TeleTrusT-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 18.06.2019

Real World Post Quantum Cryptography in Public Key Infrastructures

Stathis Deligeorgopoulos, MTG AG

MTG AG Company Profile

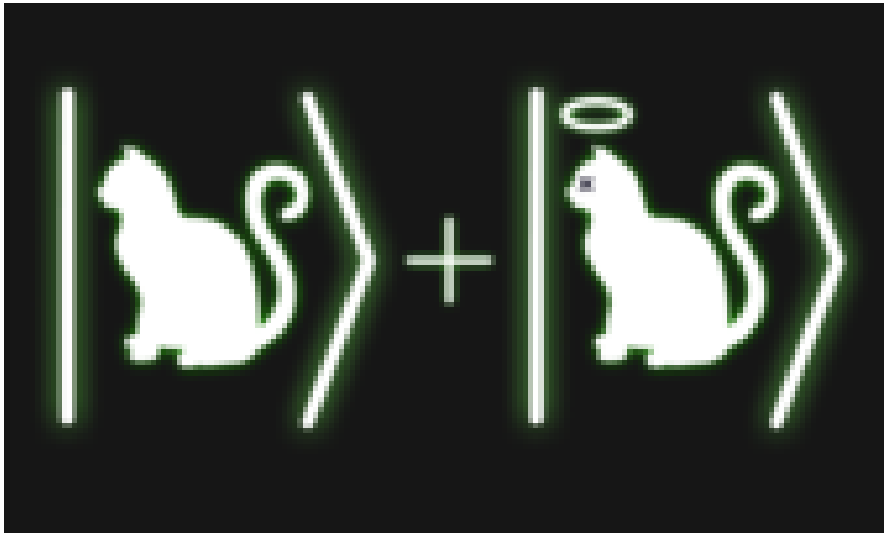
- MTG, which was founded in 1995, is a high tech software company based in the Rhein-Main region (Darmstadt, Germany) – the Germany IT security cluster.
- MTG is a leading expert for encryption technologies in Germany. MTG's IT security solutions effectively secure critical infrastructures and the Internet 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!

