MTG

MTG Post-Quantum Cryptography (PQC)

The Next Generation of Cryptography

RSA Conference, San Francisco, March 2019

MTG AG Company Profile

- MTG, which was founded in 1995, is a high tech software company based in the Rhein-Main region (Darmstadt, Germany) – the Germany IT security cluster.
- 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 security products and services, such as PKI, Key Management System, and HSM integration with best practice traditional and Post-Quantum Cryptography.

Integrate Post-Quantum Cryptography now!

Key Driver for Quantum Computing

Photos: Unsplash

- Quantum Computing is using quantum-mechanical phenomena and will significantly increase computing power
- Quantum computing will solve today‘s unsolvable problems and open new possibilities.

Classical Bit

Off = 0

OR

On = 1

- Classical computers support only one set of states per clock tick

Quantum Bit (QUBIT) is different!

Off = 0 **AND !** ON = 1

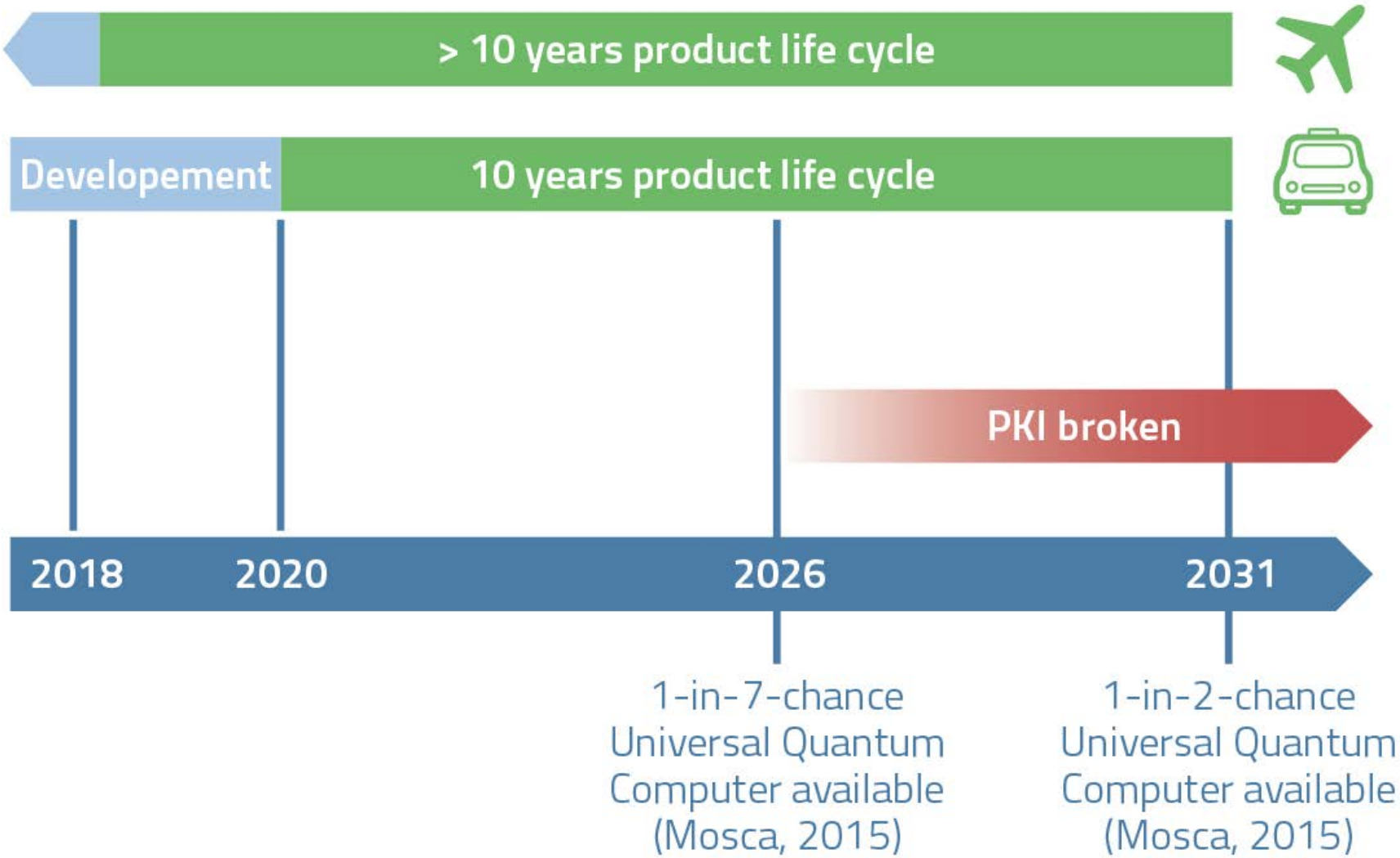
- A quantum bit (qubit) can exist in multiple states simultaneously!
- The number of states potentially grows with the number of qubits (2N , N = number of Qubits)
- Example: A system with 16 qubits can be in 2^{16} = 65.536 states at once

