MTG

Enterprise Resource Security
Mastering Cryptographic Key Lifecycles

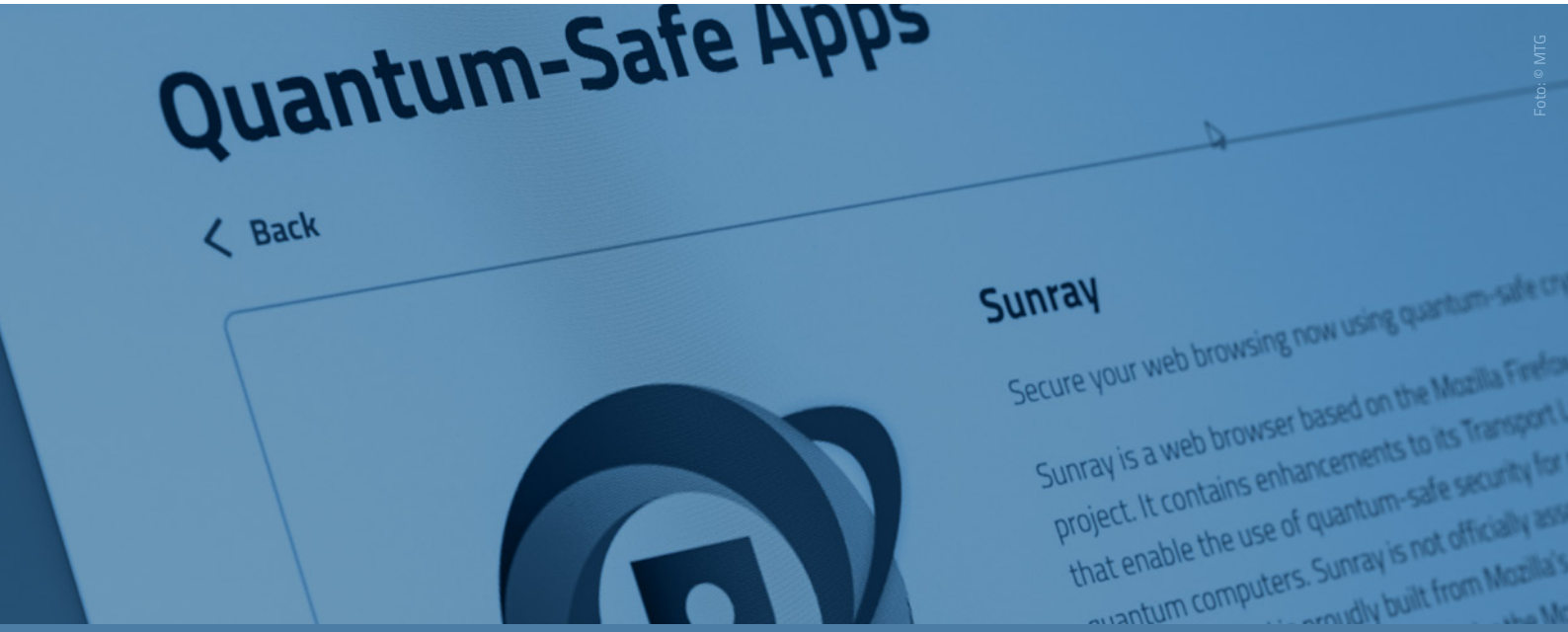
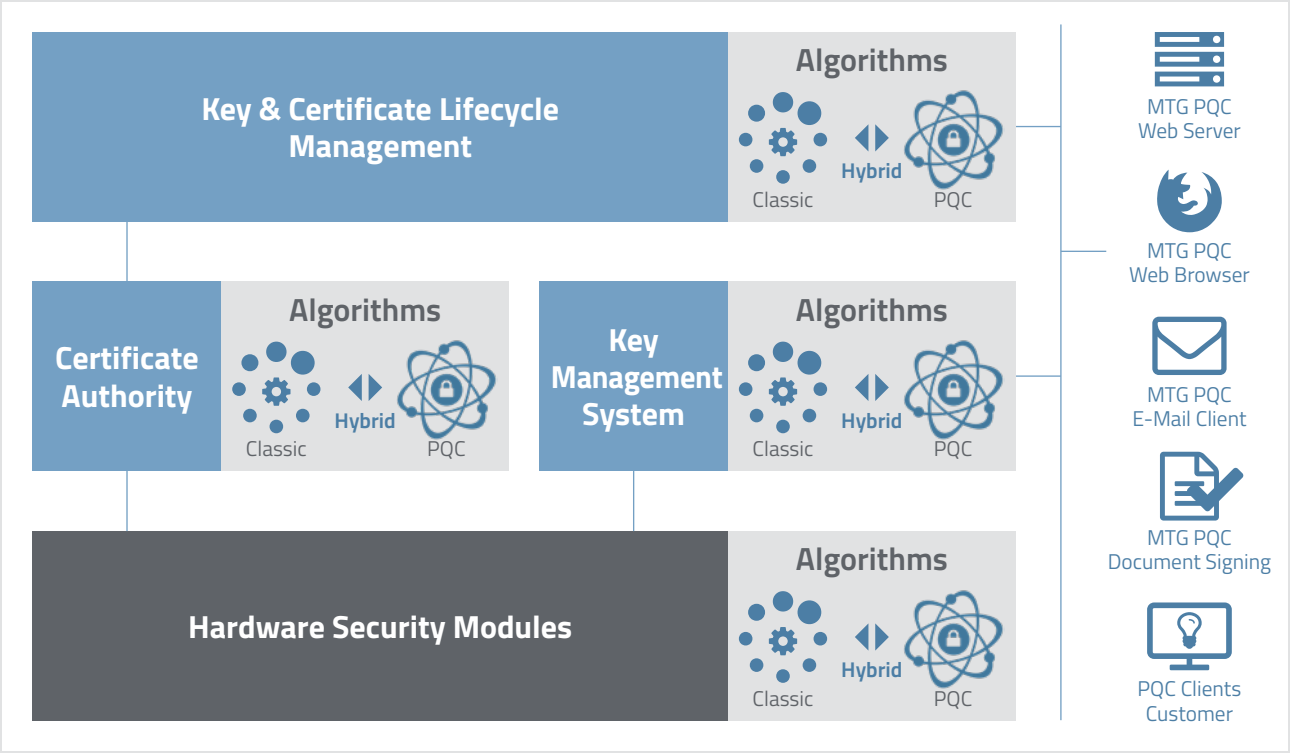


