PEARL IoT

Connected Objects

Securing and remotely managing the digital identity of IoT devices

The IoT sector is expected to expand to 20.4 billion devices by 2020*, creating a massive exchange of data on cellular or non-cellular networks. With this growth comes new security concerns about confidentiality, integrity and the control of shared information. PEARL IoT is part of IDEMIA's solution to ensure end-to-end security from connected devices to the cloud.

*Source: Gartner

Today, the vast majority of connected objects are not properly secured. Cyber attacks not only put a company brand reputation and revenue at risk, but can also be a threat to human safety. To ensure adequate security, key actors in the IoT sector must tackle several challenges: sender and receiver authentication, device and data integrity protection, as well as the confidentiality and privacy of information.

Our offer

PEARL IoT is a remotely programmable turnkey secure element. It provides a wealth of advanced capabilities to deliver robust security and trust that we have come to expect from today's IoT solutions. Tailored for end node devices in a constrained power and resources environment, it creates end-to-end security for industrial and home appliances, such as smart meters, CCTV cameras, remote patient monitoring and a variety of other connected objects. PEARL IoT is a ready to use security solution that supports strong authentication, secures physical and logical storage and allows for constant management using IDEMIA's M-TRUST security cloud platform.

Why IDEMIA?

With billions of trusted chips deployed worldwide over the past 25 years, IDEMIA has extensive know-how in secure hardware and embedded OS development, unique expertise in cryptography, security certifications and secure personalization.

Our range of embedded products (PEARL Consumer, IoT, Auto) addresses different market verticals, but always uses the same eSE secure core technology. PEARL IoT is the answer to today's IoT challenges.

Benefits

Highly secure

Tamper-proof secure element certified by independent accredited laboratories (EMVCo & CSPN certified)

Convenient

Remote device administration with simplified provisioning at manufacturing stage for OEMs/ODMs and optimized device lifecycle management

Easy to integrate

Small footprint, ultra low power, enabled by a comprehensive product support package

IDEMIA

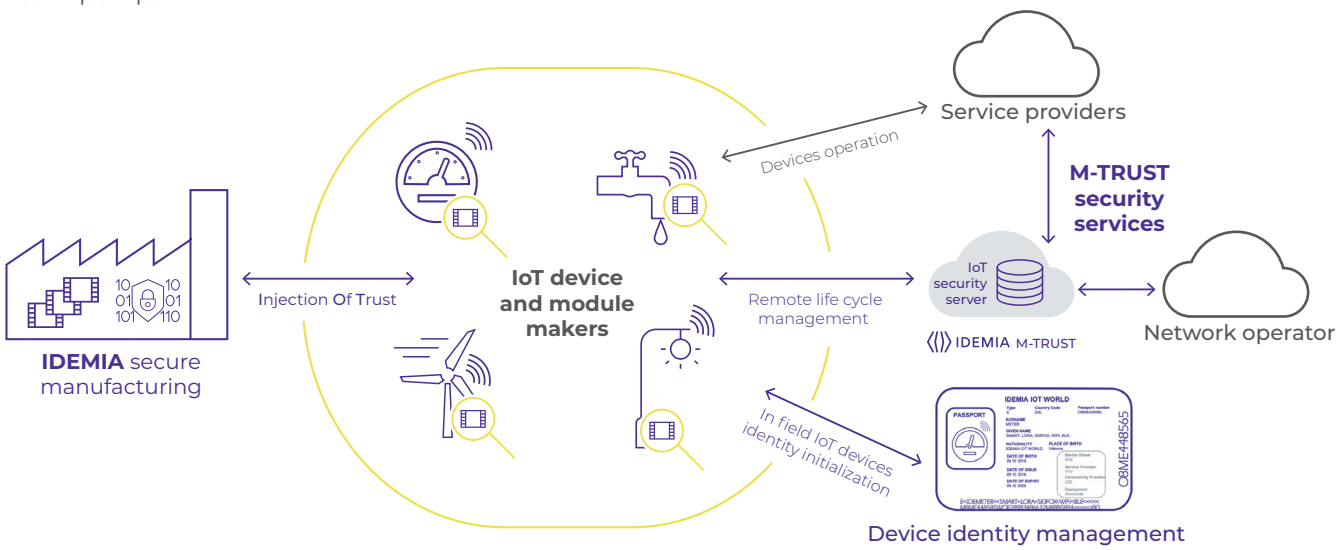
How it works?

When powered on, the IoT device connects to IDEMIA's security cloud platform, M-TRUST. Device identity is authenticated with a pre-shared secret key, securely stored in the platform and in the PEARL IoT, which prevents the use of non-authorized devices or cloning. PEARL IoT then establishes an optimized secure communication channel, matching with low bandwidth and low power constraints. This channel ensures data integrity and the exchange of authenticated encrypted information allowing users to remotely operate and control the device.

PEARL IoT features the latest cryptographic mechanisms that securely collect confidential data, such as clinic data, from an object or verify the approval of a secure command, such as triggering a critical action on an insulin pump.

Securely and remotely controlling devices creates many additional benefits:

- Simplifies the logistic flow with remote final provisioning information
- Avoids any key exposure and reduces cost impact of human intervention in the field
- Creates the possibility to modify device identity attributes throughout the product lifecycle (to reflect changes in object ownership, network or service provider)
- Evolves with the changes in security protocols
- Implements deterministic key renewal security policies.



Cutting-edge technology

HARDWARE

- Secure microcontroller: 256KB Flash, 5KB RAM, crypto HW accelerator
- Size: 3x3mm² - DFN6 package
- Communication interface: I²C + 1 GPIO
- Power consumption: 2.8mA operating current, 0µA sleep
- Power supply: 1.8V / 3V / 5V

SOFTWARE

- Native OS implementation
- Nano HSM local security tool box
- Elliptic curve and digital certificates
- Secure counters
- Optimized end-to-end secure channel (MLS - Message Level Security)
- On chip GPIO controllable over MLS secure channel
- Remote key management over MLS
- LoRaWAN & Sigfox security protocol

And tomorrow?

- Detection of abnormal application processor behavior through an advanced patented mechanism (Microcontroller Unit surveillance)
- Over-the-air security countermeasures update
- Remote management of security protocols and evolving cryptographic standards
- Remote provisioning of credentials at initial activation stage for major AEP (Application Enablement Platform) providers