Effects of quantum computers on today's cryptography

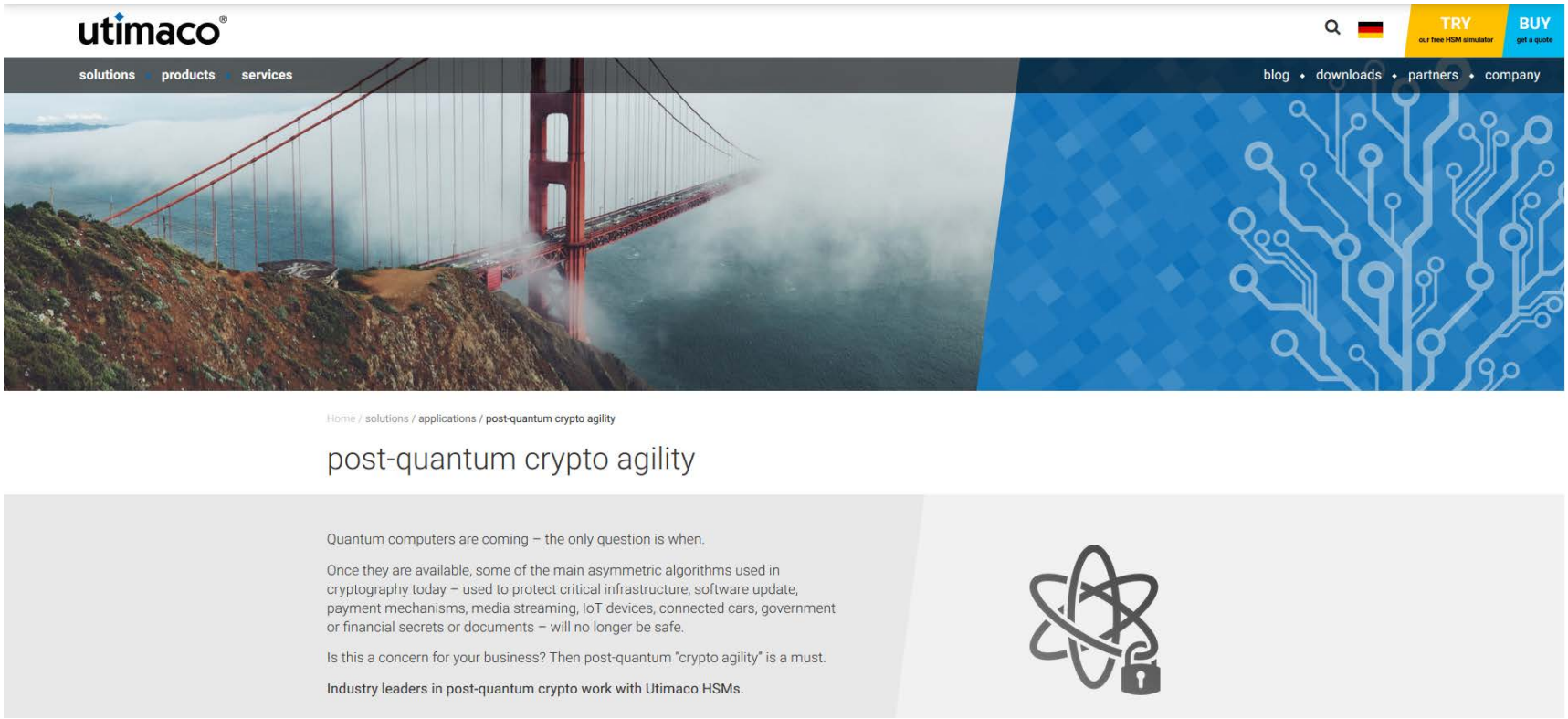
Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC256	128		
	ECC 521	256		
Symmetric	AES128	128	64	Grover's Algorithm
	AES 256	256	128	

- However, quantum computers also have a very decisive negative influence on today's IT security: quantum computers break the security of today's IT infrastructures.

