MTG

Enterprise Resource Security
Mastering Cryptographic Key Lifecycles

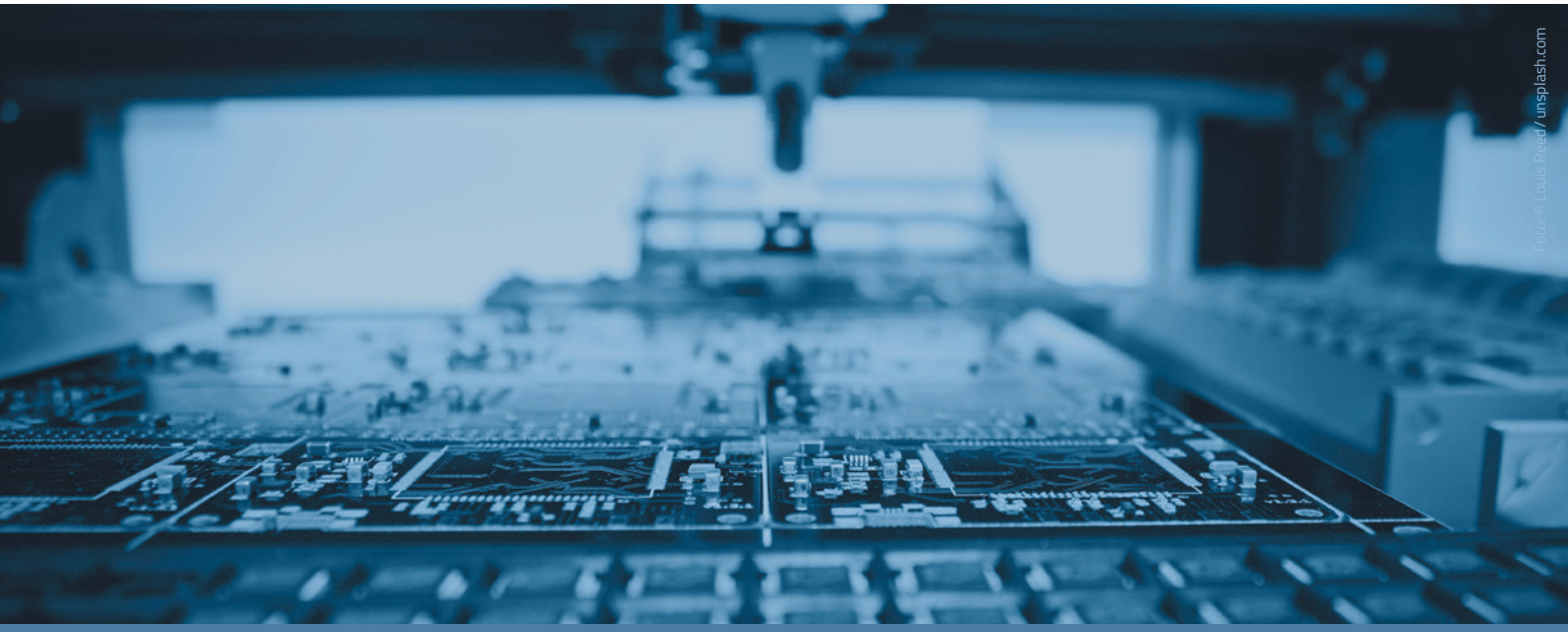


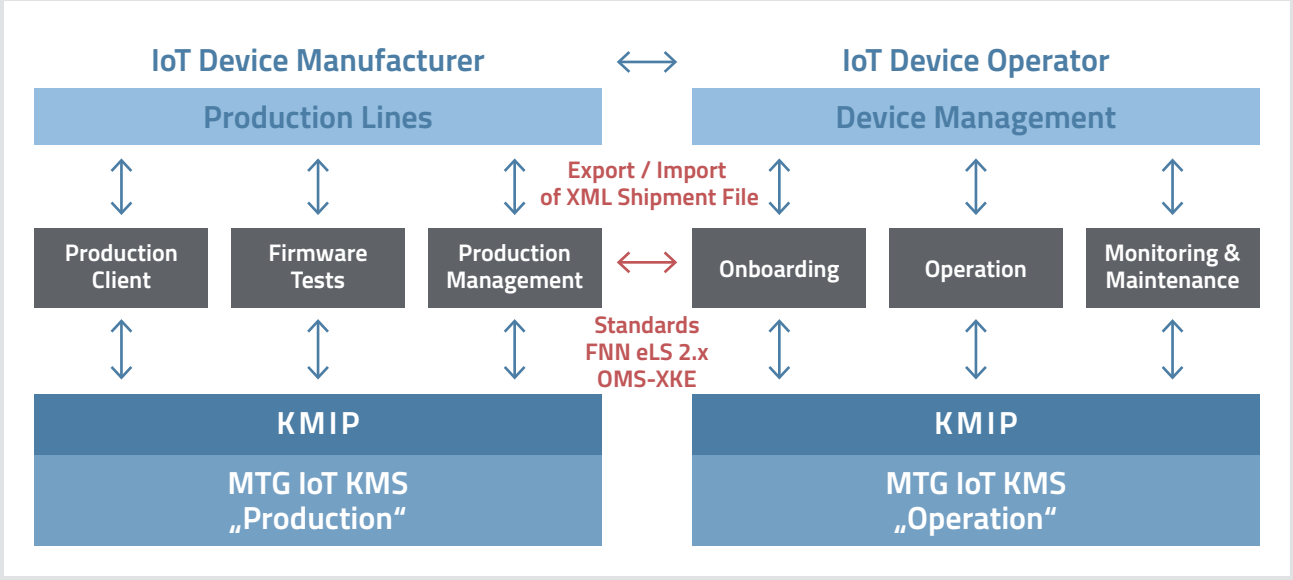
Foto: © Louis Reed / unsplash.com

MTG IoT Key Management System

Cryptographic Key Management System for manufacturing and operation of IoT devices

The MTG Key Management System (MTG IoT KMS) was specially developed for manufacturers and operators of IoT devices, making the management of a large number of individual cryptographic keys in production and at the operator's site considerably easier.

As a centralized security system with an open interface according to the international OASIS KMIP standard, the MTG KMS enables all specific IoT applications to be connected quickly and easily.

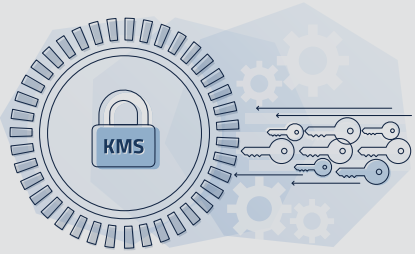


MTG KMS from IoT device production to operation

MTG IoT KMS

Functions & Benefits

MTG IoT KMS



Complete Key Management Life Cycle	▪ Complete set of operations which are needed to centrally manage cryptographic keys → create, maintain, protect, control key material
Additional Features (Control & Compliance)	▪ Support of complex rights & role concepts ▪ Logging / auditing ▪ Remote control & monitoring ▪ Access to central key material from different applications possible ▪ HSM Management
Industry Specific Modules	▪ KMIP standard Interface ▪ REST Interface for legacy applications ▪ Additional modules for IoT production ▪ Implementation of industry-specific standards (e.g. OMS for Smart Meters) ▪ Customized plug-ins & components
HSM Integration	▪ Secure storage of keys in HSM ▪ HSM models from different vendors available ▪ HSM consulting services
PKI	▪ A central Key Lifecycle Management with optional connection to PKI ▪ Corporate MTG PKI available

Easy Integration

Complete key management life cycle
The entire key management lifecycle is already supported in the MTG KMS and can be utilized via the standardized KMIP interface.

Control & Compliance
The platform supports multiple independent clients. MTG´s dedicated role and rights management ensures the correct distribution of access rights of clients to the respective keys.

