MTG **Enterprise Resource Security**
Mastering Cryptographic Key Lifecycles

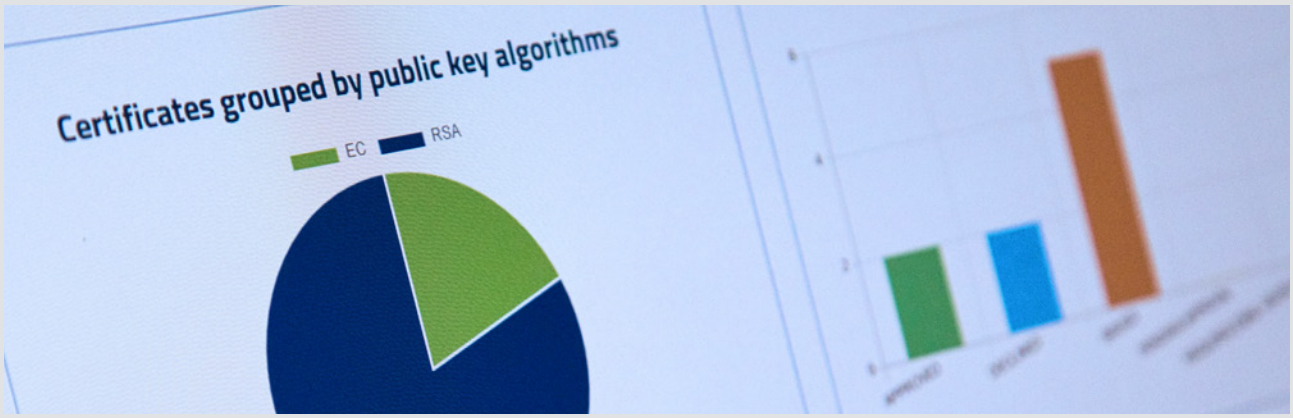
DARZ
Daten sind wertvoller als Geld


Foto: © DARZ

MTG Managed Corporate PKI

The Darmstadt-based infrastructure provider DARZ GmbH is now offering companies the opportunity to operate a dedicated corporate PKI as a managed service at a reasonable price. The underlying Corporate PKI with Certificate Lifecycle Management is provided by MTG.

MTG has developed a Corporate PKI that secures all company-relevant processes throughout the entire lifecycle of certificates. In cooperation with the long-term partner and infrastructure provider DARZ GmbH, a new managed service offering for PKI was created. Processes for issuing, renewing and revoking certificates can be centrally automated, managed and controlled for various use cases (e.g., e-mail certificates, router and server certificates or the secure connection of home office workstations ...). Certificate Lifecycle Management ensures that no certificates expire unintentionally and allows many associated processes to be automated.

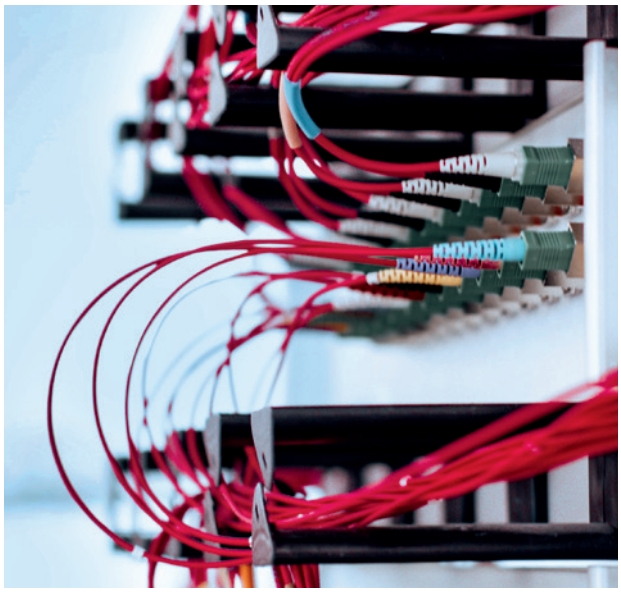


With a Managed PKI, companies are able to focus more quickly on securing their business processes and to use the ready-built PKI immediately.

MTG Managed Corporate PKI

Use Cases for Certificate Lifecycle Management

Fotos: © unsplash / a. distel, saffu, I. Kienle



Automation in Certificate Lifecycle Management

> Support for all major PKI interfaces like ACME, EST, CMP
> Support of ACME Certbot Client and other ACME clients
> REST API and REST CLM Client for automation of non-standard components
> Automatically renew and audit the installation of X.509 certificates
> Automated revocation service using OSCP and/or CRLs

Complete and Cost-effective Employee Onboarding

All required certificates can be issued in a systematic and complete procedure. A structured setup of authorizations ensures workflows in line with compliance guidelines.

> Automated device provisioning with User, VPN, SMIME and CA certificates
> Expiration notification and automated renewal
> Automated import of certificates into LDAP and Active Directory
> Map existing authorization structures and processes to certificate issuance (e. g., Active Directory roles)

Certificate Discovery

The Certificate Discovery function enables a systematic scanning for unknown certificates. Thanks to network-based sensors and agents all company public and private TLS/SSL certificates are identified and added to the certificate inventory. Dangerous outages due to expired certificates or expensive manual handling is consequently avoided.