Schrödingers Cat

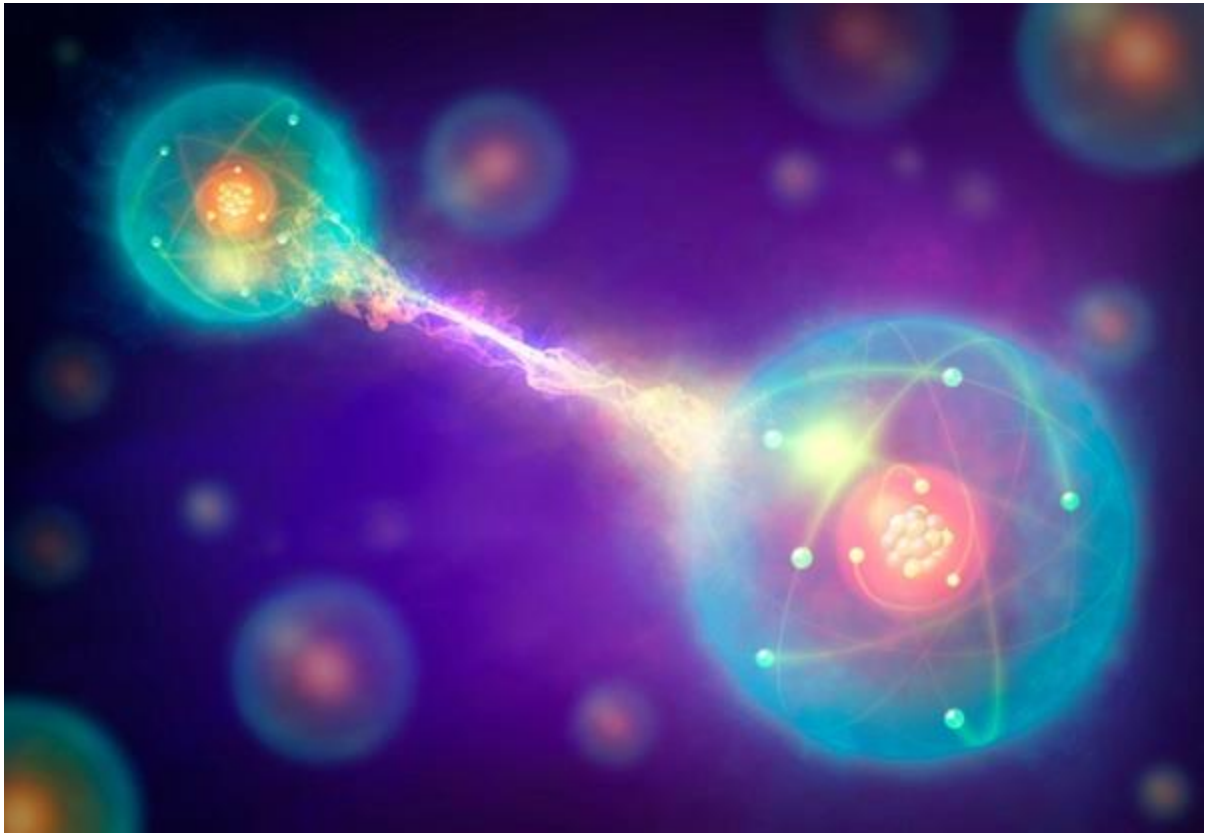
http://www.einfachtierisch.de

Quantum Superposition



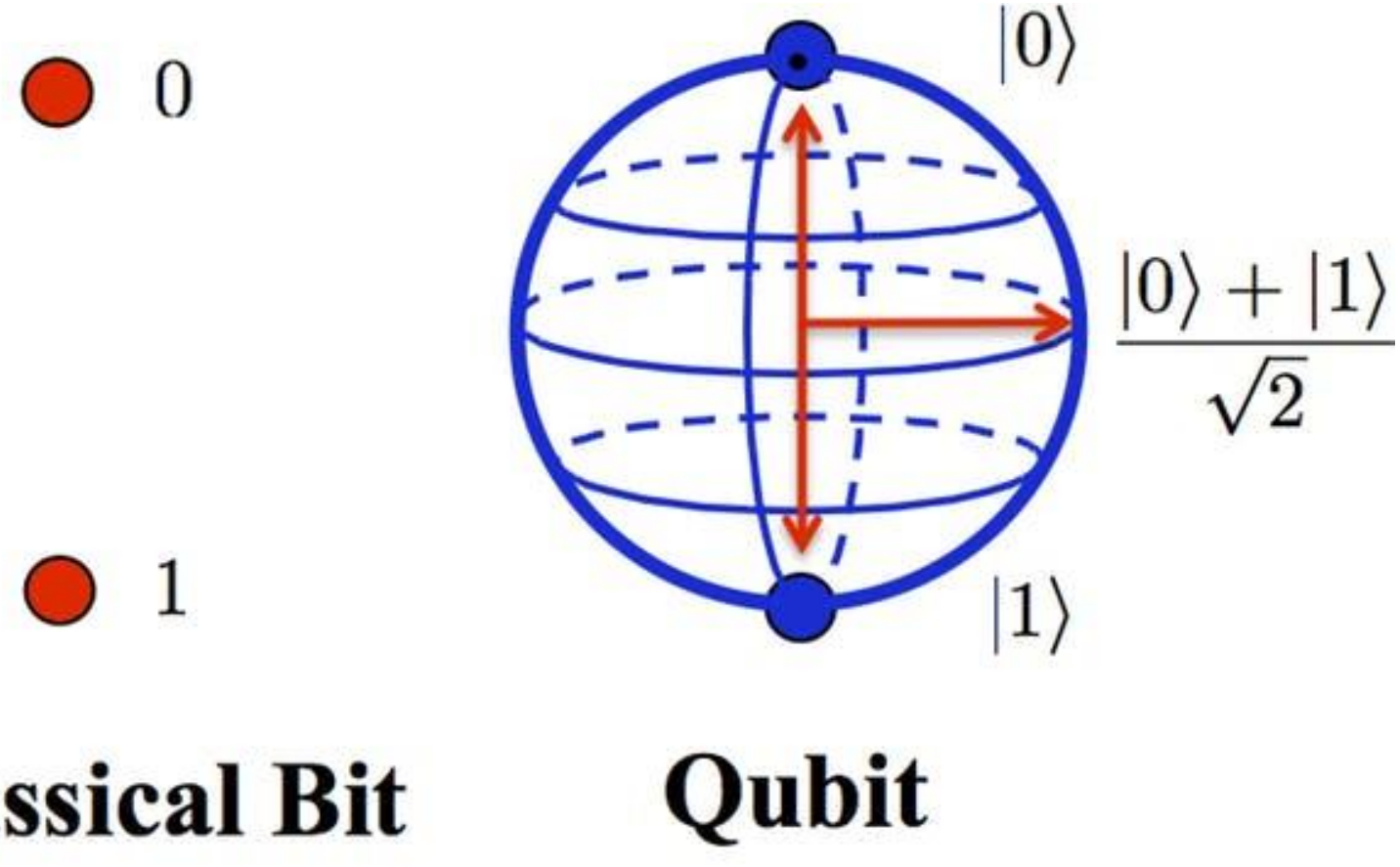
https://brilliant.org/courses/quantum-computing/

Quantum Entanglement



http://www.astronomy.com/news/2018/08/distant-quasars-confirm-quantum-entanglement