KMIP Interface
The KMIP interface enables the smooth and easy integration of existing applications. KMIP specifies all management operations for objects (e.g. digital certificates, private keys) that are stored and managed by a key management system. The KMIP standard includes operations for symmetric and asymmetric cryptographic keys, digital certificates and templates that simplify the creation of objects and control of their use.

KMIP Client Library
A specific and adaptable MTG exclusive KMIP-Library is available to facilitate the integration of applications.

REST Interface & Adapters
In case the KMIP protocol does not offer the necessary functionality (e.g. bulk jobs, legacy applications ...), a REST interface can be used to support a variety of clients and applications. Customized adapters or adapters to other widely adopted industry interfaces, like PKCS#11 or JCA/JCE, further ease the integration of applications.

Vendor independent HSM
MTG IoT KMS supports different Hardware Security Modules (HSM) vendors for the secure storage and generation of high-quality encryption keys.

PKI Integration
A Public Key Infrastructure (PKI) can be easily integrated to the MTG KMS. Besides this, a specific IoT PKI is available at MTG.

Consulting & Support
In cooperation with our customers, MTG develops a detailed specification that takes into account the project´s individual requirements. Affected departments (e.g. the production team) are fully involved and interfaces are coordinated.

Tasks and Use-Cases

Versatile and flexible use

Key injection of IoT devices during production
The creation and injection of one or more specific keys, during production is an important process for more device safety. This ensures confidentiality, integrity and authentication of million individual keys of produced IoT devices.

Customized production
For a manufacturer a customer-specific production of the key material is essential and can be controlled with the MTG IoT KMS.

Separate key management of production processes
MTG IoT KMS allows individual roles and access rights to be set up for the different production lines or products, each with its keys handled separately.

IoT device operation
For secure device management, various client applications are able to continuously access the key material managed centrally in the MTG IoT KMS throughout the entire device lifecycle:

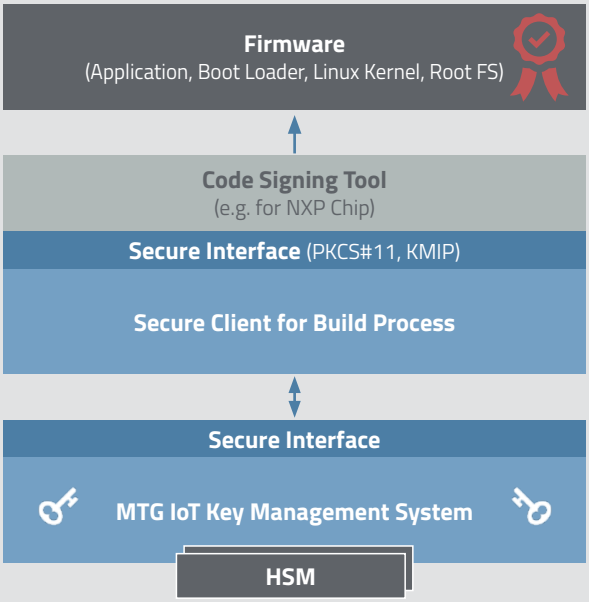
> Onboarding: device storage, registration, workforce management
> Operation: data processing & control of devices
> Monitoring & Maintenance: device updates, status, configuration

Multi-vendor support
The MTG IoT KMS can support different manufacturers and products in the management of the devices in operation.

Task specific key material
On production and operation side, keys are marked according to their function or tasks (administration, testing, updating, workforce management ...) to be used by the authorized applications / users only.

Replacement of the key material in the device
MTG IoT KMS allows to exchange key material in the devices. For example, before the validity of keys expires or broken algorithms.

MTG Secure Boot Protector for Embedded Systems
Manufacturers of embedded systems should ensure that their devices only start with original and unmodified firmware and that only authorized configuration files and updates can be used. MTG Secure Boot Protector is responsible for all crypto operations (encryption, signing, key generation ...), which are needed for secure boot, configuration and update of embedded systems. All required symmetric and asymmetric keys are securely saved in the MTG IoT Key Management System respectively HSM.



