MTG

IT Security for Critical Infrastructures
Security Made in Germany

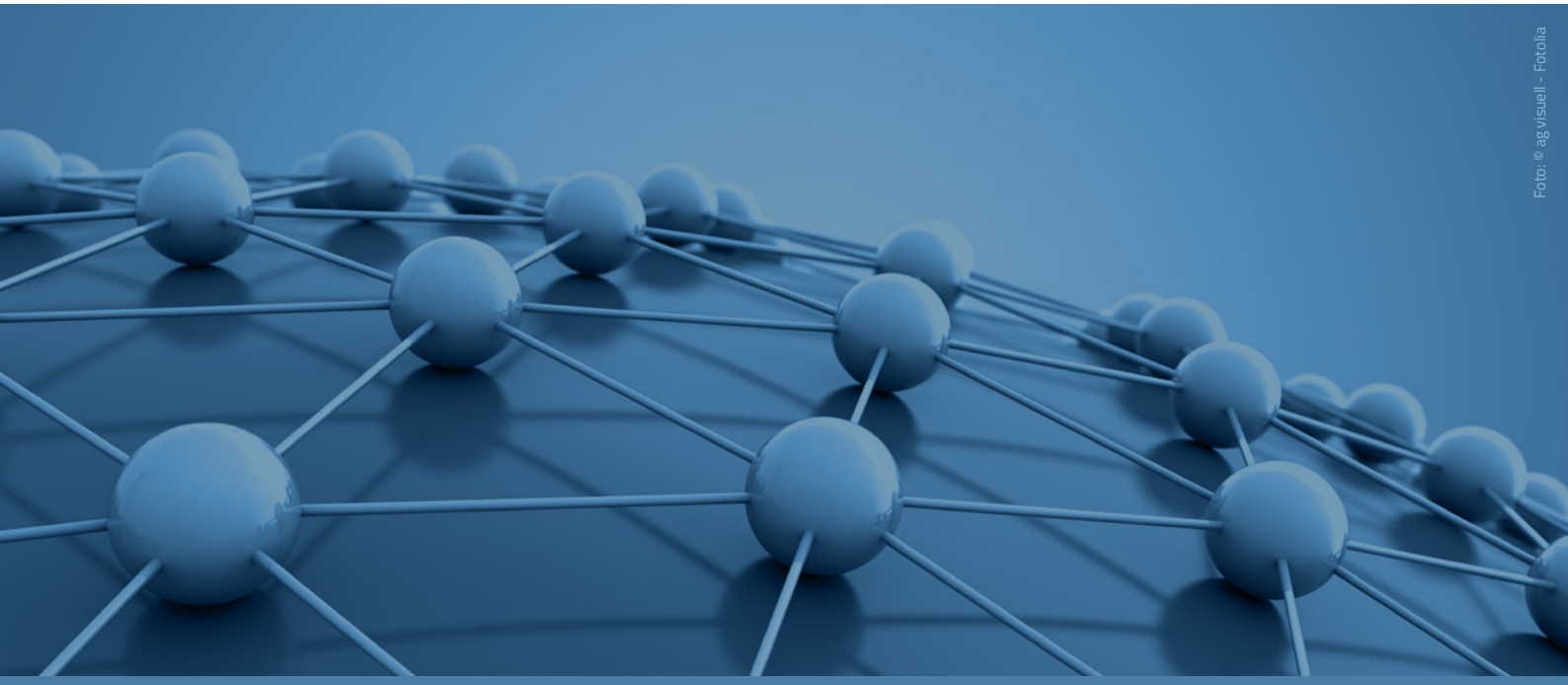


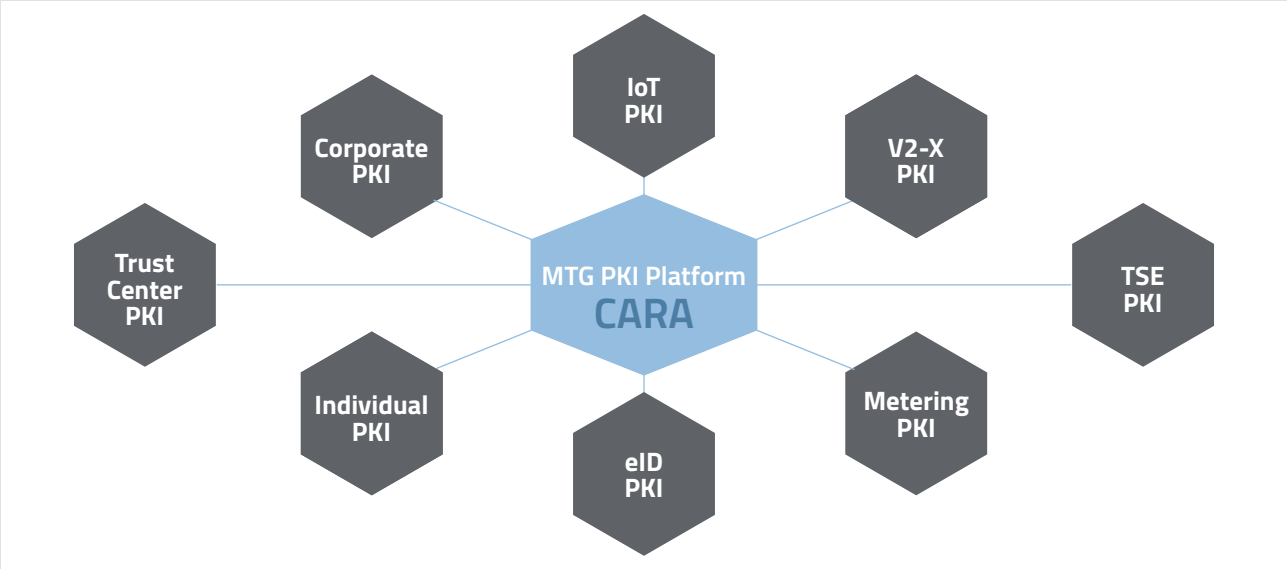
Foto: © ag visuell - Fotolia

MTG PKI Platform CARA

Industry-specific Public Key Infrastructure solutions for the generation, use and administration of digital certificates

A Public Key Infrastructure (PKI) is required for the creation, use and management of certificates. MTG CARA is a is a flexible and configurable, multitenant Certification Authority (CA) and Registration Authority (RA) system for a certificate-based and thus highly secure and confidential communication via the Internet.

Based on this PKI platform, different CA solutions are offered according to specific industry and customer requirements.



Industry-specific Public Key Infrastructure solutions based on MTG PKI Platform CARA

Corporate PKI

An enterprise PKI is a centralized service within an organization that provides strong cryptographic protection for the following use cases:

> **Enterprise identity management**
Authentication, authorization and access control of employees using personalized and centrally managed login credentials

> **Enterprise-wide email protection**
End-to-end encryption and authentication through digital signatures

> **Authentication of enterprise hardware**
Protection against serious attacks against unauthenticated malicious or infected devices on the corporate network (web servers, network routers, network switches, network printers etc.)

> **Authentication of mobile devices**
Smartphones

> **Seamless integration with a corporate Microsoft Windows infrastructure**
Automatic management of certificates (Cooperation with Secardeo company)

Industry-specific PKIs

Certificate-based solutions can be used in a variety of ways. Thanks to the modular design, the MTG PKI can be easily adapted and cost-effectively used in a wide range of industries.

MTG Metering PKI
