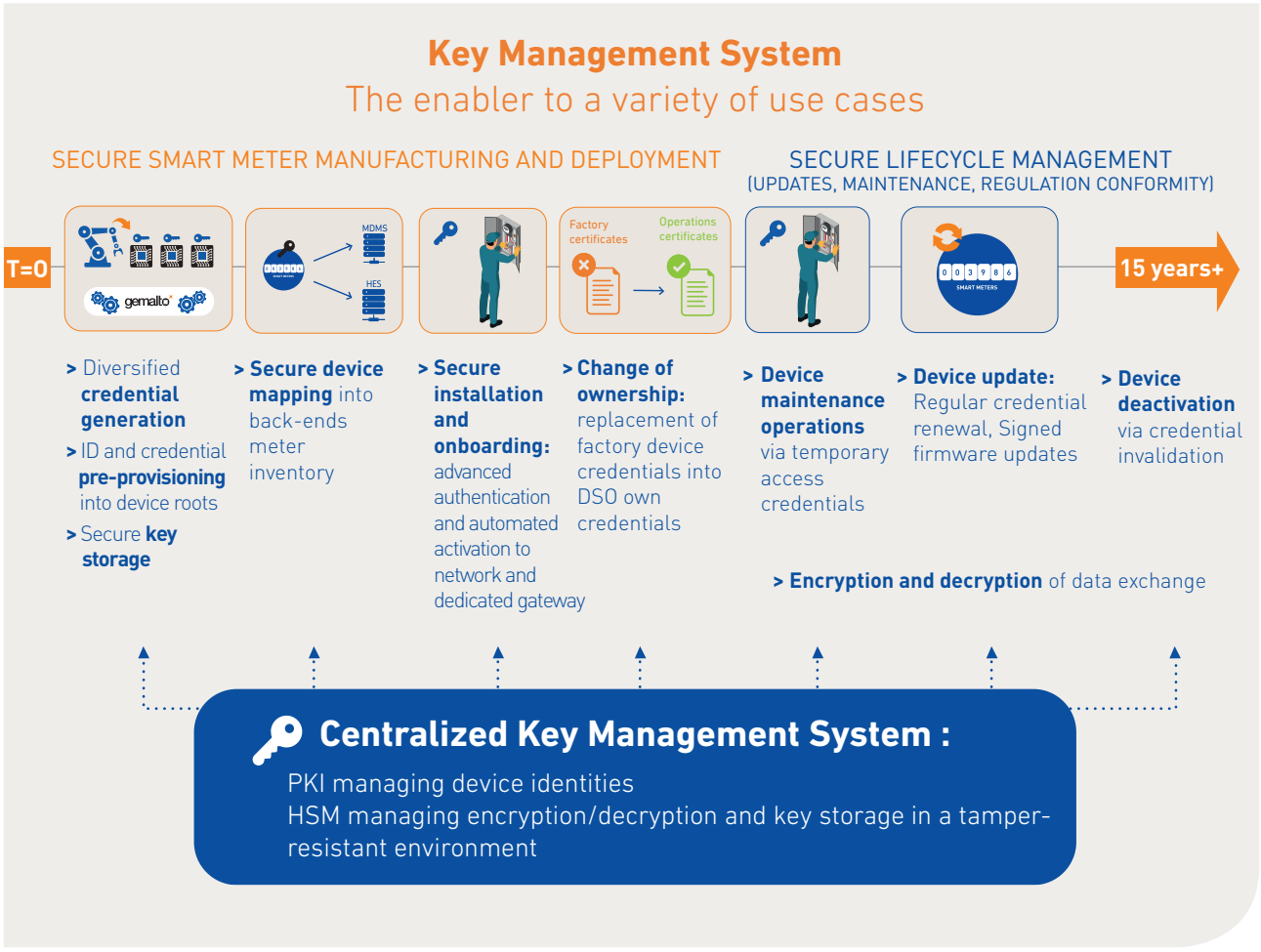
All along metering devices lifetime – from their production to their end of life – credentials need to be loaded in devices and then renewed. Secure, remote exchange of credentials allows energy actors to follow regulator recommendations or requirements for key rotation. This ensures device access is regularly replaced and a constant protection level is possible over the long run.

2. TEMPORARY ACCESS CERTIFICATES AND CREDENTIAL RENEWAL

Maintenance operations are a regular component of smart metering projects. In this context, it is important to control who gains access to data concentrators or smart meters and for how long. Third parties should be given access for a limited time only, allowing them to do the job they have to do, after which credentials should be revoked.
The PKI allows the automatic renewal of certificates while automatically revoking previous ones, based on administrator settings. This improves device and infrastructure security and mimics what users do with passwords for email, online banking, etc.). In case identity and access would be compromised, it is very easy and quick to revoke the certificate in question, hence tackling the security issue at the very beginning.

3. SIGNED SOFTWARE AND FIRMWARE UPDATES

As new applications, new security threats or even bugs are discovered, firmware updates are regularly needed during a device lifecycle. This enables devices to remain at their best operative level.
Because software updates are sent remotely to large fleets of devices, it is important to ensure that the entity sending these updates digitally signs what will be loaded into these devices. This ensures that the update comes from a legitimate entity and that the update content has not be altered on the way to the device. The PKI enables this secure process.



For more information, please check our dedicated **Gemalto smart energy webpage** with related documents.

GEMALTO.COM/IOT

THALES

gemalto
a Thales company