MTG

IT-Sicherheit für kritische Infrastrukturen
Security Made in Germany

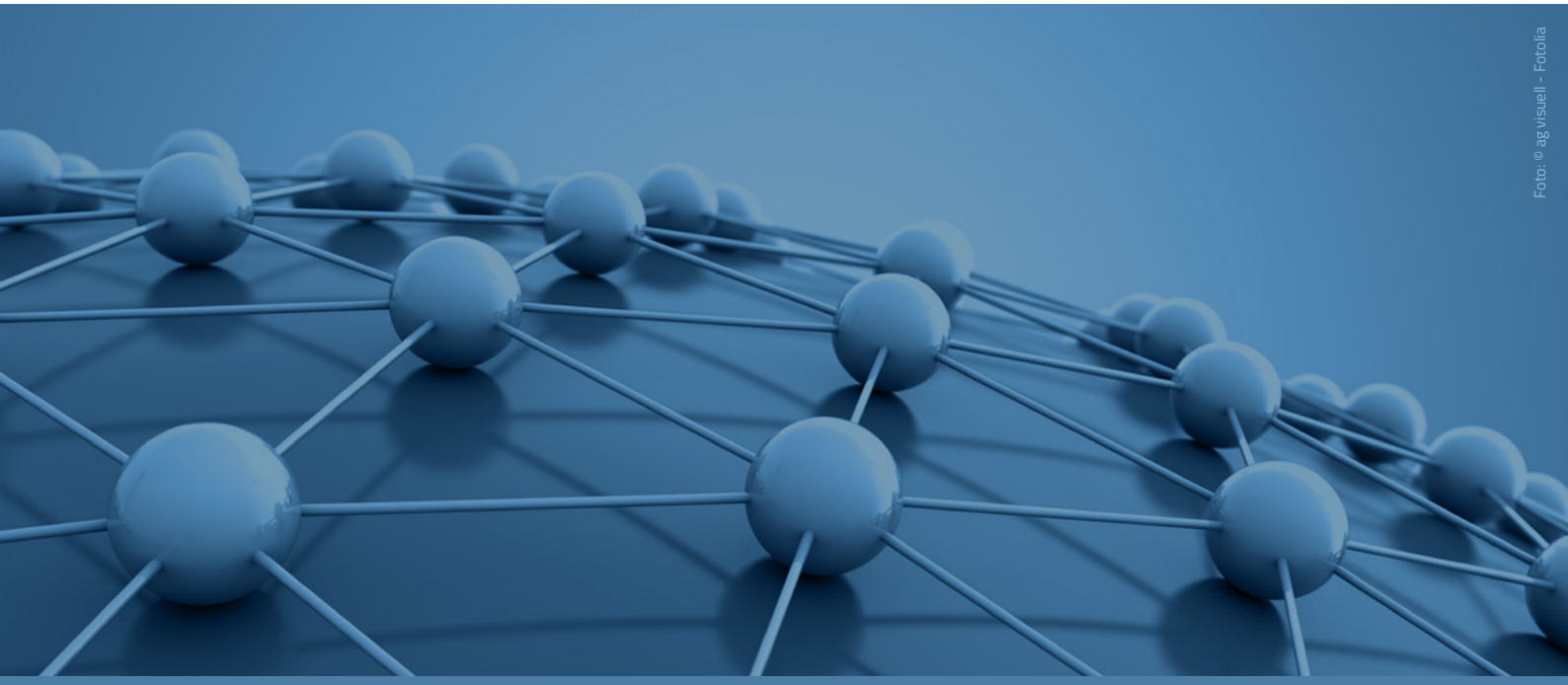


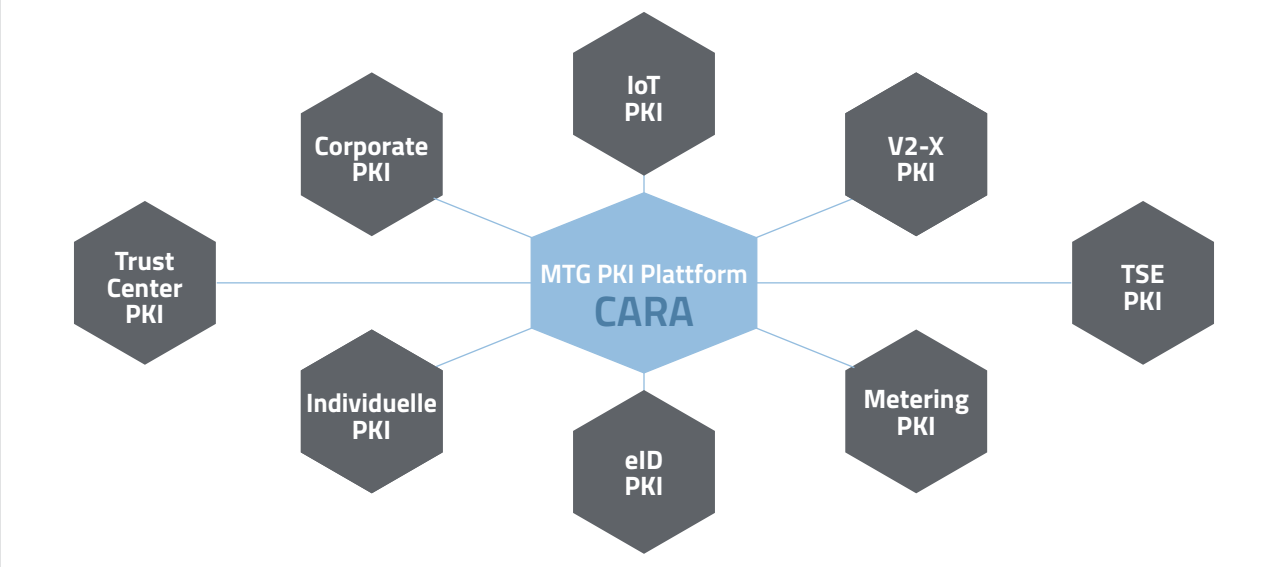
Foto: © ag visuell - Fotolia

MTG PKI Plattform CARA

Branchenspezifische Public Key Infrastructure (PKI) Lösungen zur Erzeugung, Nutzung und Verwaltung digitaler Zertifikate

Zur Erzeugung, Nutzung, Sperrung und Verwaltung von digitalen Zertifikaten ist eine Public Key-Infrastruktur (PKI) erforderlich. MTG CARA ist ein flexibel konfigurierbares, mandantenfähiges Certification Authority (CA) und Registration Authority (RA) System für eine zertifikatsbasierte und damit besonders sichere Authentifizierung und Kommunikation im Internet.

Auf Basis dieser PKI-Plattform werden unterschiedliche CA-Systeme nach spezifischen Branchen- und Kundenanforderungen angeboten.



Branchenspezifische Public Key Infrastructure Lösungen basierend auf der MTG PKI Plattform CARA

Corporate PKI

Eine Unternehmens-PKI ist ein zentralisierter Dienst innerhalb eines Unternehmens, der starken kryptographischen Schutz für die folgenden Anwendungsfälle bietet:

> **Unternehmensweites Identitätsmanagement**
Authentifizierung, Autorisierung und Zugangskontrolle von Mitarbeitern unter Verwendung personalisierter und zentral verwalteter Zugangsdaten

> **Unternehmensweiter E-Mail-Schutz**
Ende-zu-Ende-Verschlüsselung und Authentifizierung durch digitale Signaturen

> **Authentifizierung von Unternehmens-Hardware**
Schutz vor schwerwiegenden Angriffen auf nicht authentifizierte bösartige oder infizierte Geräte im Unternehmensnetzwerk (Webserver, Netzwerk-Router, Netzwerk-Switches, Netzwerk-Drucker usw.)

