



MTG Post-Quantum Cryptography (PQC)

The Next Generation of Cryptography

RSA Conference, San Francisco, March 2019



- 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!**



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.



Off = 0

OR



On = 1

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

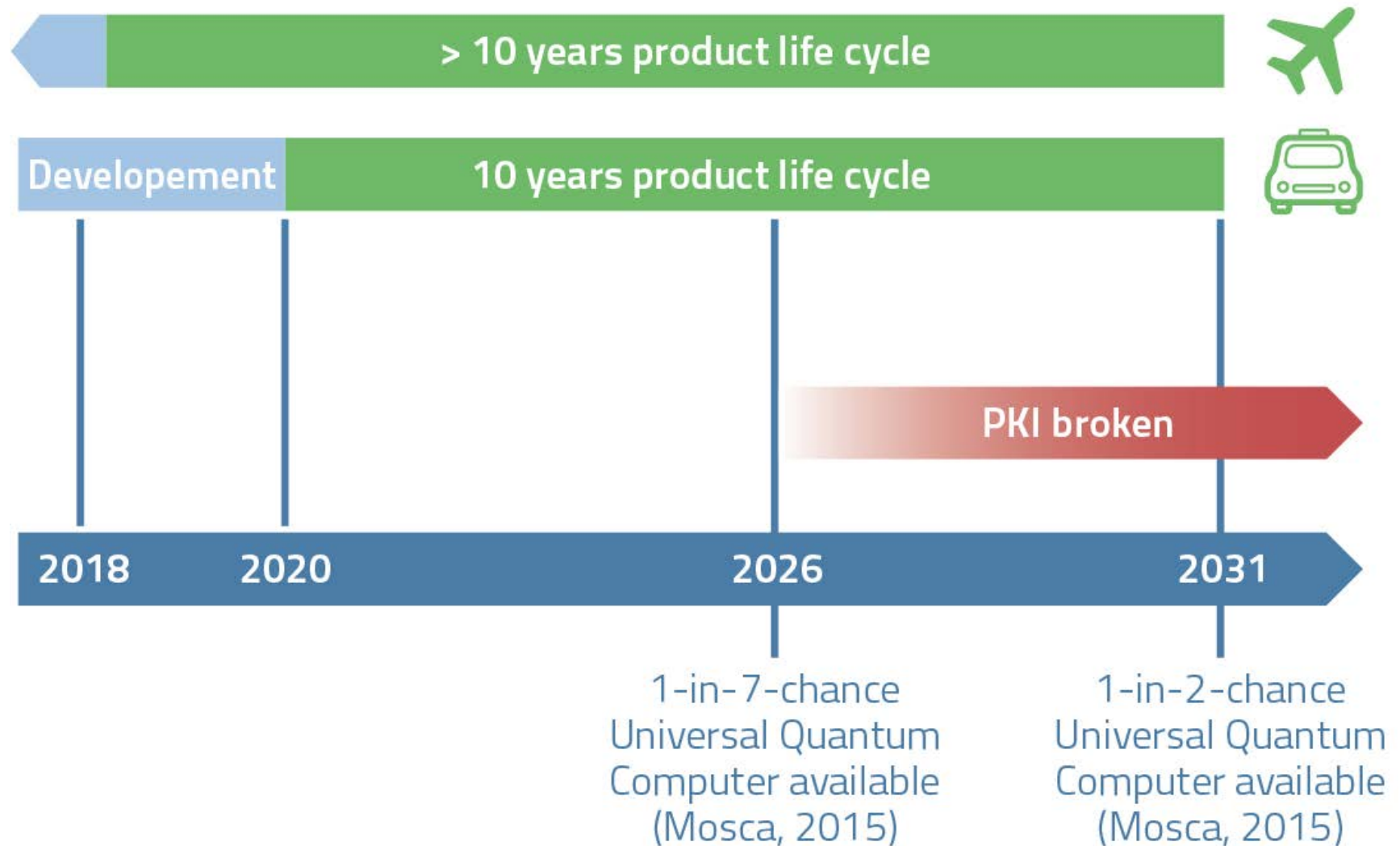