The MTG Metering-CA is a PKI system for creating and managing certificates for the Smart Meter Rollout in Germany. The technical requirements from BSI TR-03109-04, BSI TR-3145 as well as the certificate policy of the Smart Metering PKI are completely fulfilled. The MTG Metering CA is used by SMGW manufacturers, Smart Meter Gateway administrators and in market communication.

MTG TSE PKI
MTG offers retail chains and cloud service providers a TSE PKI for the legally compliant operation of a CTSS/TSE (Certified Technical Security System) for cash register systems. The required CTSS certificates are provided by the MTG TSE PKI, which also fulfils the requirements according to BSI TR-03145. The MTG TSE PKI can also be operated as an on-premise solution in your own certified computer center or at one of our partners and supports both local TSEs and so-called cloud TSEs.

MTG IoT PKI
In the Internet of Things, a large number of devices communicate with each other in network infrastructures. In order to protect these systems, no device may have access unless it has proven that it is trustworthy. The secure identification and authentication is guaranteed by the use of digital certificates supplied and managed by the MTG IoT PKI.

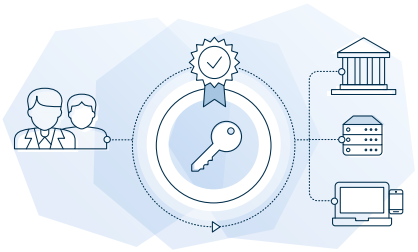
MTG V2-X PKI
Autonomous driving requires a networked communication between vehicles. To ensure that the traffic infrastructure can be used safely and smoothly, safe and secure communication between autonomous vehicles and traffic control systems is absolutely essential. The interaction between vehicles among each other and with the control systems is called V2X (Vehicle-to-X). A V2X-CA is indispensable for securing the communication.

MTG eID PKI
MTG eiD CA can be used worldwide as a Country Verifying Certification Authority (CVCA) and Country Signing Certification Authority (CSCA) for Machine Readable Travel Documents (MRTD), identity cards and electronic residence permits and is ideally suited for use as a Document Verifying Certification Authority (DVCA) and SPOC (Single Point of Contact).