Quantum impact



PQC Partnerships, Research & Development



- When developing our PQC solutions and services, we remain in regular cooperation with other PQC specialized companies (e.g. Isara) and also work closely with research institutions (e.g. Fraunhofer SIT and universities).
- We constantly monitor the developments of the NIST Competition to determine the future PQC schemes. This ensures that only recognized and tested PQC schemes are implemented in our products and projects.

MTG PQC Solutions Today

MTG PQC Portfolio 2019

MTG

PQC Key Management

PQC PKI

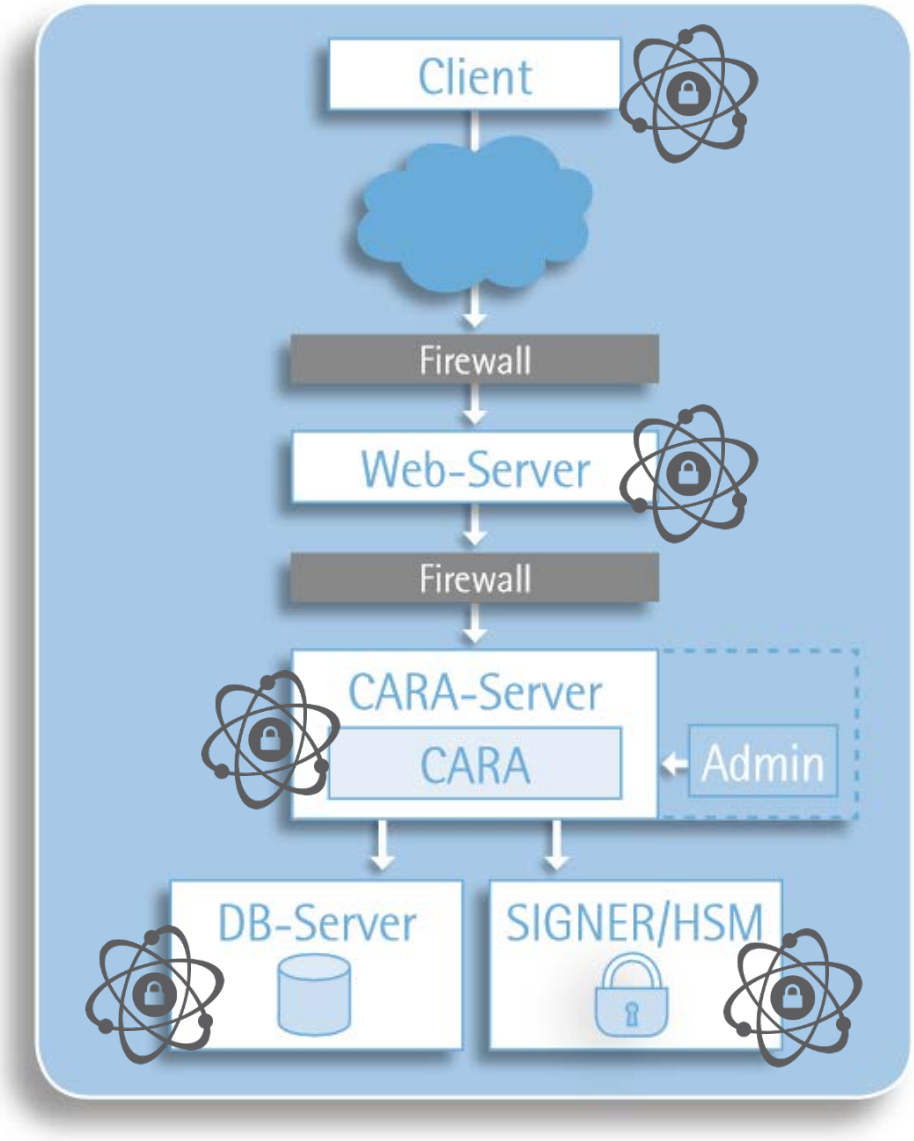
PQC Suite
(Web Browser, Web Server, Email Client, Document Signing & Encryption))