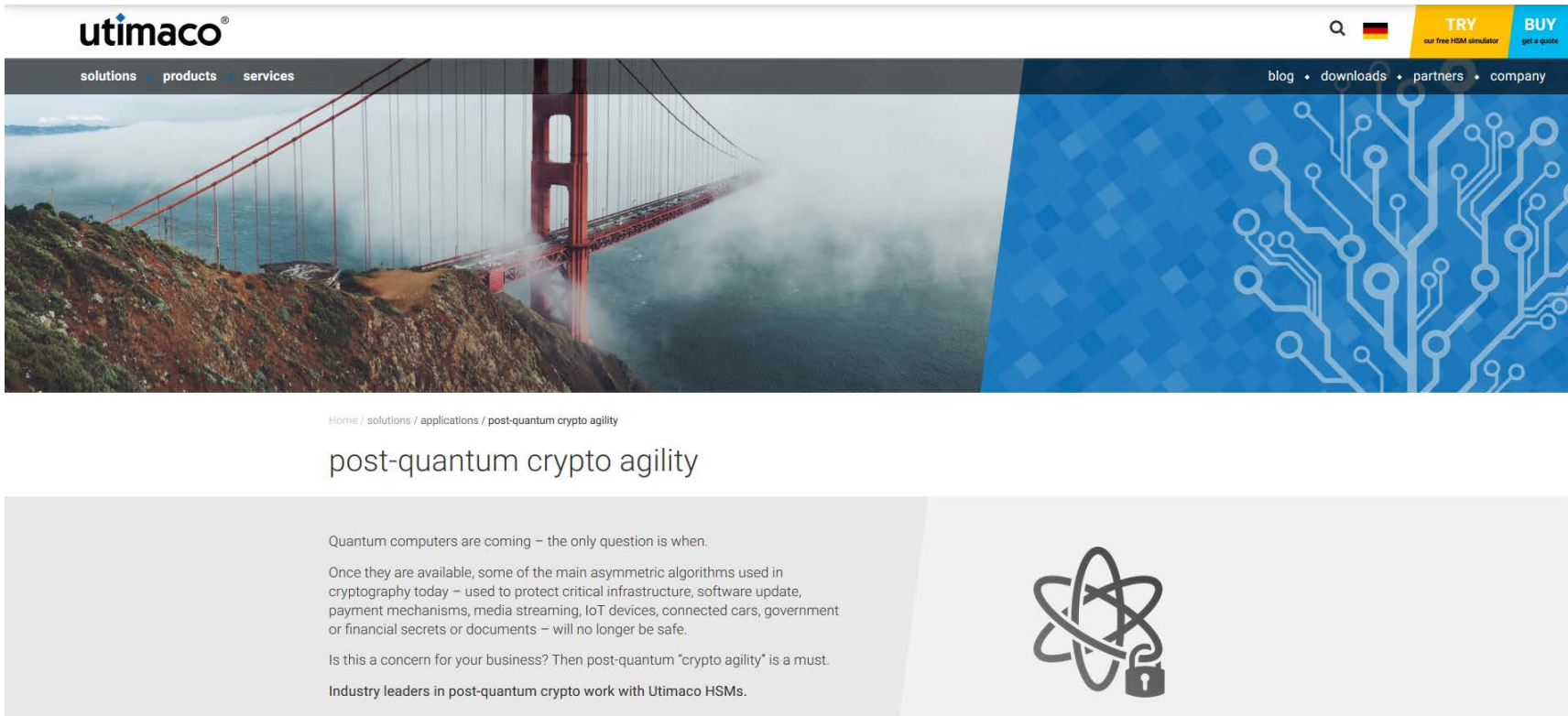
Off = 0 **AND !** ON = 1

- A quantum bit (qubit) can exist in multiple states simultaneously!
- The number of states potentially grows with the number of qubits (2^N , N = number of Qubits)
- Example: A system with 16 qubits can be in $2^{16} = 65,536$ states at once

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.