> **Authentifizierung von mobilen Geräten**
(Smartphones)

> **Nahtlose Integration in eine unternehmenseigene Microsoft Windows-Infrastruktur**
Automatisches Management von Zertifikaten (Kooperation mit Firma Sacardeo)

Branchenspezifische PKIs

Zertifikatsbasierte Lösungen können vielfältig eingesetzt werden. Dank des modularen Designs kann die MTG PKI für die verschiedensten Branchen einfach angepasst und kostengünstig genutzt werden.

MTG eID PKI
MTG eiD CA kann weltweit als Country Verifying Certification Authority (CVCA) und Country Signing Certification Authority (CSCA) für Machine Readable Travel Documents (MRTD), Personalausweise und elektronische Aufenthaltstitel genutzt werden und ist für den Einsatz als Document Verifying Certification Authority (DVCA) und SPOC (Single Point of Contact) bestens geeignet. MTG eiD PKI wird in Deutschland als Root-CA für hoheitliche Dokumente eingesetzt.

MTG TSE PKI
Für den gesetzeskonformen Betrieb einer TSE (Technischen Sicherheitseinrichtung) für Kassensysteme bietet MTG Handelsketten und Cloud-Dienstleister eine TSE PKI an. Die erforderlichen TSE Zertifikate werden von der MTG TSE PKI bereitgestellt, welche auch die Anforderungen nach der BSI TR03145 erfüllt. Die MTG TSE PKI kann auch als On-Premise Lösung im eigenen zertifizierten Rechenzentrum oder bei einem unserer Partner betrieben werden und unterstützt sowohl lokale TSEs als auch sogenannte Cloud-TSEs.

MTG IoT PKI
Im Internet der Dinge kommunizieren unzählige Geräte in Netzinfrastrukturen miteinander. Um diese Systeme zu schützen, darf kein Gerät Zugriff haben, solange es nicht bewiesen hat, dass es vertrauenswürdig ist. Die sichere Identität eines Gerätes wird durch den jeweiligen Einsatz eines individuellen, eindeutigen und geheimen Schlüssels ermöglicht. Die MTG IoT PKI liefert die benötigten Zertifikate für asymmetrische Verschlüsselungsverfahren.

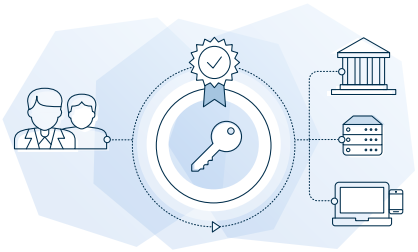
MTG V2-X PKI
Autonomes Fahren setzt die vernetzte Kommunikation zwischen Fahrzeugen voraus. Damit die Verkehrsinfrastruktur sicher und reibungslos genutzt werden kann, ist außerdem eine sichere und eindeutige Kommunikation zwischen autonomen Fahrzeugen und Verkehrssteuerungsanlagen zwingend notwendig. Das Zusammenspiel zwischen Fahrzeugen untereinander und mit den Steuerungsanlagen wird kurz als V2X (Vehicle-to-X) bezeichnet. Für die Absicherung der Kommunikation ist eine V2X-CA unerlässlich.

MTG Metering PKI
Die MTG Metering-CA ist ein PKI-System zur Erstellung und Verwaltung von Zertifikaten für den Smart Meter Roll-out in Deutschland. Die technischen Anforderungen aus der BSI TR-03109-04, BSI TR-3145 sowie der Certificate Policy der Smart Metering PKI werden hierbei vollumfänglich erfüllt. Die MTG Metering CA kommt bei SMGW-Herstellern, Smart Meter Gateway Administratoren und in der Marktkommunikation zum Einsatz.