Foto: © MTG

MTG Post-Quantum Cryptography

Decision-makers in security-critical industries who especially use asymmetric encryption methods have to take action today in order to adequately protect themselves against future threats from quantum computers. All components of the MTG ERS® system are PQC-ready!

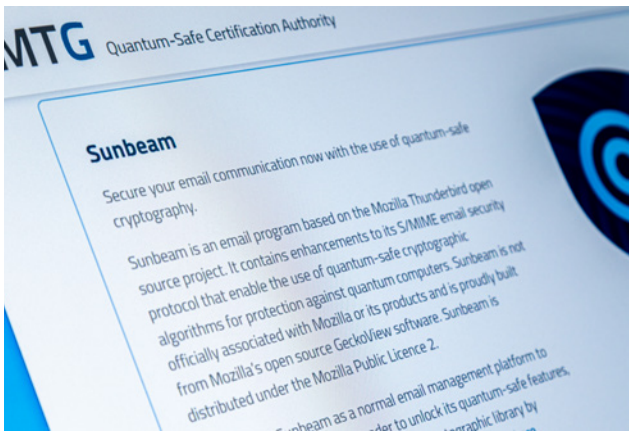
With our PQC portfolio, it is already possible to protect data against future decryption by quantum computers. For this purpose, existing MTG ERS® components have been extended with PQC algorithms.