Quick and Easy Provision of Digital Certificates for Networked Devices

> Support for all major network hardware manufacturers (Cisco, HP, Palo Alto, etc.)
  - Support of all SCEP and EST based devices
  - Other devices with individual clients possible
> Support for Active Directory managed devices

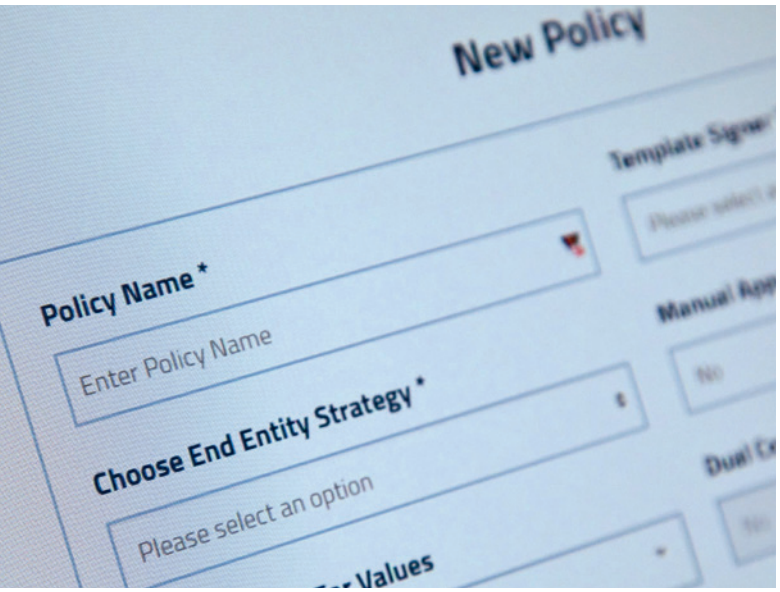
Automated Digital Certificate Provisioning for Servers

Automated seamless provisioning of digital certificates prevents server downtime and resulting costs and damages. It ensures the availability of internal services, production or the accessibility of corporate websites.

> Support for Windows and Linux Servers
> Provision of Active Directory managed servers
> Support for the ACME protocol
> Fully automated certificate renewal
> Additional flexibility and configurability thanks to CLI client

MTG Managed Corporate PKI

Features



» *Preconfigured policies are provided for common use cases!*

Detailed Monitoring & Reporting

Always track the status of your certificates and avoid surprises! MTG CLM provides a comprehensive notification system about certificate status changes. Users are informed in time and several times before certificates expire. Punctual and seamless renewal is thus ensured at any time.

> Extensive, user-friendly dashboards provide insights into the certificate state of each business domain and allow a quick overview at-a-glance.
> Advanced filtering and search functionality enables easy identification and presentation of results that can then be easily exported in CSV format for further processing.
> Audit metadata is tracked throughout all application steps and is readily available to MTG CLM administrators.

Access Control & Compliance

The role and rights management can be managed centrally and offers detailed options for the settings of certificates and certificate holders. Configuration options are possible on several levels (per user, realm & policy). Quick and easy provision of digital certificates for networked devices.

Create & Support Multiple Business Domains

The MTG CLM allows an individual organization of access rights for digital certificates.

> The respective areas (realms) can be structured according to departments, user groups or hierarchies
> It is also possible to differentiate between authorized users who can only view certificates and those who can configure them.
> Notification rules can be customized accordingly.
> The user interface adapts to the respective settings.

Certificate Policy Enforcement – Complete and Failure-free Generation of Certificates

The Policy Enforcement Form contains a comprehensive collection of rules that are required for the configuration of different certificates. This ensures that entries are complete, error-free, and compliant. Individual policies can be created for emails, servers, networked hardware or mobile devices.

> Limitation of the choice to only approved algorithms
> Permitted use of specific key material
> Setting of the validity of certificates
> Choice of manual or automatic approval of certificate requests
> Establishment of a 4-eyes principle

Central Identity Management with Keycloak

Keycloak allows to flexibly use different authentication protocols for all MTG ERS® applications (CLM, PKI, KMS) via a central sign-in and sign-out function.

MTG Managed Corporate PKI

Range of Services

New PKI Service Offer

The Managed Corporate PKI is operated in a geo-redundant and fail-safe manner in an ISO27001 and DIN EN50600 Cat III certified data center. Trusted authentication, verification, integrity and encryption for critical and sensitive corporate processes and applications are thus available at short notice. Companies can concentrate more quickly on securing their business processes and use the ready-built PKI immediately.

Services	Description
Setup Root CA	A dedicated Root CA is set up for each customer as a trust anchor for the entire company.
Setup Sub CA	The customer receives a Sub CA under this Root CA which he can operate to issue his use-case-specific certificates. Additional Sub CAs can be set up easily at customer request. This makes sense, for example, if different trust chains need to be defined for different areas of the company.
Private & public certificates	The Managed PKI allows cost-effective private certificates to be generated and managed for a wide range of use cases in the company. In addition, it is possible to use the Managed PKI to apply for public certificates directly from public CAs and to use them for further administration in the Managed PKI.
Hotline DARZ	Ticket system and hotline are available for questions and problems.
Operation and Managed Services	The Managed PKI is operated in an ISO27001 and DIN EN50600 Cat III certified data center in a geo-redundant and fail-safe mode. The managed service comprises: > Setup and configuration of the dedicated Root and Sub CAs, CLM, ACME EST, CMP servers and OCSP responders by experienced PKI experts in accordance with BSI crypto requirements TR-03116 > Connection to a HSM cluster > Security patch management of the underlying operating systems and databases > Maintenance of the PKI software > Monitoring the availability of the infrastructure and applications > Proactive monitoring of log files > Monitoring and renewal of the certificate validity periods of the Root CA and Sub CA > Backup and restore processes
Trainings	Detailed training videos are available online to familiarize users with the essential functions.
Consulting packages	Useful consulting packages facilitate the start of PKI operations and support the preparations as well as the implementation of specific use cases: e.g., consulting for the automation of processes, creation of a Certificate Policy and Certificate Practice Statement, design of certificate templates, set-up of a comprehensive reporting system, etc.
Professional Services	With a Professional Service Contract signed directly with MTG, users get full support from MTG's experienced PKI experts.

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