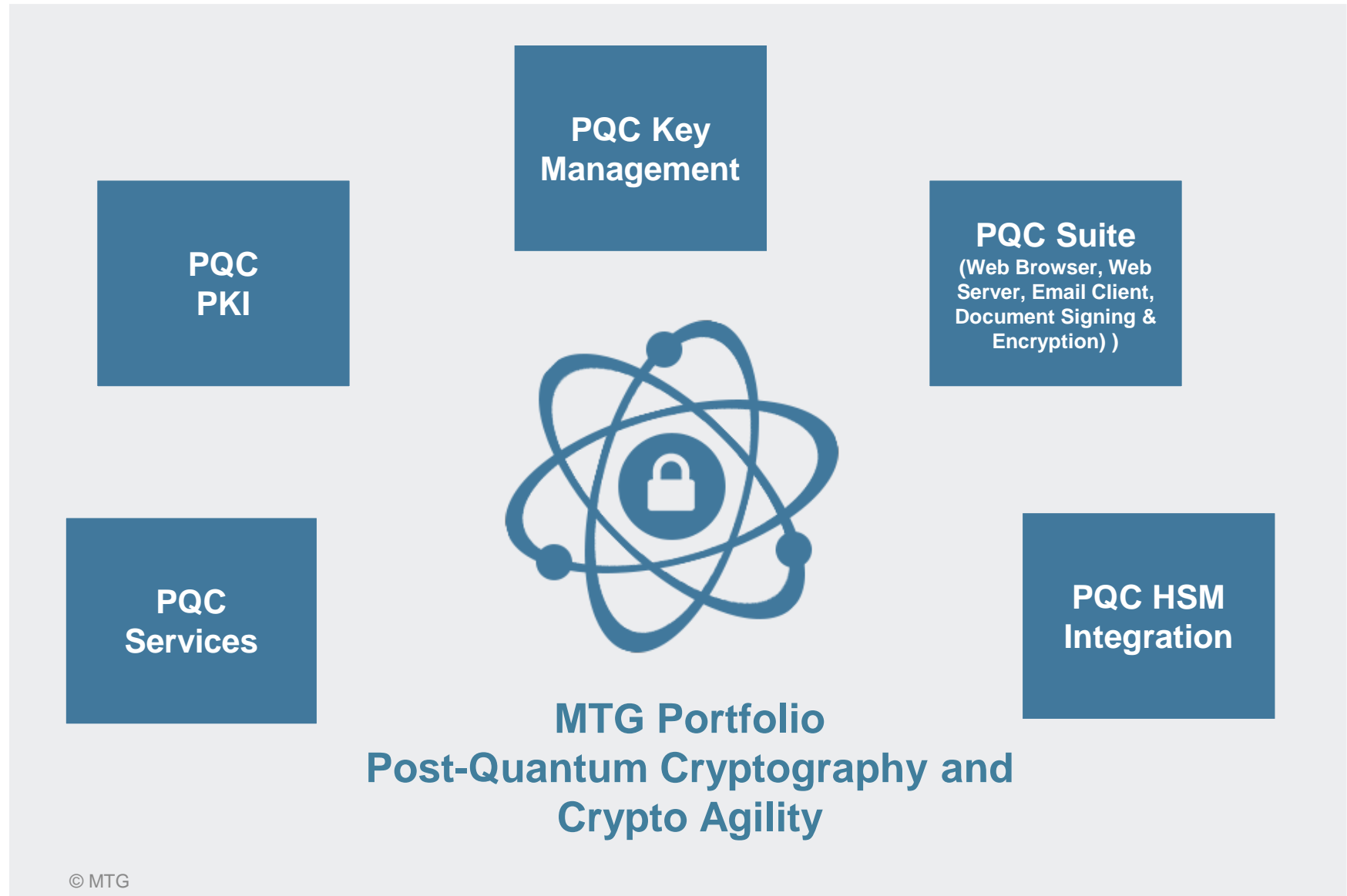


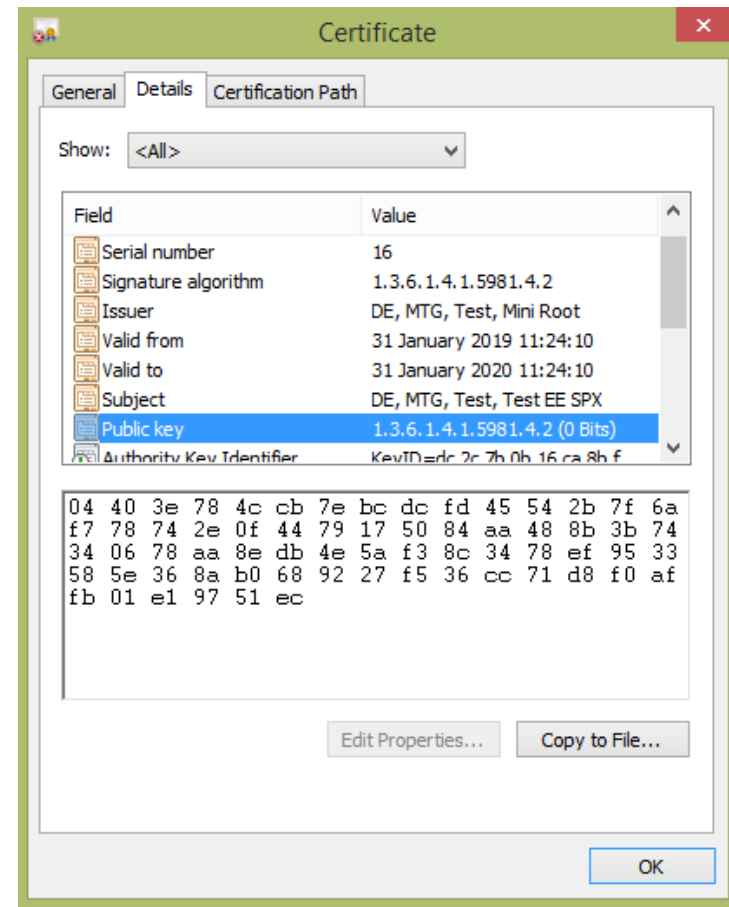
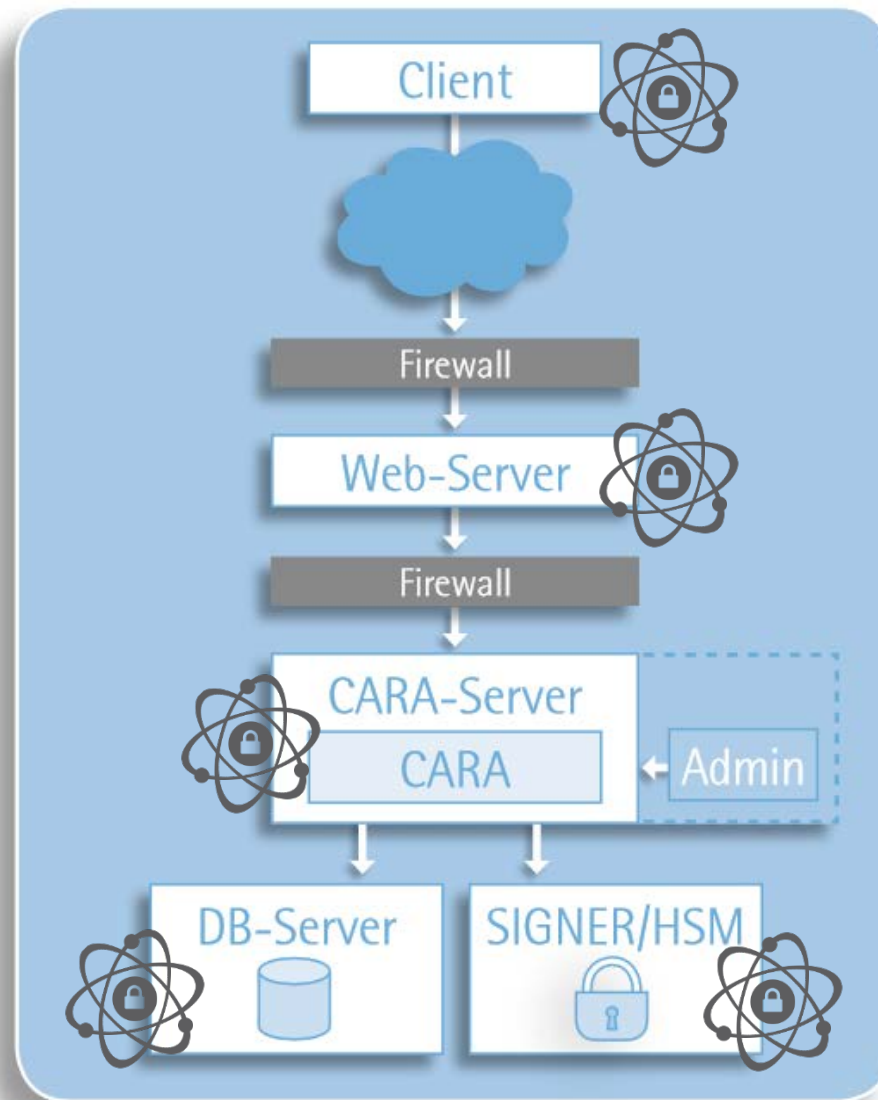
The screenshot shows the Utimaco website. The header includes the Utimaco logo, navigation links for solutions, products, and services, a search icon, a German flag, and buttons for 'TRY' (our free HSM simulator) and 'BUY' (get a quote). Below the header is a large banner featuring a photograph of the Golden Gate Bridge on the left and a blue background with white circuitry patterns on the right. The banner text reads: 'Home / solutions / applications / post-quantum crypto agility' followed by 'post-quantum crypto agility'. Below this, a grey box contains the following text: 'Quantum computers are coming – the only question is when. Once they are available, some of the main asymmetric algorithms used in cryptography today – used to protect critical infrastructure, software update, payment mechanisms, media streaming, IoT devices, connected cars, government or financial secrets or documents – will no longer be safe. Is this a concern for your business? Then post-quantum “crypto agility” is a must. Industry leaders in post-quantum crypto work with Utimaco HSMs.' To the right of this text is an icon of an atom with a padlock.