PQC Applications

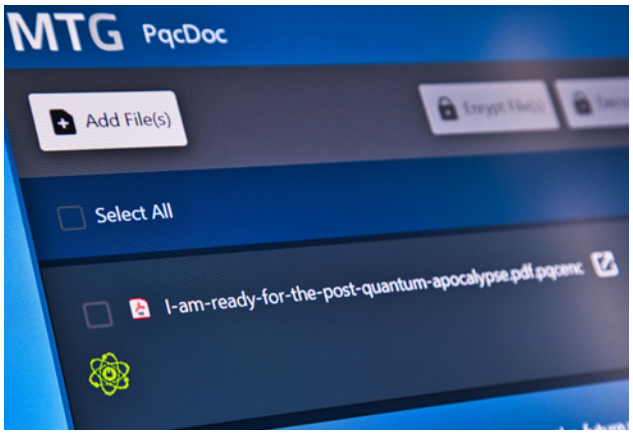
PQC Web Browser & Web Server

During development, MTG incorporated various PQC schemes into its MTG ERS®. For this purpose, a Mozilla Firefox-based browser (Sunray) and an Apache Tomcat-based web server with integrated support for PQC TLS were implemented. During development, MTG incorporated various PQC schemes into its MTG ERS®. For this purpose, a Mozilla Firefox-based browser (Sunray) and an Apache Tomcat-based web server with integrated support for PQC TLS were implemented.



PQC E-Mail-Client Sunbeam

For the encryption and signing of e-mails, an extension to the Thunderbird mail program and the S/MIME format was developed. The newly created program Sunbeam allows users to encrypt e-mails using Classic McEliece and sign them using SPHINCS+. The encryption is a hybrid encryption. The message and any attachments are encrypted with a symmetric key and this key is encrypted with a Classic McEliece public key.



PQC Document Signing

The PQCDoc application enables signing and encryption of archived documents with selected PQC algorithms. The application can be used to secure data-at-rest (e.g. data archives) as well as data-in-transit (e.g. email attachments). The choice of algorithms ensures long-term security and counters "Store Now Decrypt Later (SNDL)" attacks from the very beginning. Data that is secured with PQCDoc is of no value to any third party, now and at a future point in time when powerful quantum computers will eventually be available.

The PQCDoc application enables signing and encryption of archived documents with selected PQC algorithms.

MTG Post-Quantum Cryptography

PQC Consulting

PQC Migration and Integration

There are a number of challenges and rules to consider when integrating PQC algorithms. More space must be considered for PQC keys and signatures, which can cause problems with limited database schemes or source codes (e.g., for Firefox or Libraries). When selecting algorithms, systems should be able to flexibly adapt to current progress in ongoing standardization processes. An often underestimated aspect is the holistic view of a PQC implementation project. When using PQC algorithms, it is crucial that the complete key management lifecycle is taken into account.

MTG supports companies in migrating their systems to Post-Quantum Cryptography and in using PQC in new products.

Consulting Focus

Identification and analysis of the current processes in use
Selection of a suitable post-quantum scheme (algorithms, hybrid schemes, KEM combiners, etc.) for replacement as well as identification and documentation of the resulting requirements (e.g., adaptation to databases due to larger keys, etc.).
Documentation of required adaptations to products as well as support during implementation, integration and realization.
Implementation of PQC in public key infrastructures, key management systems and hardware security modules
Implementation of PQC in Embedded Systems
Consulting on PQC standards and status of migration of standards and protocols (e.g., TLS, SSH, IPsec etc.) to PQC. Specification of protocols after final standardization of algorithms.
Support for the compliance with regulatory requirements (e.g., PCI DSS, BAIT, Gematik etc.)
Supporting the creation of a crypto inventory. Creation of a catalog of procedures currently in use for development-related technical tasks.

Workshop & Key Notes Topics

When introducing PQC in companies or for specific PQC projects, key notes and kick-off workshops are an effective way to meet future stakeholders and to raise awareness of the current challenges at an early stage. The following main topics are covered in this context.

> Introduction: What is a quantum computer, when is it expected to be available, and what problems are associated with it?

