MTG IT Security for Critical Infrastructures
Security Made in Germany

MTG Post-Quantum Cryptography

MTG offers a comprehensive portfolio of state-of-the-art quantum-safe security products and services

The protection of your data against future decryption by quantum computers is already possible today with our PQC portfolio. To this end, we have developed a new generation of MTG products which allow the seamless integration of PQC algorithms.

MTG Portfolio
Post-Quantum Cryptography and Crypto-Agility

PQC PKI	PQC KMS	PQC HSM Integration	PQC Services	PQC Suite
Flexible, configurable, multi-tenant PQC-PKI CA system for generation and administration of certificates using traditional and post-quantum cryptography	Centralized Key Management System (KMS), highly available management and encryption of both traditional keys and PQC keys for various applications	Protection and usage of PQC keys for compliance with industry standards	Seamless integration of PQC into existing customer applications	Complete suite of crypto-agile applications (web server, browser, email, document signing and encryption) using hybrid PQC schemes

»

Anyone developing long-lived products or who is responsible for highly sensible data should start getting to grips with PQC today!

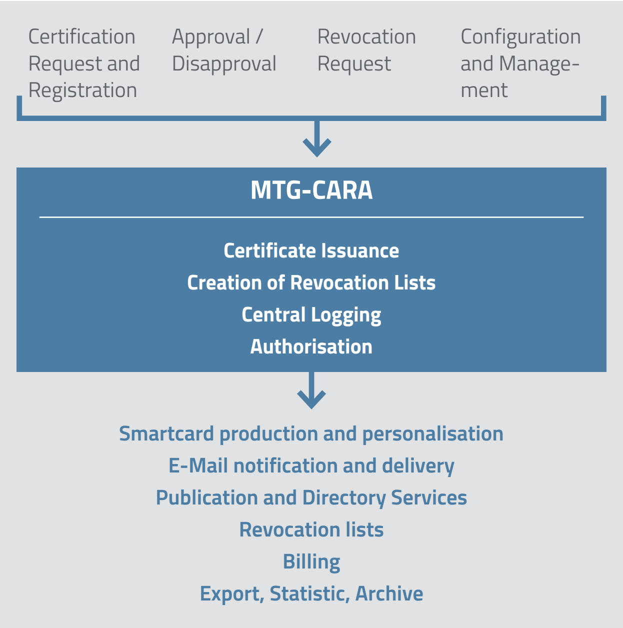
MTG Post-Quantum Cryptography (MTG PQC)

Protect current systems against future quantum computer threats

Public Key Infrastructure – PQC PKI

Use cases

- Corporate PKI
- General Purpose PKI
- Health/Insurance PKI
- Government PKI
- IoT PKI
- e-Energy PKI



Certification Request and Registration

Approval / Disapproval

Revocation Request

Configuration and Management

MTG-CARA

Certificate Issuance
Creation of Revocation Lists
Central Logging
Authorisation

Smartcard production and personalisation
E-Mail notification and delivery
Publication and Directory Services
Revocation lists
Billing
Export, Statistic, Archive

Short description & features

- MTG-CARA is a flexible, configurable, multi-tenant CA for the generation and administration of certificates using traditional and post-quantum cryptography (PQC)
- Certification and Registration Authority
- Supports standardized interfaces such as SOAP, SCEP, LDAP and OCSP
- Generation and management of X.509, AC, Card Verifiable (CV) certificates
- Modular design allows fast, low-cost customizing
- Special rights and roles concept to map individual organizational structure
- Support for software/chip card/network-HSM signing
- Scalable from a single-server solution up to the operation of a large scale CA

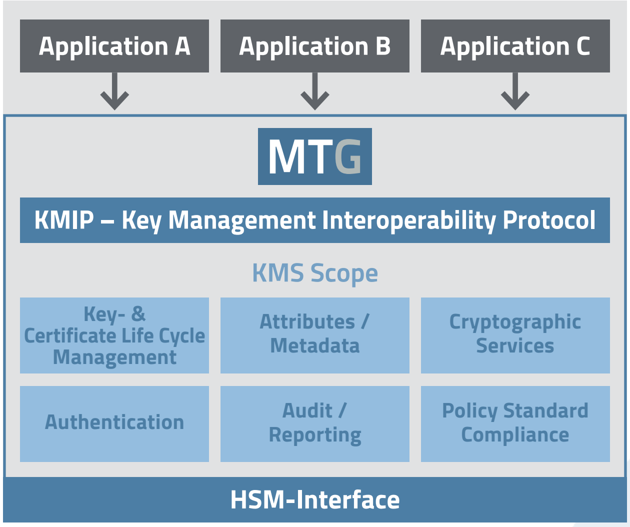
MTG Key Management System – PQC KMS

Use cases

- Production & operation of IoT Devices (e.g. Smart Meters)
- Central Management of ERP-systems

Short description & features

- Highly available management of traditional and PQC keys for various applications
- Detached, central security module, able to perform all necessary cryptographic operations
- Multi-tenant architecture
- Fine-granular rights management
- Management of the entire life cycle of keys
- Standardized KMIP interface v1.4
- HSM support for multiple vendors



Application A

Application B

Application C

MTG

KMIP – Key Management Interoperability Protocol

KMS Scope

Key- & Certificate Life Cycle Management	Attributes / Metadata	Cryptographic Services
Authentication	Audit / Reporting	Policy Standard Compliance