- 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.

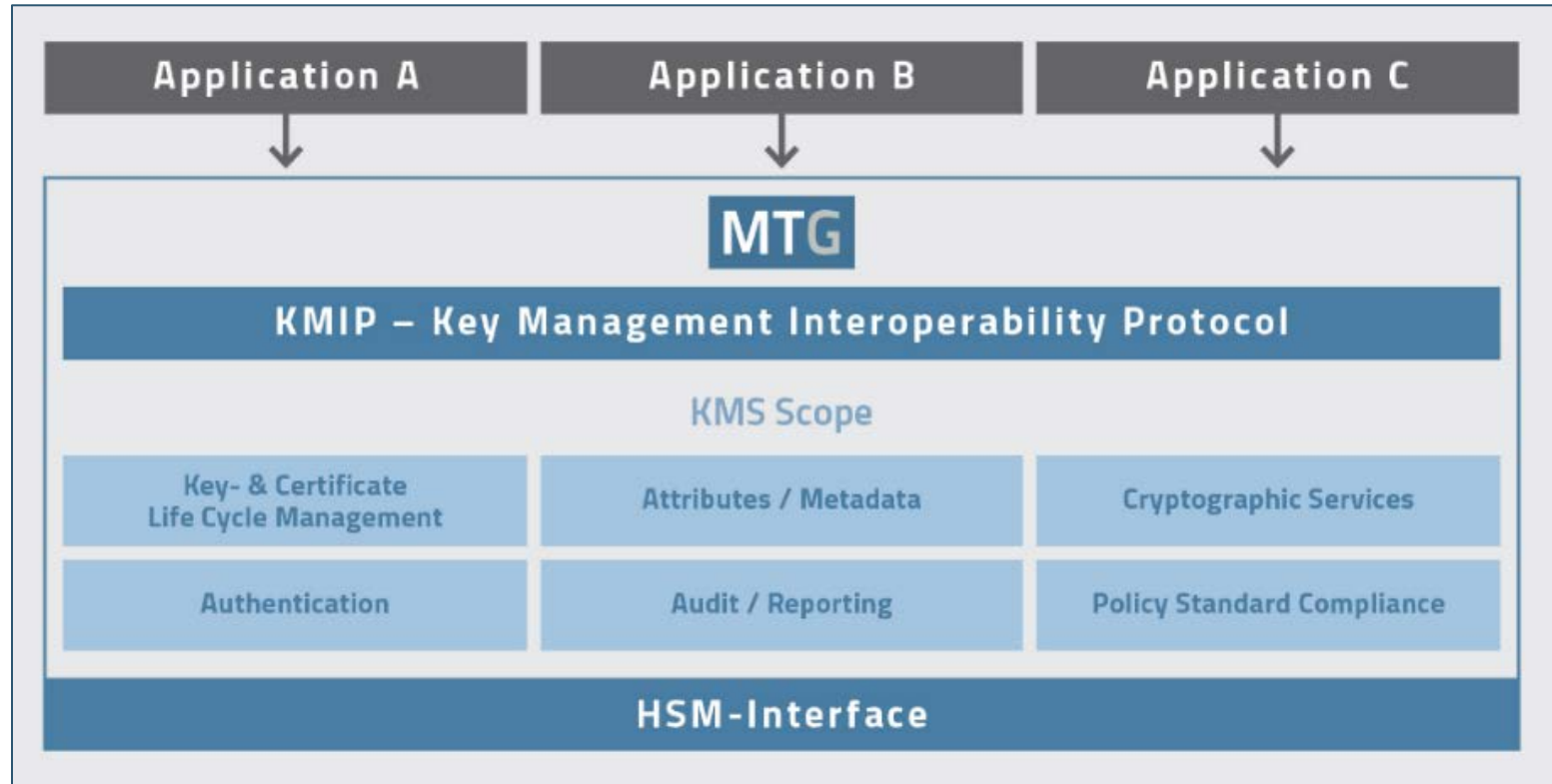


MTG PQC Solutions Today





CARA PKI: SPHINCS+ and Classic McEliece certificates



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



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



Page Info - https://localhost:8443/

General Media Permissions Security

Website Identity

Website: **localhost**
Owner: **This website does not supply ownership information.**
Verified by: **MTG**
Expires on: **Friday, January 10, 2020**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? **Yes, 15 times**

Is this website storing information on my computer? **No** [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? **No** [View Saved Passwords](#)

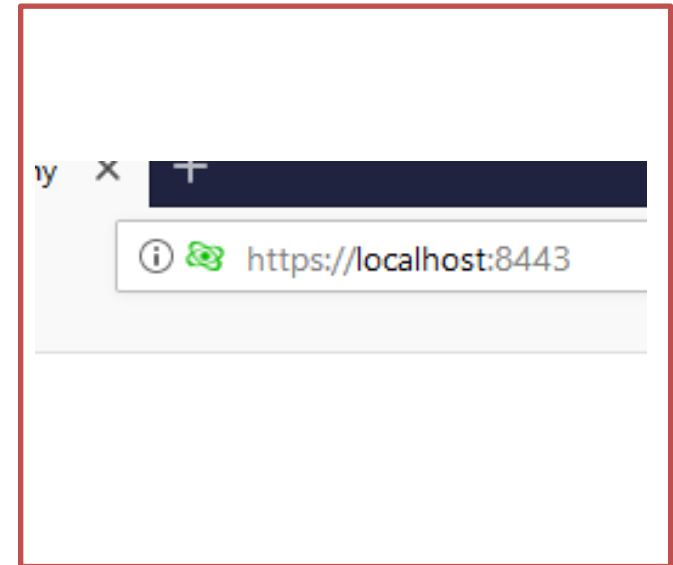
Technical Details

Connection Encrypted (TLS_CAMEL_SPHINCSPLUS_WITH_AES_256_GCM_SHA256, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)



Post-Quantum Cryptography X

https://localhost:8443

MTG IT Security for Critical Infrastructures
Security Made in Germany

mtg.de | Legal notice

Quantum Computers Target Group Protection Hybrid Schemes Standardizations PQC Services Contact

WHITE PAPER

POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography (PQC) is the field of cryptography that deals with cryptographic primitives and algorithms that are secure against an attack by a large-scale quantum computer. While this area gained widespread attention among academics, it has been largely overlooked by industry. As we will see in this white paper, this is indeed a matter that industry should take seriously.