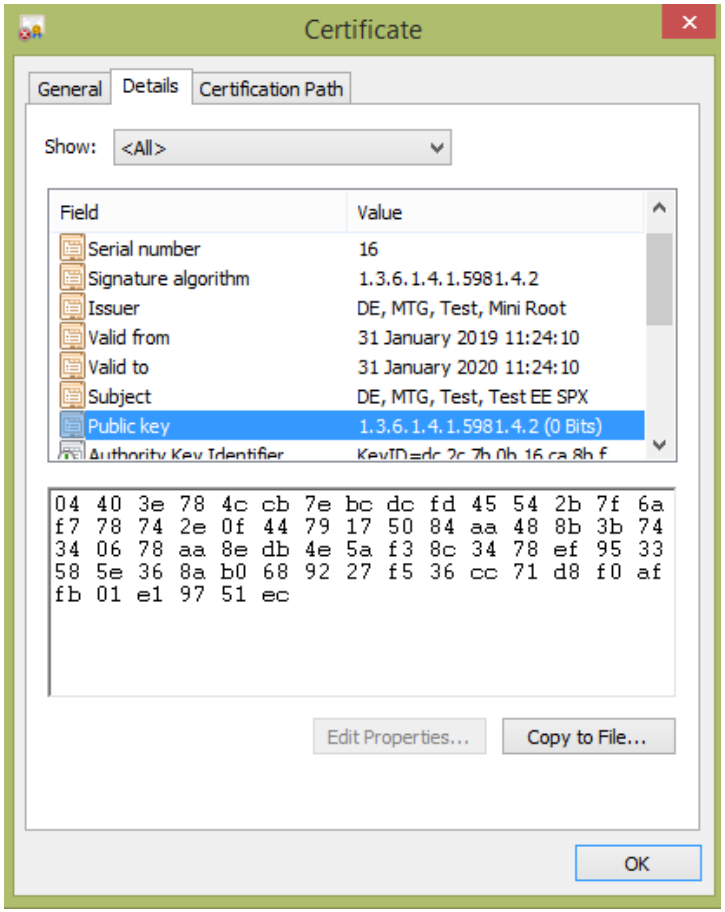
PQC Services

PQC HSM Integration

MTG Portfolio
Post-Quantum Cryptography and Crypto Agility

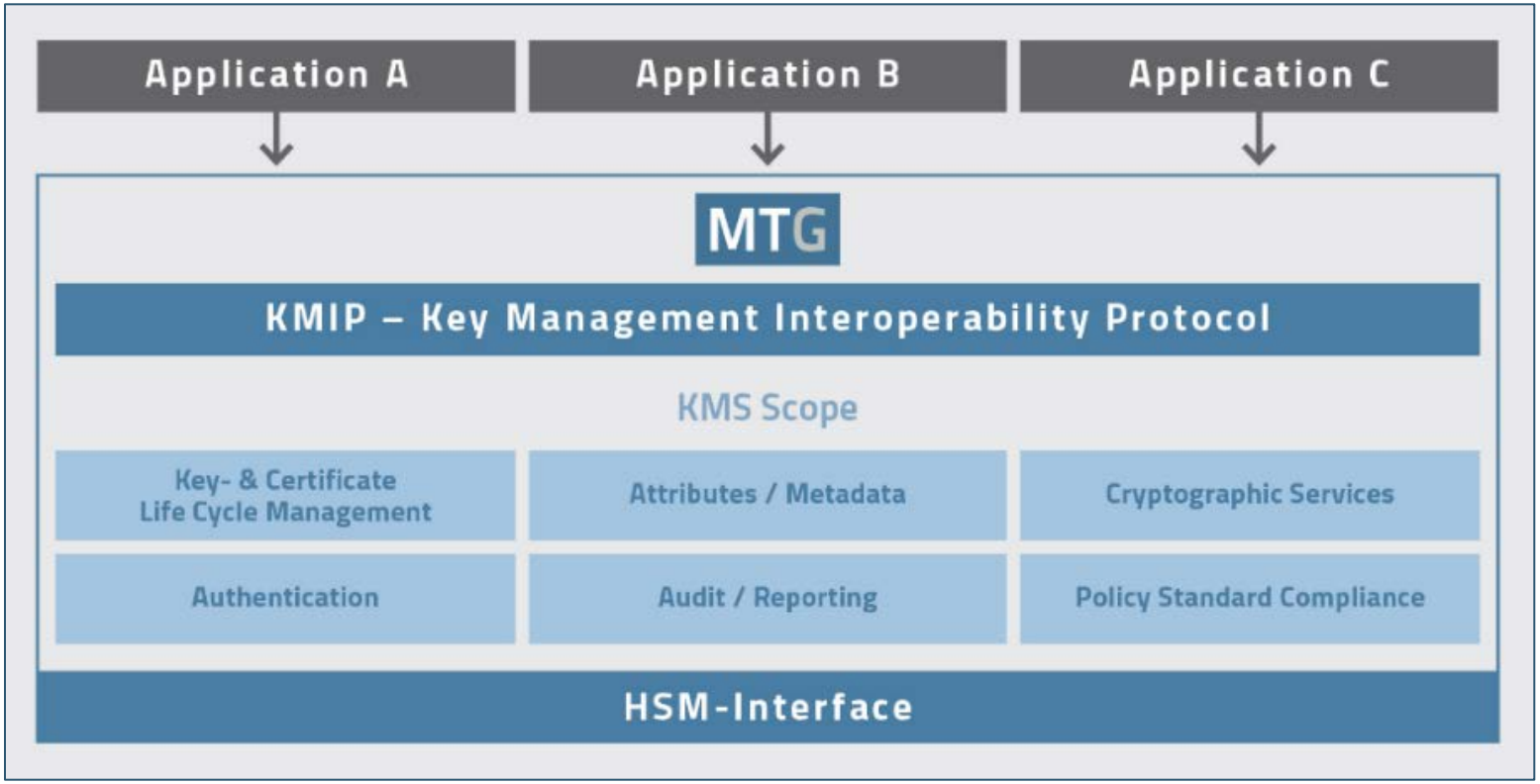
PKI MTG CARA - PQC Adaptations





CARA PKI: SPHINCS+ and Classic McEliece certificates

