MTG

IT Security for Critical Infrastructures
Security Made in Germany

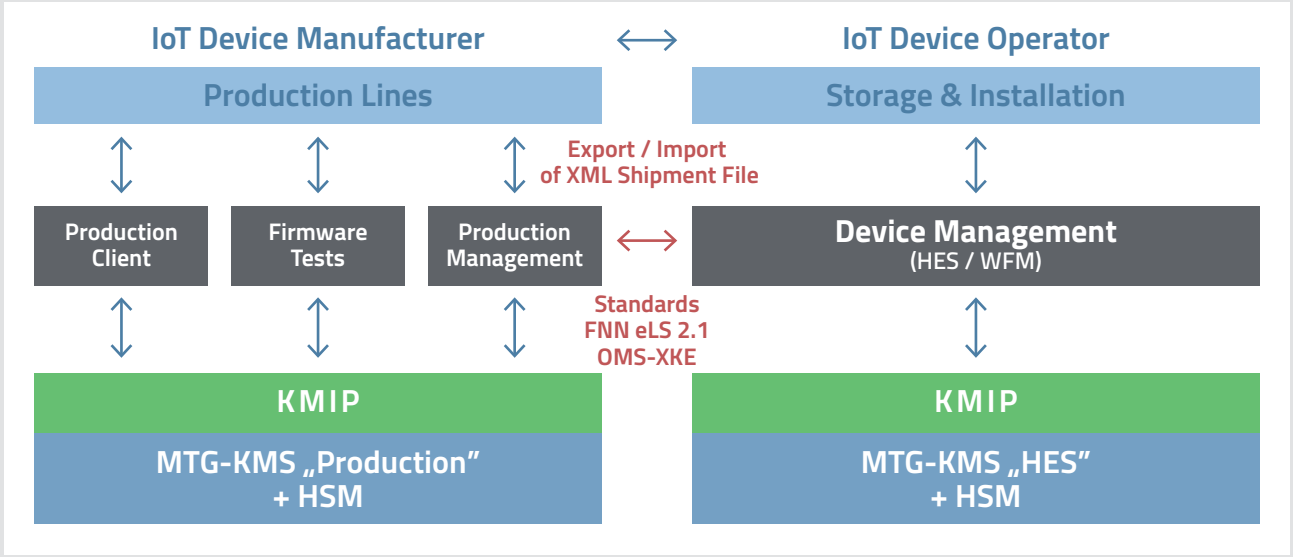
Illustration:
A. Limbach/ © fotolia.com

MTG Key Management System

High-performance management of device-specific keys via a central security system

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

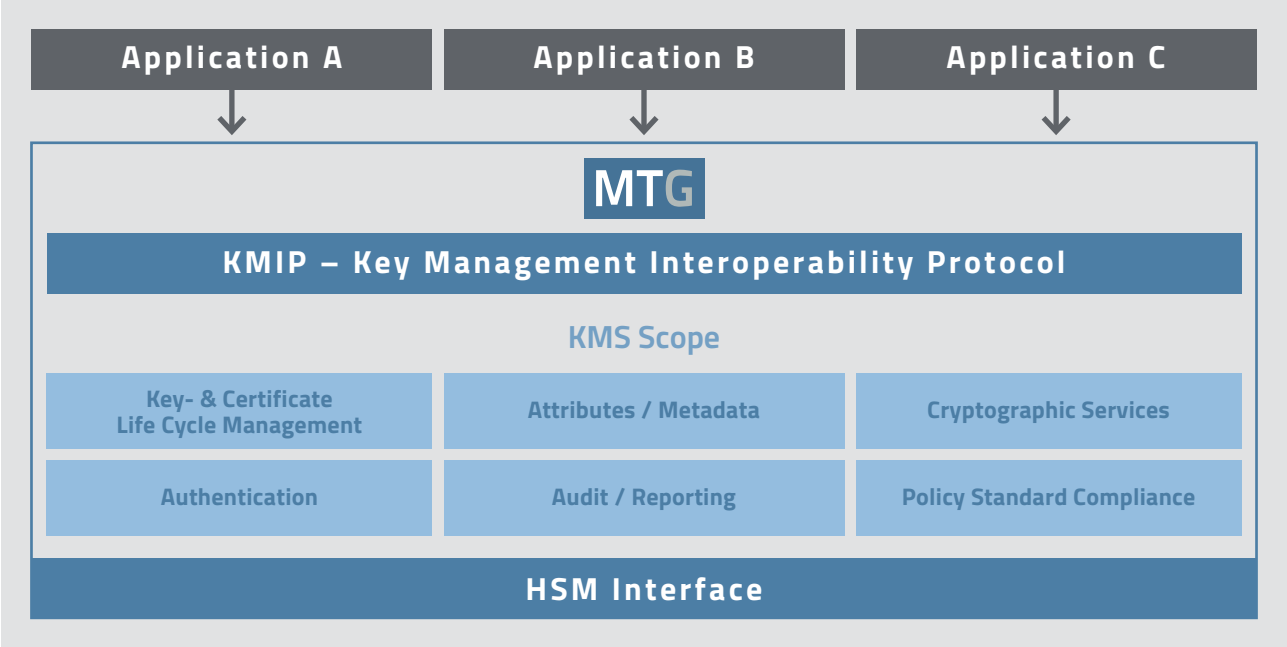
As a centralized security system with an open interface according to the international OASIS KMIP standard, the MTG KMS enables all specific applications of manufacturers to be connected quickly and easily.



