MTG

IT Security for Critical Infrastructures
Security Made in Germany

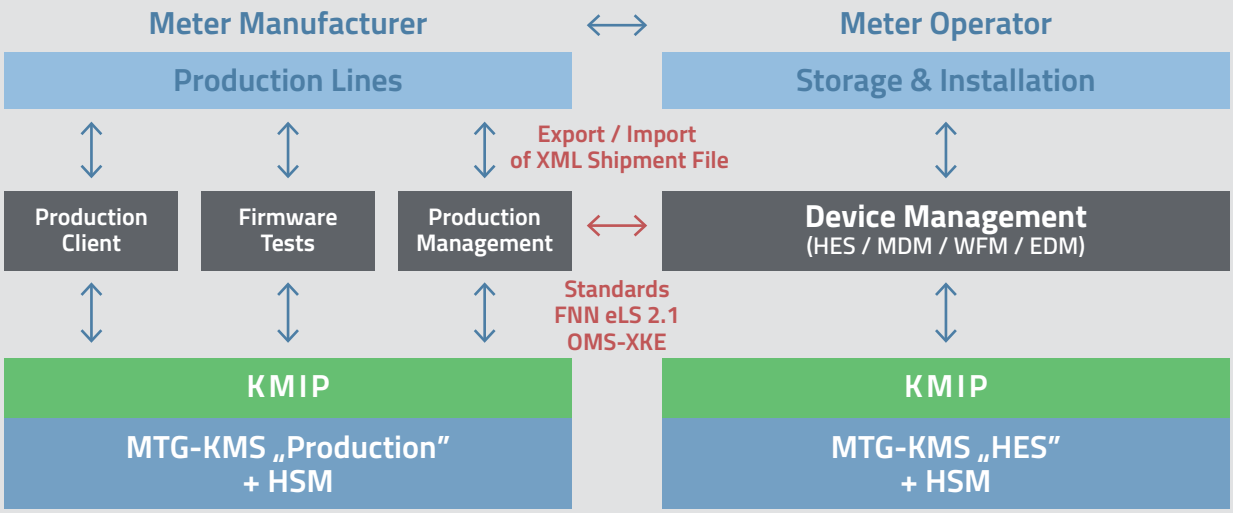
Illustration: A. Limbach/ © fotolia.com

MTG Key Management System

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

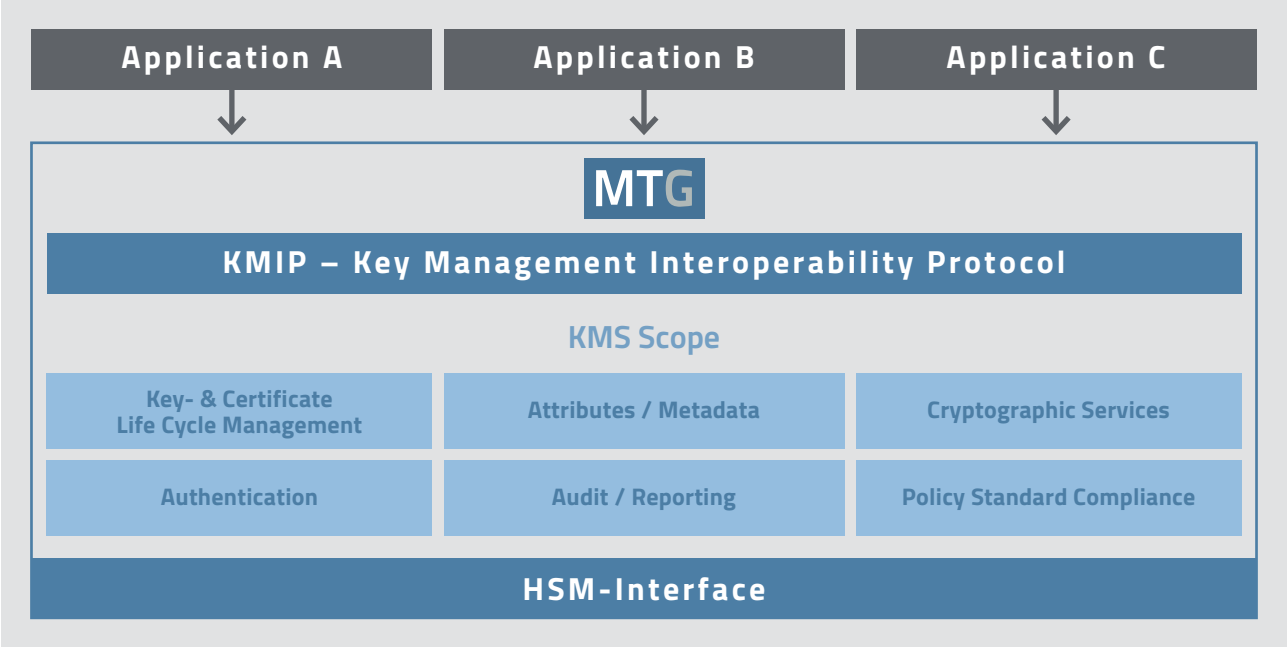
MTG has developed a key management system (MTG-KMS) specifically tailored to the requirements of the smart metering market. This can be used by manufacturers in production as well as by energy suppliers for device management.

The MTG-KMS is a centralized security system with an open interface according to the international OASIS KMIP standard. All specific applications on the manufacturer side or at the utility company can be connected quickly and easily.



MTG-KMS from device production to operation

Functions & Benefits



MTG-KMS already supports all cryptographic functions from the KMIP standard

MTG Key Management System (Key- and Certificate Management)

The European General Data Protection Regulation (GDPR) demands the pseudonymisation and encryption of personal data. Violations are subject to high penalties. In order to meet the high requirements, all manufacturers of intelligent measuring devices will need a KMS in the future. These include, for example, smart meter manufacturers as well as manufacturers of heating cost meters, water meters and all other intelligent measuring devices that process personal or sensitive data.

Without a central KMS, the level of complexity for key management increases. If each supplier of an application supplies its own key management, it must also be maintained individually.

Smart meter manufacturer, manufacturer of heat meters, Heating cost meters, water meters and all other intelligent measuring devices that 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 the application 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. if 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 further developed and updated.

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

For the en- and decryption of an electronic shipment file we offer all necessary „crypto functionalities". 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, it is always possible to work with a non-MTG KMS on the side of the manufacturer or energy supplier.

Secure management of individual keys

In the future, each intelligent IoT device will receive one or more individual keys. The MTG-KMS enables to manage millions of individual device keys efficiently and centrally. The importance and relevance of managing individual keys in practice is well represented by the increasing numer of so-called botnets. These take benefit 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 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 BSI-CC-PP-0095-2017 (protection profile 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 the electronic shipment file enables the standardized transfer of the key material.

MTG Key Management System (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

- Archivate
- 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. Applications for production or device management can be quickly and easily integrated into the MTG-KMS.

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

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

mtg.de