[Download PQC White paper](#)



Get Messages Write Chat Address Book Tag

From pqc@mtg.de
Subject **Fist Post Quantum Secure Email!**
To pqc@mtg.de

Reply Forward More 10:37

Hello World,

This email is protected by Post-Quantum Cryptography and is secure against attacks by Quantum Computers.

Have a great Quantum Apocalypse!

The MTG team

Message Security

Message Is Signed
This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: SPX Email
Email address: pqc@mtg.de
Certificate issued by: SPX MTG Root CA

View Signature Certificate

Message Is Encrypted
This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.

OK

Certificate Viewer: "SPX Email"

General Details

This certificate has been verified for the following uses:
Email Signer Certificate

Issued To

Common Name (CN)	SPX Email
Organization (O)	MTG
Organizational Unit (OU)	PQC
Serial Number	03

Issued By

Common Name (CN)	SPX MTG Root CA
Organization (O)	MTG
Organizational Unit (OU)	PQC

Period of Validity

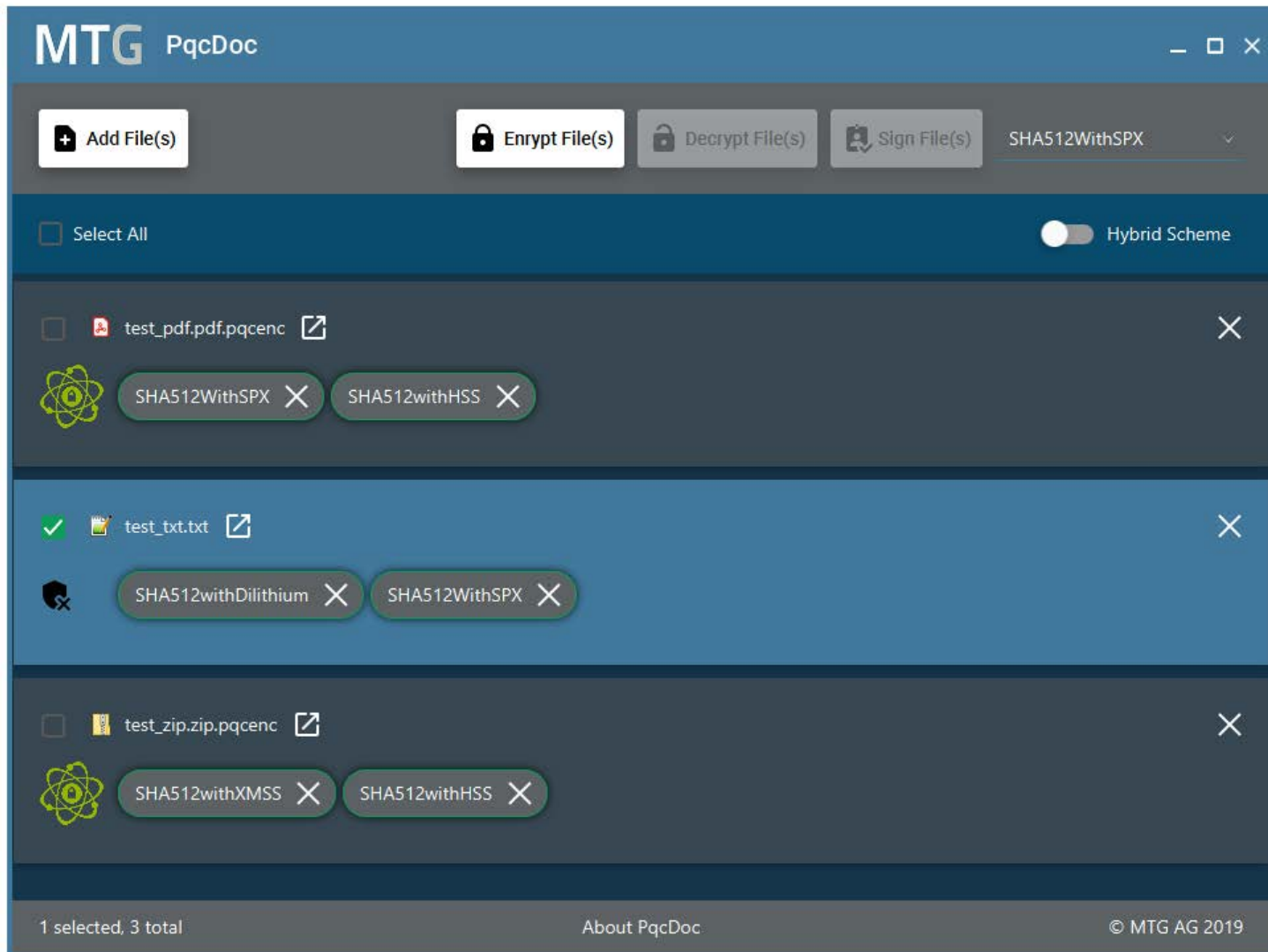
Begins On	Dienstag, 5. Februar 2019
Expires On	Donnerstag, 6. Februar 2020