MTG KMS from IoT device production to operation

MTG Key Management System (MTG KMS)

Functions & Benefits



MTG KMS already supports all cryptographic functions defined in the KMIP standard

MTG Key Management System (key- and certificate management)

In the future, every IoT device will have to be assigned one or more individual keys in order to meet the growing security and data protection requirements. Instead of managing a few keys for many devices, a large number of individual keys now have to be generated, assigned to individual devices, and managed. This poses new challenges for IoT device manufacturers and their customers.

The MTG KMS Server enables different applications in production and operation to access a detached, central security module that can perform all necessary crypto operations. The platform supports multiple independent clients and features granular rights management to ensure that access rights are distributed correctly to the respective keys.

For the secure storage of encryption keys and crypto operations, it is also possible to connect the MTG KMS to hardware security modules (HSM). To support a significant number of certificates, an external public key infrastructure (PKI) can be easily connected to the MTG KMS. In addition, communication via TLS/DLMS is available as an optional component.

IoT device manufacturers who process personal or sensitive data will need effective key management in the future.

MTG Key Management System (MTG KMS)

Functions & Benefits

Future-proof and flexible

A central key management system relieves applications from complex security tasks, standardizes security processes and thus reduces costs. The MTG KMS enables manufacturers and users to comply with company-wide security policies and quickly identify potential security threats, e.g. whether key material is cryptographically obsolete.

MTG KMS users are prepared for future developments. Already today, the entire life cycle of keys in the MTG KMS is supported and can be used via the standardized KMIP interface. The encryption and cryptography procedures used are constantly being developed and updated.

Electronic Shipment Files (FNN eLS 2.1 / OMS-XKE)

We offer all necessary „crypto functionalities" for the encryption and decryption of electronic shipment files. The application for the electronic delivery note can be connected quickly and easily to fulfill all encryption tasks. For the eLS, we rely on common standards such as OMS-XKE (OMS XML key exchange of the Open Metering System Group) and FNN eLS 2.1 (Germany). Thanks to the key transfer via standardized interfaces, manufacturers or their customers always have the option to use a non-MTG KMS.

Secure management of individual keys

The MTG KMS makes it possible to manage millions of individual device keys efficiently and centrally. The importance and relevance of managing individual keys in practice becomes evident in light of the increasing number of so-called botnets, which take advantage of weak or even identical serial keys to paralyze entire IoT networks.

Cost-effective mini HSM: MTG smartHSM

The smartHSM ensures that high-quality key material is generated during key generation. The MTG KMS also uses the HSM to protect the sensitive key material from external access. The HSM used here is particularly secure because it has been certified according to Common Criteria EAL 4+. In addition, the legal requirements as per BSI-CC-PP-0095-2017 (protection for a mini HSM), BSI TR-03109 and CP Smart Metering PKI are fulfilled. MTG KMS is compatible with HSM from UTIMACO and SafeNet Luna. Other HSM manufacturers can be connected on request.

A standard encryption method for electronic shipment files enables a standardized transfer of key material.

MTG Key Management System (MTG KMS)

KMIP Standard

KMIP – OASIS Key Management Interoperability Protocol

The OASIS Standard Key Management Interoperability Protocol (KMIP) was developed as an interoperable protocol that defines the standard communication between key management servers and clients. 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 their use.

Scope of KMIP Operations

Supported KMIP Operations

- Activate
- Add Attribute
- Archive
- Cancel
- Certify
- Check
- Create
- Create Key Pair
- Create Split Key
- Decrypt
- Delete Attribute
- Derive Key
- Destroy
- Discover Versions
- Encrypt
- Get
- Get Attribute List
- Get Attributes
- Get Usage Allocation
- Hash
- Join Split Key
- Locate
- MAC
- MAC Verify
- Modify Attribute
- Notify
- Obtain Lease
- Poll
- Put
- Register
- Register Query
- Re-certify
- Recover
- Re-key
- Re-key Key Pair
- Revoke
- RNG Retrieve
- RNG Seed
- Sign
- Signature Verify
- Validate

KMIP Object Types

- Certificate
- Opaque Object
- PGP Key
- Private Key
- Public Key
- Secret Key
- Split Key
- Symmetric Key
- Template

Encodings

- TTLV
- HTTPS/TTLV
- HTTPS/JSON
- HTTPS/XML

Interoperability is ensured by the KMIP interface. Production and device management applications can be integrated quickly and easily into the MTG KMS.

MTG is a leading specialist for sophisticated encryption technologies in Germany. Our innovative IT security solutions effectively secure critical infrastructures and the Internet of Things.

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

mtg.de