> Possible solutions: Quantum Cryptography and Post-Quantum Cryptography (PQC)

> Post-quantum cryptography methods: comparison of parameters (key size, computational effort, size of ciphertexts)

> Challenges and obstacles in PQC projects: Which process is suitable for which application? Which aspects need to be taken into special consideration during migration and integration?

> Status of standardization activities (NIST Competition etc.)

> Possible procedure of a migration from classical cryptography to PQC

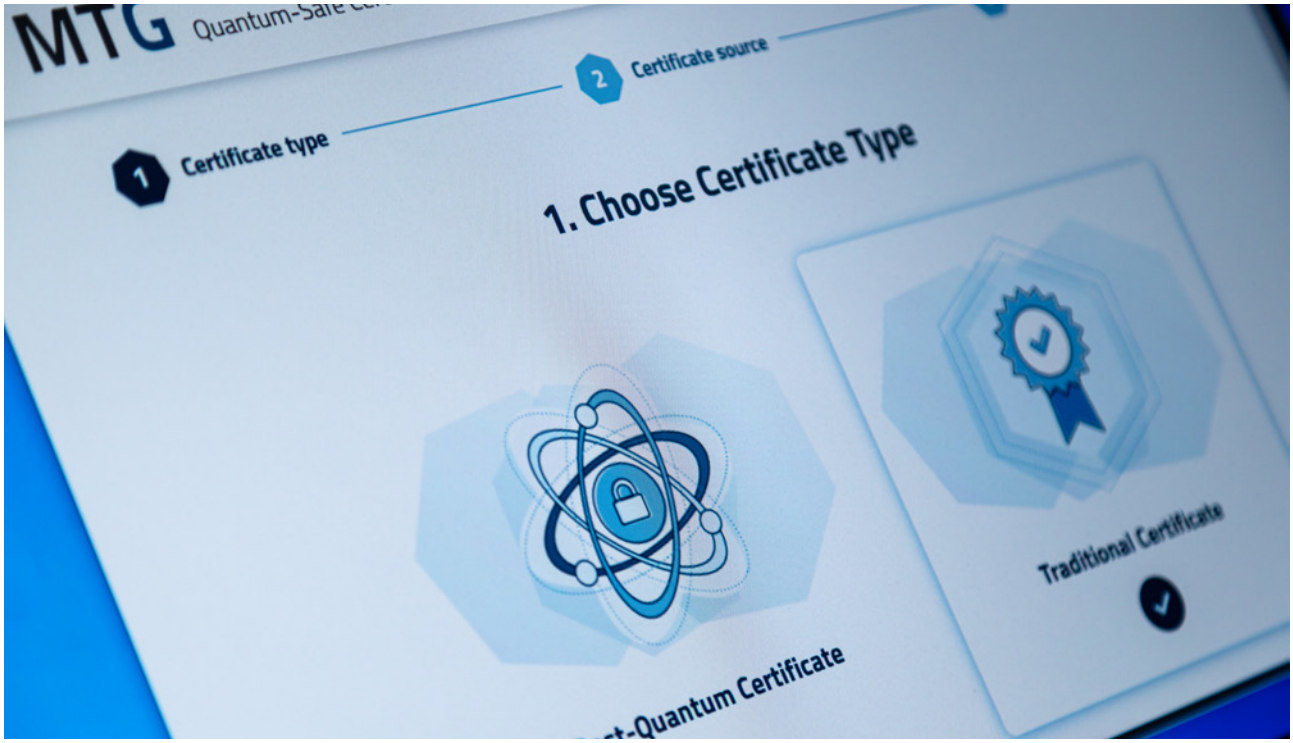
MTG Post-Quantum Cryptography

PQC Demo for Apps and PKI

Free PQC Online Demo

MTG has developed PQC solutions that can already be applied and tested today. We would like to offer interested parties the opportunity to see for themselves that quantum safe applications can already be put into practice today. Our online PQC platform, which is open to the public, allows you to create your own cost-free post-quantum and traditional certificates for testing purposes. These can then be deployed to various provided PQC demo applications.

pqc-pki.mtg.de



As soon as long-lived products and services run into the quantum computing era with current encryption methods, it will be too late for companies to act in time.

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