MTG PKI

Features, Add-ons & Post-Quantum Certifcates

Features



Standardised & Modular Design	▪ Certificate formats: X.509, CVC (Card Verifiable Certificates), AC (attribute certificates) ▪ Certificate types: CA, mail, SSL, router, etc. ▪ Support of common interfaces (CMP, SCEP, REST, ACME ...) ▪ Portability through Java and web technologies
Special Rights & Role Concept	▪ Separation of roles and rights (e.g. acc. to BSI TR-03145) ▪ Specialised rights and roles concept to map your organisational structure ▪ Support of different Registration Authority (RA) processes
Multitenant Capability	▪ Multi-tenant capability through virtual CAs ▪ Virtual CAs for different tasks ▪ Management of large volumes of certificates by the domain concept
Central operation	▪ Central administration and centralised logging ▪ XML export for CRM, billing, statistics etc. ▪ Scalable from a single-server solution up to the operation of a Trust Center
Individual Features & Add-ons	▪ Highly customizable to customer layout/design and processes ▪ Activation of various HSMs (smart card, smartHSM, network-HSM) ▪ Customisable workflows ▪ Central key storage in CA

Add Ons

Easy Integration
Our MTG PKI platform supports standardized interfaces such as REST, ACME, CMP, SCEP, EST, LDAP and OCSP. Security functions can thus be flexibly and seamlessly integrated into corporate or governmental processes to achieve automation and increased efficiency of business processes.

MTG Smart Bridge
Card personalization for different card types (e.g. TCOS, CardOS, StarCos) via web application or stand-alone application. In addition to certificate management features, PDF signatures (QES) can also be created. It supports smartcard-based web login without PKCS#11 module in browser. No JRE installation is required on the client system. It is available for Windows, Linux and Macintosh for all common browser types.

MTG OCSP Revocation-Info Server
The MTG Revocation-Info Server provides certificate users with up-to-date revocation information. It acts as an OCSP responder and a revocation list distribution point. The OCSP Responder works according to RFC 6960 and RFC 6961.

LDAP / LDAPS Integration
MTG CARA can easily use existing LDAP servers to store revocation lists and certificates according to different policies. It supports CRLs and Root, intermediate CA and end-user certificates.

Time Stamping
A time stamping server according RFC 3161 is available.

HSM Support
Utimaco, Thales Luna, SmartHSM are already integrated. Other HSMs can be integrated on request.

Post-Quantum Certificates

The protection of your data against future decryption with quantum computers is already possible with our MTG PKI platform. A seamless integration of PQC Algorithms is available on request. Until standardization of PQC schemes, we rely on highly secure, hash-based algorithms like XMSS and SPHINCS+ and code-based algorithms like Classic McEliece for asymmetric public key encryption and key exchange.

Register now

for a cost-free demo use case for the creation of conventional or PQC Certificates.

https://pqc-pki.mtg.de

MTG ERS – Enterprise Resource Security

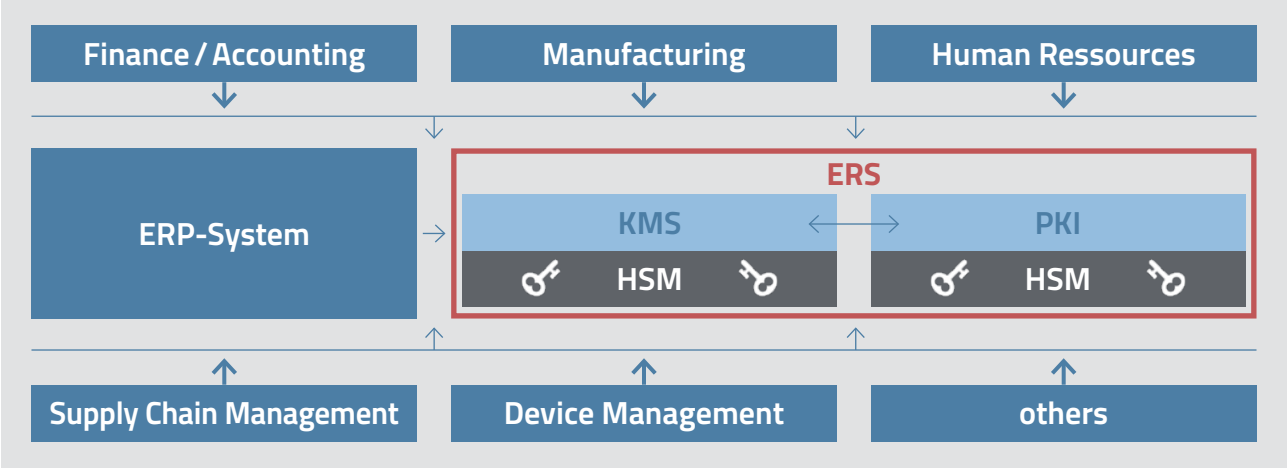
The triple set of essential security elements

IT Security protection – an ongoing task with increasing complexity!

The management of cost-effective security processes needs a clear and effective infrastructure. Organizational guidelines with dedicated rights and role management are mandatory. If every department manages its own security processes, the complexity and handling costs will go up dramatically with the growing number of keys and certificates being used in various cases.

Therefore, it is essential that organizations have an central overview how keys and certificates are used on their network at any point in time. They need to know who has access to them and need to control how and when they are used.

Indispensable for security conscious companies
Our offer consists of the triple set of essential security elements: **Key Management System (KMS), Public Key Infrastructure (PKI)** and the appropriate **Hardware Security Modules.** MTG´s holistic consulting approach covers all three product areas. Customized adaptations for easy integration and seamless operation enable our customers to meet the highest security standards within shortest time.



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

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

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

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

mtg.de