MTG Key Management System – PQC KMS



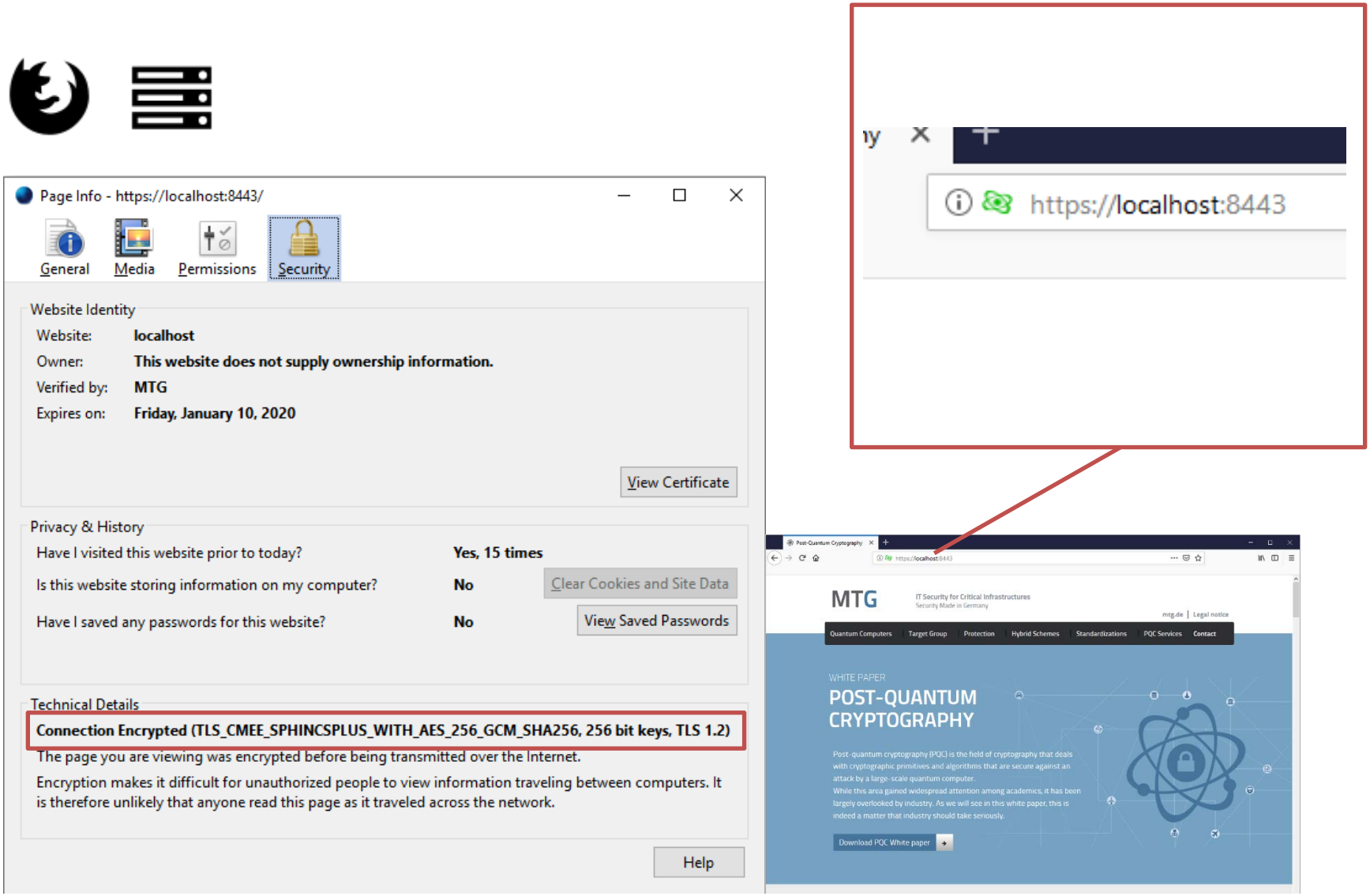
- Highly available management of traditional and PQC keys for various applications
- Detached, central security module, able to perform all necessary cryptographic operations