MTG PKI

Features, Zusatzmodule & Post-Quantum-Zertifikate

Features



Standardisiertes und modulares Design	▪ Zertifikatsformate: X.509, CVC (Card Verifiable Certificates), AC (Attribut-Zertifikate) ▪ Zertifikatstypen: CA, Mail, SSL, Router, etc. ▪ Unterstützung von gängigen Schnittstellen (CMP, SCEP, REST, ACME ...) ▪ Portierbarkeit durch Java- und Web-Technologien
Spezielles Rollen- und Rechtekonzept	▪ Trennung von Rollen und Rechten (z. B. nach BSI TR-03145) ▪ Spezielles Rechte- und Rollenkonzept zur Abbildung Ihrer Organisationsstruktur ▪ Unterstützung unterschiedlicher Registration Authority (RA)-Prozesse
Mandanten-fähigkeit	▪ Mandantenfähigkeit durch virtuelle CAs ▪ Virtuelle CAs für unterschiedliche Aufgaben ▪ Verwaltung großer Mengen von Zertifikaten durch das Domänenkonzept
Zentraler Betrieb	▪ Zentrale Verwaltung und zentralisierte Protokollierung ▪ XML-Export für CRM, Abrechnung, Statistiken etc. ▪ Skalierbar von einer Single-Server-Lösung bis hin zum Betrieb eines Trust Centers
Individuelle Features und Zusatzmodule	▪ Hochgradig anpassbar an Kunden-Layout/Design und Prozesse ▪ Ansteuerung verschiedener HSMs (Chipkarte, smartHSM, Netzwerk-HSM) ▪ Individuell anpassbare Workflows ▪ Zentrale Schlüsselablage in CA

Zusatz-Module

Einfache Integration
Unsere MTG PKI Plattform unterstützt standardisierte Schnittstellen wie REST, ACME, CMP, SCEP, EST, LDAP und OCSP. Sicherheitsfunktionen lassen sich so flexibel und nahtlos in Unternehmens- oder Behördenabläufe integrieren, um die Automation und Effizienzsteigerung von Geschäftsprozessen zu erzielen.

MTG Smart Bridge
MTG SmartBridge ermöglicht die Kartenpersonalisierung für verschiedene Kartentypen (z. B. TCOS, CardOS, StarCos) mittels Web-Applikation oder Stand Alone Applikation. Neben Features zur Verwaltung der Zertifikate können auch QES-Signaturen für PDF-Dokumente erstellt werden. MTG SmartBridge setzt keine JRE-Installation auf dem Clientsystem voraus und ist für Windows und Linux für alle gängigen Browsertypen verfügbar.

MTG OCSP Revocation-Info Server
Der MTG Revocation-Info Server versorgt Zertifikatsnutzer mit aktuellen Sperrinformationen. Er fungiert als OCSP-Responder und als Verteilstelle für Sperrlisten. Der OCSP-Responder arbeitet nach RFC 6960 und RFC 6961.

LDAP / LDAPS Integration
MTG CARA kann problemlos vorhandene LDAP-Server nutzen, um Sperrlisten und Zertifikate nach verschiedenen Richtlinien zu speichern. Es unterstützt CRLs und Root-, Intermediate-CA- und Endbenutzer-Zertifikate.

Zeitstempelung
Ein Zeitstempelserver nach RFC 3161 ist verfügbar.

HSM Support
Utimaco, Thales Luna, SmartHSM sind bereits integriert. Andere HSMs können auf Anfrage integriert werden.

Post-Quantum Certificates

Mit unserem PQC-Portfolio können Ihre Daten bereits heute gegen eine spätere Entschlüsselung durch Quantencomputer geschützt werden. Eine nahtlose Integration von PQC Algorithmen ist auf Wunsch möglich. Bis zur Standardisierung von PQC-Verfahren setzen wir auf hochsichere, hash-basierte Algorithmen wie XMSS und SPHINCS+ sowie code-basierte Algorithmen wie Classic McEliece für asymmetrische Public-Key-Verschlüsselung und Schlüsselaustausch.

Jetzt registrieren!