Fingerprints

SHA-256 Fingerprint	B5:D3:4D:73:20:AB:80:8F:08:E9:F1:C5:13:43:09:B3:79:0F:AD:7B:75:F0:89:D6:B8:7F:C9:4C:36:6E:DA:4B
SHA1 Fingerprint	F8:CD:D5:26:A6:EF:16:0A:C3:BC:1F:C1:0F:B4:06:C0:DC:8A:97:54

Get Involved

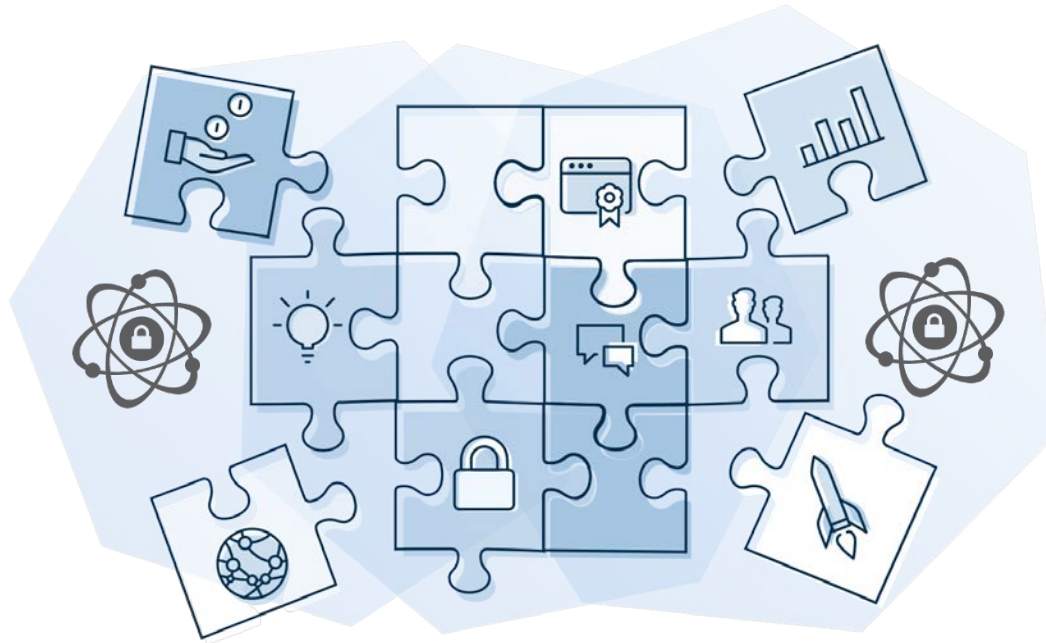
Don't just use the Daily release, help other use which means anyone can contribute ideas, team that creates Thunderbird.



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



- 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

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