MTG PQC Suite

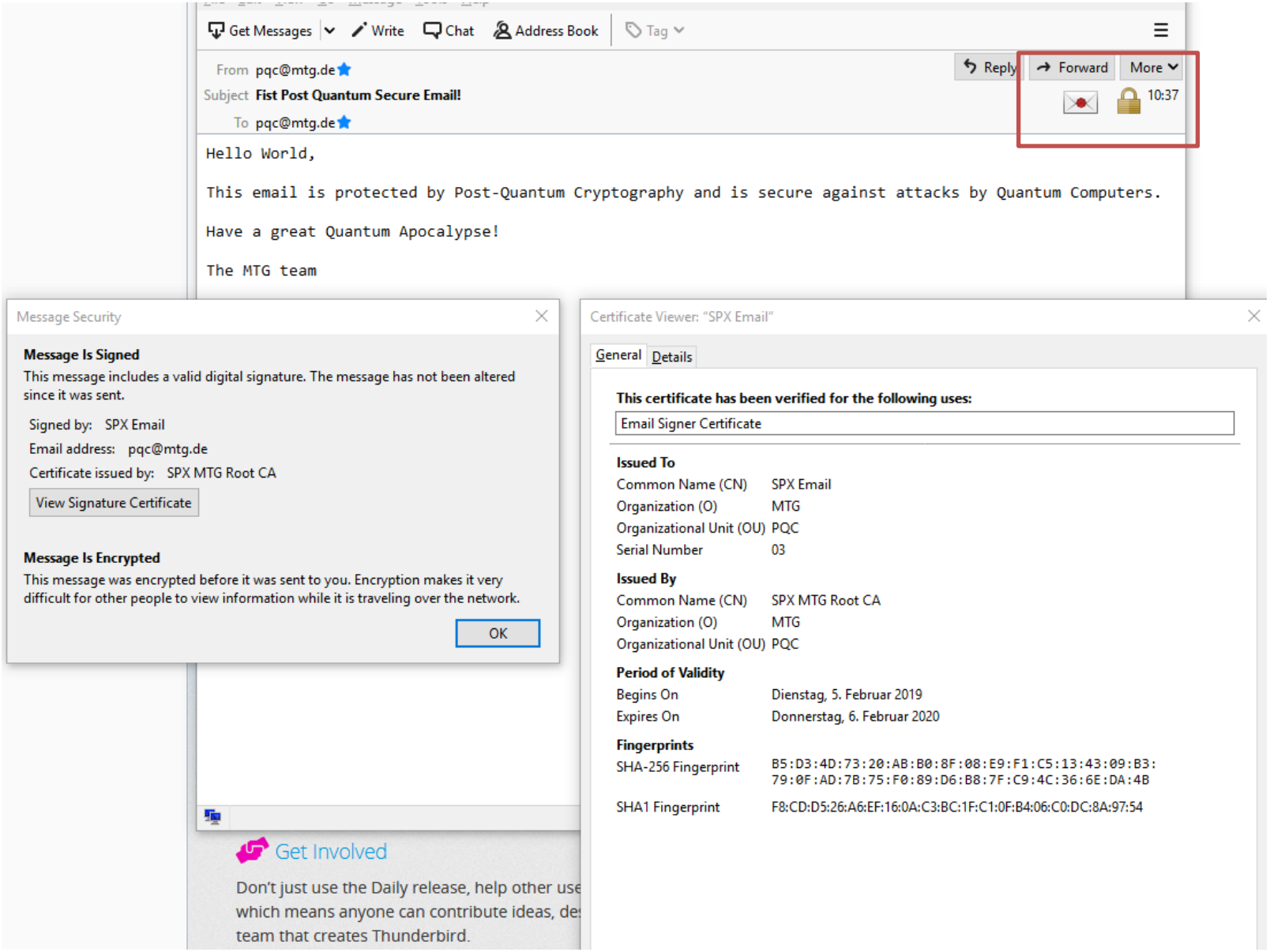
Ready to Use PQC Applications!