Kostenloses Demo-Use Case
für die Erstellung von traditionellen
oder PQC-Zertifikaten

https://pqc-pki.mtg.de

MTG ERS – Enterprise Resource Security

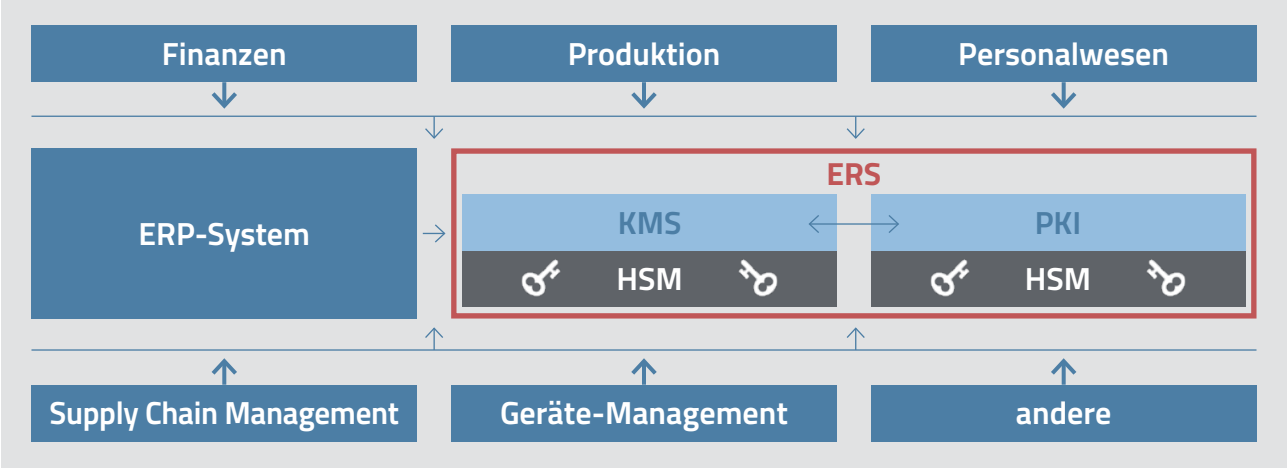
Dreiklang der IT-Security

IT-Sicherheit - eine fortwährende Aufgabe mit zunehmender Komplexität!

Das Management von kosteneffizienten Sicherheitsprozessen braucht eine klare und effektive Infrastruktur. Organisatorische Richtlinien mit dediziertem Rechte- und Rollenmanagement sind hierbei zwingend erforderlich. Wenn jede Abteilung ihre eigenen Sicherheitsprozesse verwaltet, steigen die Komplexität und die Kosten mit der wachsenden Anzahl von Schlüsseln und Zertifikaten, die in verschiedenen Fällen verwendet werden. Deshalb ist es wichtig, dass Organisationen einen zentralen Überblick haben, wie Schlüssel und Zertifikate in Ihrem Netzwerk zu jedem Zeitpunkt verwendet werden. Sie müssen wissen, wer Zugriff auf sie hat und wie und wann sie verwendet werden.

Unverzichtbar für sicherheitsbewusste Unternehmen

Unser Angebot besteht aus dem Dreiklang von wesentlichen Sicherheitselementen: **Key Management System (KMS), Public Key Infrastruktur (PKI)** und den entsprechenden **Hardware Sicherheitsmodulen**. Der ganzheitliche Beratungsansatz von MTG deckt alle drei Produktbereiche ab. Maßgeschneiderte Anpassungen für einfache Integration und reibungslosen Betrieb ermöglichen unseren Kunden die Umsetzung höchster Sicherheitsstandards innerhalb kürzester Zeit.



MTG bietet mit der ERS-Lösung die Verwaltung des kompletten IT-Sicherheits-Lebenszyklus mit dem nötigen Expertenwissen aus einer Hand!

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

TÜV SAARLAND ISO 27001

MTG AG ist ein führender Spezialist für anspruchsvolle Verschlüsselungstechnologien „Made in Germany". Unsere innovativen IT-Security Lösungen sichern kritische Infrastrukturen und das Internet der Dinge effektiv ab.

MTG

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

mtg.de