Thales Trusted Key Manager

THALES

End-to-End Cyber Security **for Critical IoT Infrastructures**

The IoT connected devices ecosystem is in rapid expansion, leading to an increasingly interconnected world where various devices and systems communicate and exchange data. Unfortunately it creates opportunity for cyber attacks. For cirtical infrastructures such as healthcare, automotive or smart energy, **there is a strong need to secure connected devices for their long life operation.**

Thales offers a device centric security lifecycle management solution that ensures end-to-end protection of valuable IoT assets and data.

The IoT offers unprecedented benefits. Connected devices generate insightful data on market activity and customer usage patterns for products and services. But if not well protected, these devices could easily be hacked to gain access to sensitive data, to alter consumption information, or even to damage critical governmental infrastructures. The consequences of cyber-attacks could be devastating for companies and lead to a loss of reputation, customers, and revenue.

Steady security is paramount to the success of critical infrastructures

In response to the growing number of cyber threats, governments and regulators launched initiatives that mandate specific protection protocols for critical IoT deployments. 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.

IoT devices such as smart meters can have a lifecycle of up to 15 years. Therefore, an advanced security mechanism to replace aging keys and enable remote security management is paramount.

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

Strong encryption and authentication tools must be considered and implemented before IoT devices 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 critical infrastructures

As IoT networks expand, vulnerability and attack points multiply at every touchpoint:

- **IoT devices:** Unprotected points of connectivity can become digital doorways to the entire ecosystem, allowing device cloning, device data manipulation, or alteration of a device's global performance.
- **Communication layer:** As data transitions through a gateway or directly to an IoT management platform, 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:** IoT or business application platforms receiving and analysing data generated by IoT devices must have strong authentication and encryption mechanisms in place. This ensures the applications are legitimate and the data can be trusted.

Cricital IoT infrastructures require seamless, built-in security at every layer to ensure complete system integrity.

Thales Trusted Key Manager: Ensuring end-to-end security for critical infrastructures

Leveraging decades of digital security expertise, Thales offers an advanced cybersecurity solution: the Trusted Key Manager. The solution protects massive IoT devices deployments and ensures integrity and reliability for the entire lifecycle of devices.

The Thales cybersecurity 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 leverages leading-edge authentication and encryption technology with digital code signing certificates. This ensures IoT data is received from a legitimate source while safeguarding against data tampering and fraud at all points. The solution facilitates dynamic credential and security updates and authorizations – without costly service in the field.

The Thales solution provides 3 pillars of security to ensure global protection:

- **Device Key Provisioning**
  The Thales solution expertly manages key and credentials provisioning, allowing device makers to focus on their core competencies. It securely provisions encrypted keys in IoT devices at the time of manufacturing, which eliminates the need to send keys over the air and greatly reduces the cyber-attack surface of the ecosystem.
- **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 devices and applications that can prove their legitimacy. The process leverages standardized cryptographic algorithms and a highly reliable digital authentication handshake between data sender and receiver. The mutual authentication and encryption mechanisms ensure that data transferred over the network has not been altered, is coming from a legitimate source, and is undecipherable to eavesdroppers.
- **Security Lifecycle Management**
  Because IoT lifecycles can span many years, new players will come and go, hackers will become smarter, and keys will depreciate.

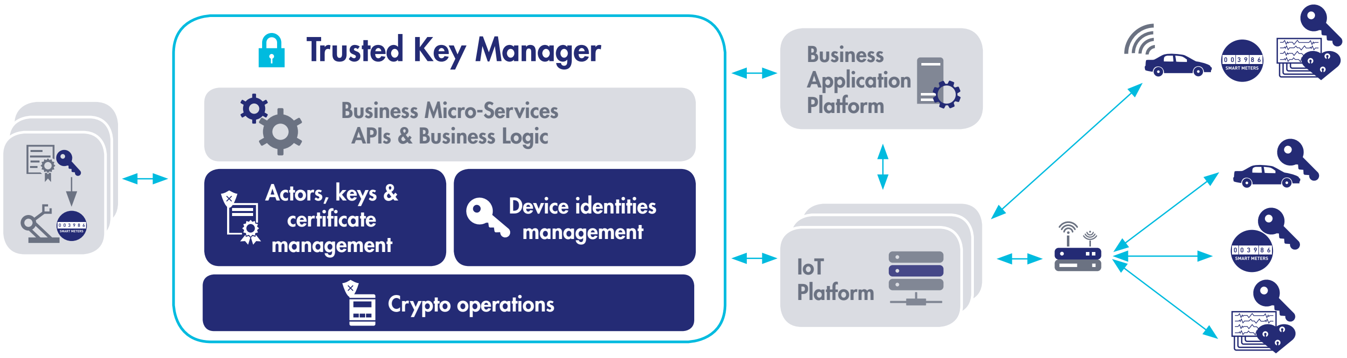
  Thales solves this challenge and provides continuous protection through remote credential management, thus enabling secure updates and renewal of crypto keys over the lifetime of devices.

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

The Thales Trusted Key Manager acts as a safe certificate authority to guard keys and credentials, keeping the most critical infrastructures protected against ever-evolving cyber threats. IoT device owners can keep security at its highest level, without increasing operational time and cost.

Learn more on our dedicated [Trusted Key Manager webpage]

Trusted Key Manager – At the center of all IoT operations


Trusted Key Manager
Business Micro-Services
APIs & Business Logic
Actors, keys & certificate management
Device identities management
Crypto operations
Business Application Platform
IoT Platform
SMART METERS