M-TRUST

Securing the identity of objects and communications for IoT devices

Connected Objects

Mobile Operators

The IoT sector is expected to grow to 20.4 billion devices by 2020*, connected on cellular or non-cellular networks and exchanging tons of data. New security concerns are emerging about confidentiality, integrity and control of shared information. M-TRUST is IDEMIA's solution to ensure end-to-end security from the connected device to the cloud.

*Gartner

Today, the vast majority of connected objects are not properly secured. Cyberattacks represent a risk for a company's brand reputation and revenues, but can also be a threat to human safety. To ensure the appropriate level of security, the main actors of the IoT sector have to tackle several challenges: authentication of sender and receiver, device & data integrity protection, information confidentiality & privacy.

Our offer

M-TRUST is a cloud server platform that enables the secure management of connected objects. It ensures that data exchanged will not be tampered or read by unauthorized parties.

This network-agnostic solution addresses cellular (3G / 4G / 5G /Cat M1 / NB-IoT) and non-cellular (LoRa / Sigfox / short-range) networks. Regardless of the communication network used, M-TRUST securely identifies the devices and servers and ensures authenticated encryption for secure data and command exchanges. It prevents security breaches such as device cloning giving an entry point for malicious code or data mining.

Combined with remote monitoring services, M-TRUST provides advanced features to guaranty the integrity of the data, function and device such as secure booting to achieve software updates and implement security standards evolution.

Why IDEMIA?

IDEMIA stands for Augmented Identity, capitalizing on its innovation and experience to enable robust digital identity solutions for the connected objects of the IoT.

Recognized as a major security player, IDEMIA leverages its expertise in remote connectivity management and in digital software signature to extend it to remote security management of connected devices. As a main stakeholder in the IoT ecosystem, IDEMIA has forged strong strategic partnerships to address the entire market.

Benefits

Highly secure

Managed in our certified data centers as a service (SaaS) or deployed as an outsourced platform, M-TRUST brings top-level end-to-end security.

Convenient

M-TRUST enables remote device administration with simplified provisioning at the manufacturing stage for OEMs/ ODMs and optimized device life cycle management for applications, network operators and service providers.

One-stop shop

IDEMIA provides security solutions from the connected object to the cloud. It is no longer necessary to piece together different products from multiple vendors.

IDEMIA

How it works?

With a complete offering of secure elements (e.g SIM/eUICC/eSE/etc...), TEE (Trusted Execution Environment) and associated middleware, protecting data and keys stored in the end-point devices, M-TRUST features a comprehensive set of security services including the creation and management of connected objects' digital identities (keys, digital certificates).

Device onboarding and activation can be easily achieved through initial remote provisioning. Secure commands, device configuration and key rotation are also available through remote administration services. Such services come with extensive notifications attesting to the proper execution on the device.

IoT security fundation

Secure elements PEARL IoT, PEARL Auto, DAKOTA IoT, DIM®

Several form factors based on tamper proof secure hardware

Various cryptography

Secure Triangle

Secure factory & datacenter

Physical & logical security

Secure management of keys, certificates & customer credentials

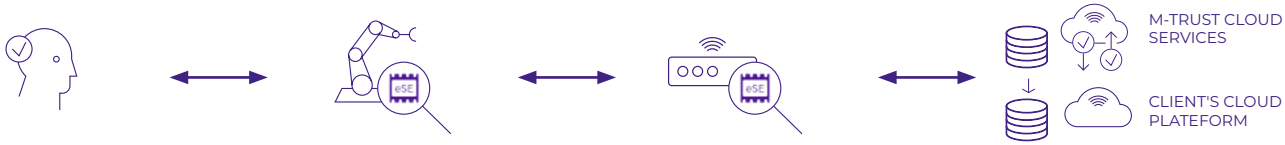
Server M-TRUST

Key Management Server (KMS) based on Hardware Security Module (HSM)

Advanced cryptography

Secure storage of keys and certificates

IDEMIA M-TRUST for IoT security



Users/Artificial Intelligence

- Identity & Access Management (IAM)

Devices

- Initial provisioning
- Secure storage
- Intra-device communications
- Data stamping
- Secure boot
- Trusted firmware updates

Communications

- Device authentication
- End-to-end encrypted data

Security lifecycle

- Remote device credential management:
  - Key renewal
  - Certificate verification, revocation and renewal
  - Blacklist / whitelist
- Security diagnosis:
  - Device logs
  - Device behavior analysis
- Security recovery:
  - Degraded mode

Cutting-edge technology

- Network-agnostic solution
- Flexible platform capable to match with various security policies and requirements
- Compliant with the latest security market standards and certifications (EMVCo, PCI, Common Criteria, CSPN, SaS GSMA)
- Unified interface for security services administration to minimize development effort with application enablement platforms
- Designed for scalable deployment

And tomorrow?

- Security diagnosis: execution check, event logs, analytics, counter measures with local decision making will be available in the next M-TRUST release
- Artificial Intelligence: behavioral analysis, quality of services

© Copyright 2018 All rights reserved. IDEMIA | EN - 09/18 | Photo: IDEMIA

IDEMIA

All rights reserved. Specifications and information subject to change without notice.
The products described in this document are subject to continuous development and improvement.
All trademarks and service marks referred to herein, whether registered or not in specific countries, are the property of their respective owners.

Join us on

www.idemia.com