Secure life cycle management of digital certificates & secret keys needed for the secure boot management process

Secure electronic shipment files
A secure handover of the key material when sending the physical devices to the customer or between production sites has to be ensured with an electronic shipment file. For the en- and decryption of an electronic shipment file we offer all necessary „crypto key functionalities".

MTG ERS – Enterprise Resource Security

The ERP System for IT Security!

MTG ERS® – Indispensable for Security Conscious Companies

MTG ERS® unlocks the full potential of secure digitization across industries and processes. Based on verified identities, trusted communication and centralized storage of encrypted data become possible.

The product range of MTG ERS® consists of several aligned elements:

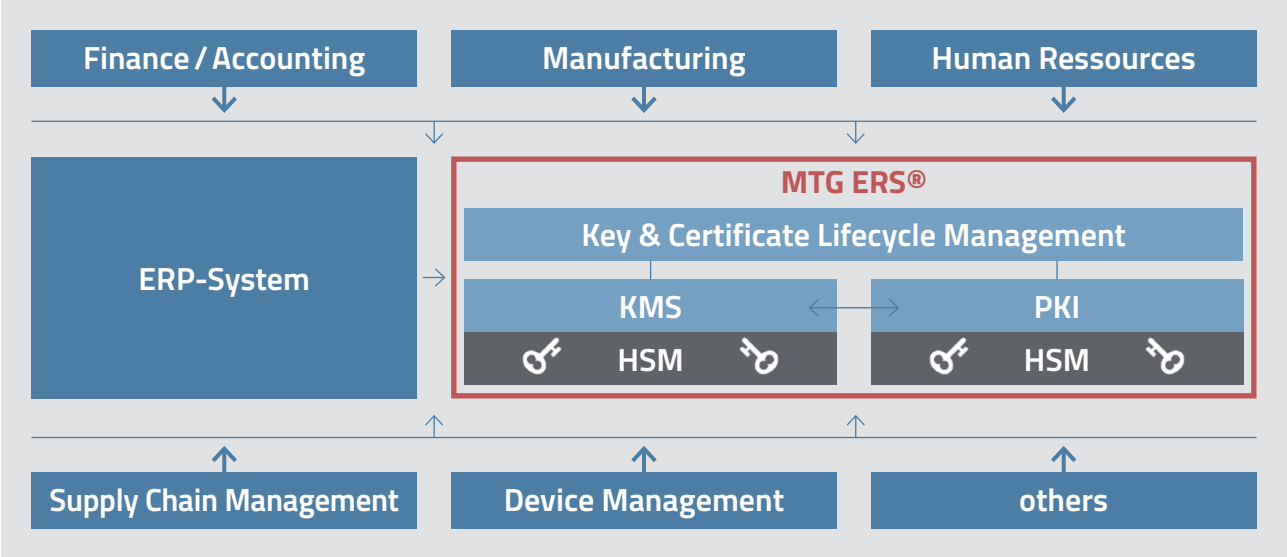
> MTG Certificate Lifecycle Manager

> MTG PKI Platform / Certificate Authority (CARA)

> MTG Key Management System

> Appropriate Hardware Security Modules for specific use cases

MTG ERS® simplifies and centralizes the management of cryptographic keys and identities in enterprises and public institutions. MTG ERS® allows industry-specific implementation and easy integration of a complete key management lifecycle in selected enterprise processes.



MTG offers a single-sourced ERS solution for managing the entire corporate IT Security Life Cycle with direct access to MTG-expertise

MTG AG is a leading specialist for sophisticated encryption technologies "Made in Germany". We simplify and centralize the management of cryptographic keys and identities throughout the complete key management lifecycle.

MTG AG · Dolivostrasse 11 · 64293 Darmstadt · Germany
Tel +49 6151 8000-0 · contact@mtg.de

mtg.de