HSM-Interface

MTG Post-Quantum Cryptography (MTG PQC)

Protect current systems against future quantum computer threats

PQC HSM Integration

Use cases

- Strong protection and use of PQC keys is necessary
- Compliance with industry standards is mandatory
- A customised hardware solution is required to use proprietary formats or workflows, for example

Short description

- Integration of PQC algorithms in HSMs
- Extension Module can be added to already deployed HSMs
- Developed with UTIMACO SDK
- Extensive key management inside the HSM
- 2-factor authentication with smartcards
- “m out of n” authentication (e.g. 3 out of 5)
- Configurable role-based access control and separation of functions
- Multi-tenancy support
- Remote management
- Co-operation partner UTIMACO

utimaco® certified
Value Added Reseller

PQC Services

Use cases

- Migration of business applications, products, custom protocols to PQC
- Insight in dealing with large keys and signatures
- Efficient implementations of PQC algorithms
- Mitigation of risks in transition phase

Short description

- Seamless integration of PQC into existing customer applications and products by leading PQC experts
- In close cooperation with our customers, we integrate PQC into existing applications and protocols in joint projects
- Hardware and software optimisations
- Hybrid schemes which benefit from both universes: tried and tested crypto methods (such as RSA or ECC) combined with new quantum-safe methods

Photo by Mathew Schwartz on Unsplash

PQC Suite

Use cases

Where long term security is needed in:

- Web Server & Client
- Email Communication
- Document Signing
- Document Encryption

Examples:

- Registration Portals
- Credentials over the Web
- Transfer of personal data
- E-Banking
- Handling of confidential documents

Short description

- **PQC Web Server:** based on Apache Tomcat, offers all the features of a modern web server with integrated support for PQC TLS
- **PQC Web Browser:** based on Mozilla Firefox, offers all the features of a modern browser with integrated support for PQC TLS
- **PQC Email Client:** based on Mozilla Thunderbird, offers all the features of a modern email client with integrated support for PQC S/MIME
- **Document Signing:** Solution for generic document signing and encryption using state of the art PQC algorithms

MTG Post-Quantum Cryptography (MTG PQC)

When will the quantum computer age start?

Quantum Computers and Cryptography

Small-scale quantum computers have already been created by large companies and organisations around the world. These computers are expanding rapidly, and the goal of a large-scale quantum computer seems within reach in the not-too-distant future.

When these computers become available, current public-key cryptosystems like RSA or elliptic curves will become insecure. Shor's algorithm shows how, using a quantum computer, the prime factorisation of a large number and the calculation of discrete logarithms can be done in polynomial time.

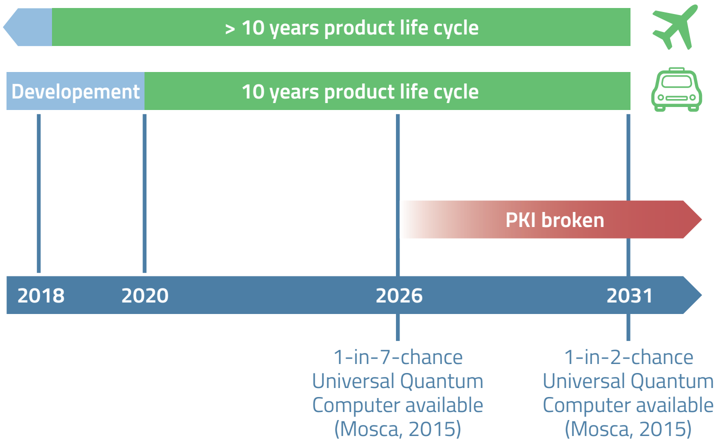
Additionally, symmetric encryption algorithms and hash functions that are not directly tied to a mathematical problem are also at risk, as Grover's algorithm shows. In this case, the impact is not as devastating as in public-key cryptography, but the time it takes to break a symmetric scheme or a hash function through a brute-force attack or an exhaustive search is reduced by almost half.

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC256	128		
	ECC 521	256		
Symmetric	AES128	128	64	Grover's Algorithm
	AES 256	256	128	

Source: isara.com

Who is affected

The probability to break RSA 2048 by 2031 is estimated at 50 %. Complex software solutions and products usually entail long and arduous product development processes. Additionally, many industries like automotive, aerospace, transportation, public and critical infrastructure, design and produce goods today that will be on the market for the next 20 to 50 years.



> 10 years product life cycle
Developement
10 years product life cycle
PKI broken
2018
2020
2026
2031
1-in-7-chance Universal Quantum Computer available (Mosca, 2015)
1-in-2-chance Universal Quantum Computer available (Mosca, 2015)

Another interesting aspect of these industries is their reliance on pre-orders that are produced now, but delivered far off in the future (+10 years). These products will most certainly face the threat of quantum computers. Consequently, it is essential to plan ahead and integrate the required protection mechanisms in the design and production processes that take place today.

»

The probability to break RSA 2048 by the year 2031 is estimated at 50 percent.

MTG is a leading expert for encryption technologies in Germany. MTG's IT security solutions effectively secure critical infrastructures and the Internet of Things (IoT). MTG offers a comprehensive portfolio of state-of-the-art quantum-safe security products and services. Working closely with our customers, we integrate PQC into existing applications and protocols by means of hybrid processes.

For further information feel free to contact us!

MTG

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