- **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 SMIME
- **Document Signing & Encryption:**
  Solution for generic document signing and encryption using state of the art PQC signature algorithms

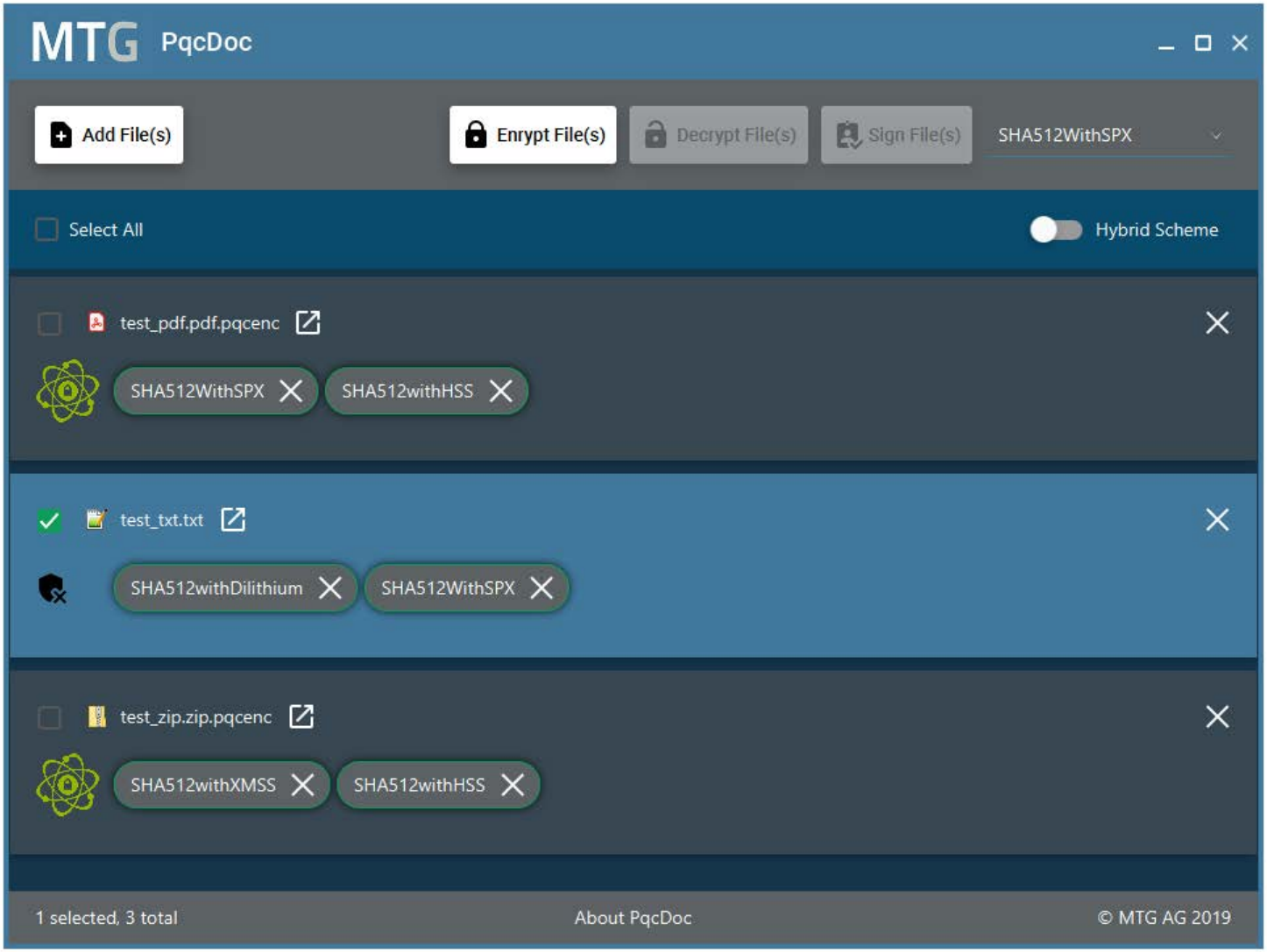
Use Case: PQC Web Browser & Web Server



Use Case: PQC Email Client



Use Case: PQC Document Signing & Encryption

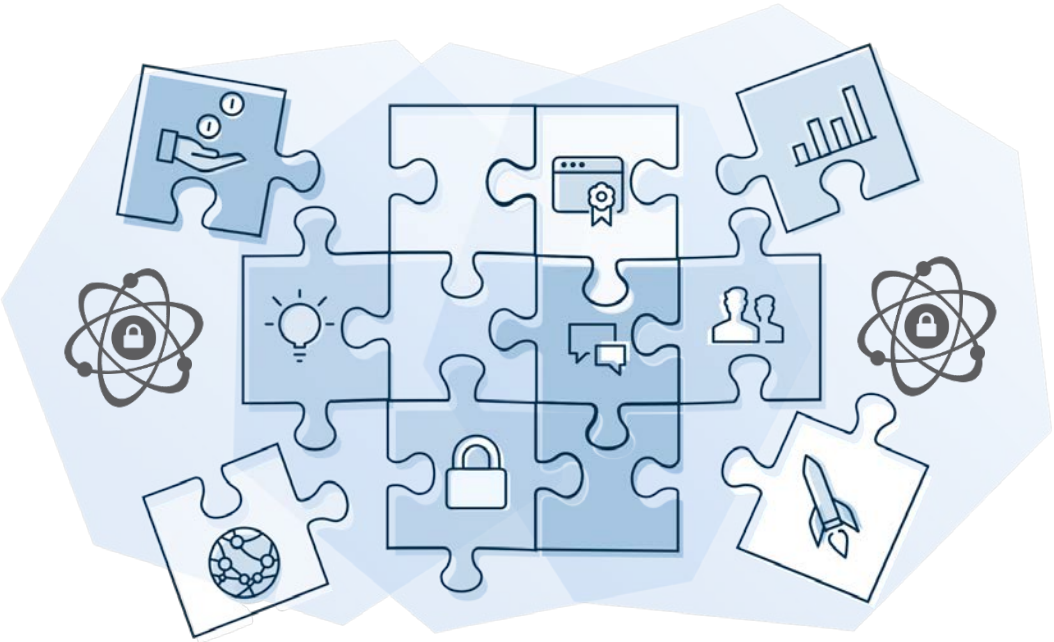


PQC HSM Integration

utimaco® certified Premier
Value Added Reseller

- When strong protection and usage of PQC keys is necessary
- Integration of PQC algorithms in HSMs
- Extension Module can be added to already deployed HSMs

PQC Services



- Seamless integration of PQC into existing customer applications and products by leading PQC experts
- In close cooperation with our customers, we are implementing the integration of PQC into existing applications and protocols in joint projects

Thank You!


MTG
Let's meet!
North Hall, Hall D | German Pavilion | Booth 5671S
MTG presents:
Post-Quantum Cryptography
Made in Germany
mtg.de
RSAConference2019
San Francisco | March 4–8 | Moscone Center

Contact

Jürgen Ruf

jruf@mtg.de

+ 49 6151 8000 12

Tamer Kemeröz

tkemeroez@mtg.de

+ 49 6151 8000 11