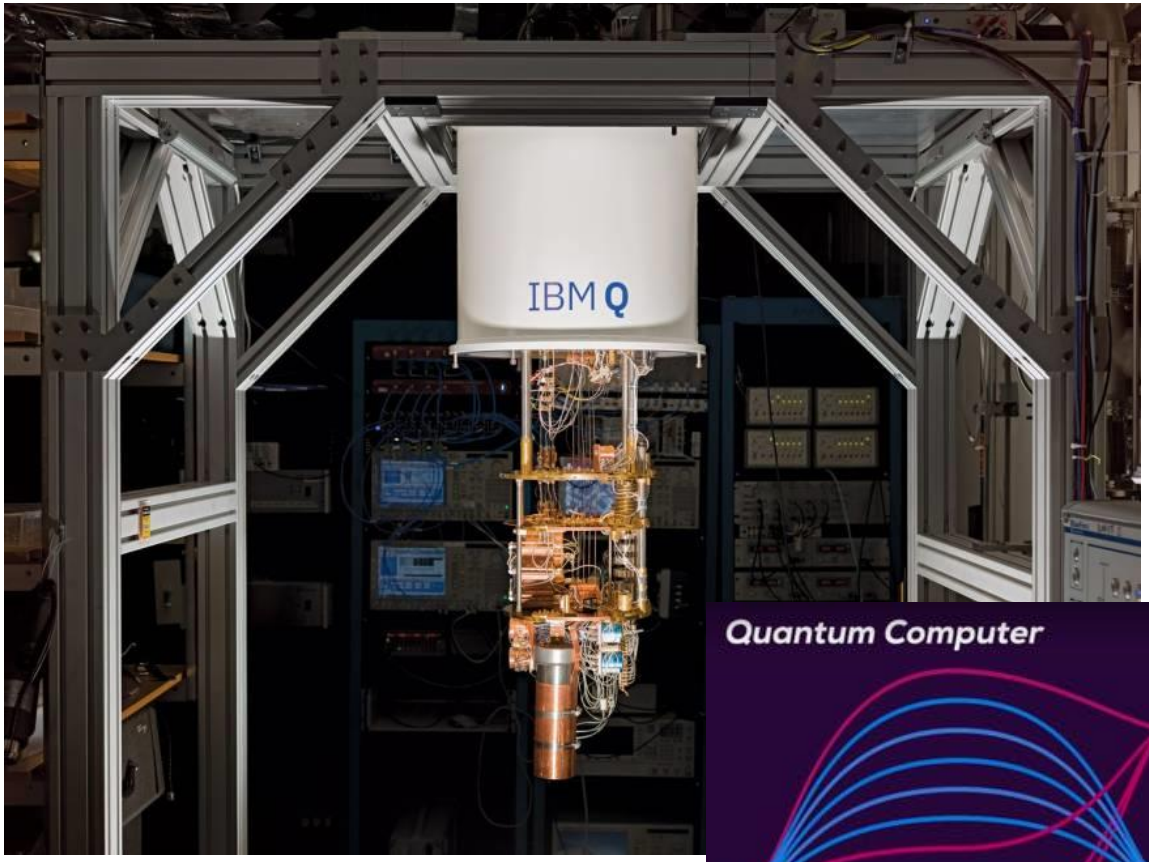
Qubits



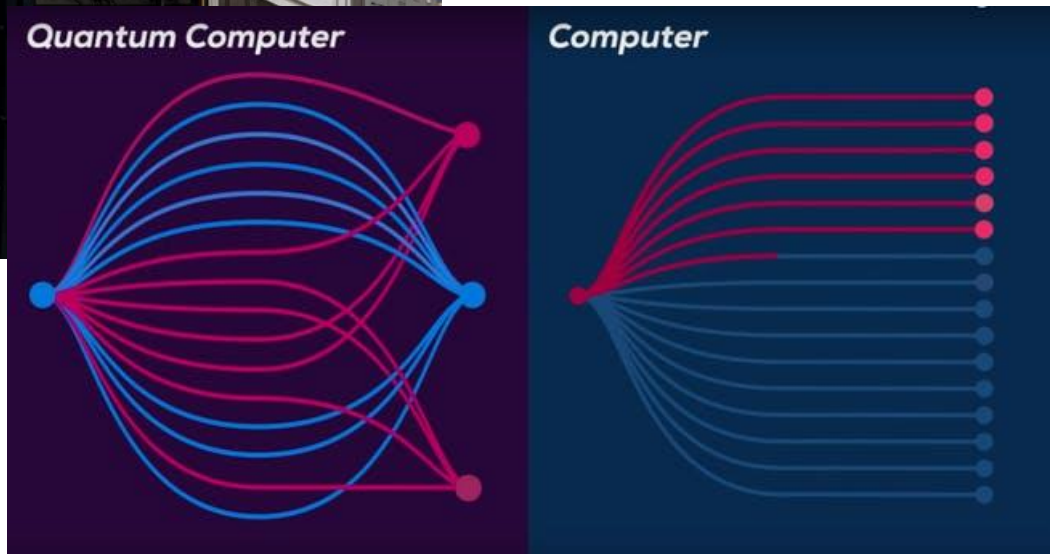
https://www.inverse.com/article/38860-quantum-computers-are-almost-here

- 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

Quantum Computers



https://www.japantimes.co.jp/news/2017/06/16/business/tech/quantum-computing-machines-tomorrow/



https://www.inverse.com/article/38860-quantum-computers-are-almost-here

Key Driver for Quantum Computing

Pictures: Unsplash

https://www.ibm.com/thought-leadership/technology-market-research/quantum-computing-report.html

Effects of quantum computers on today's cryptography

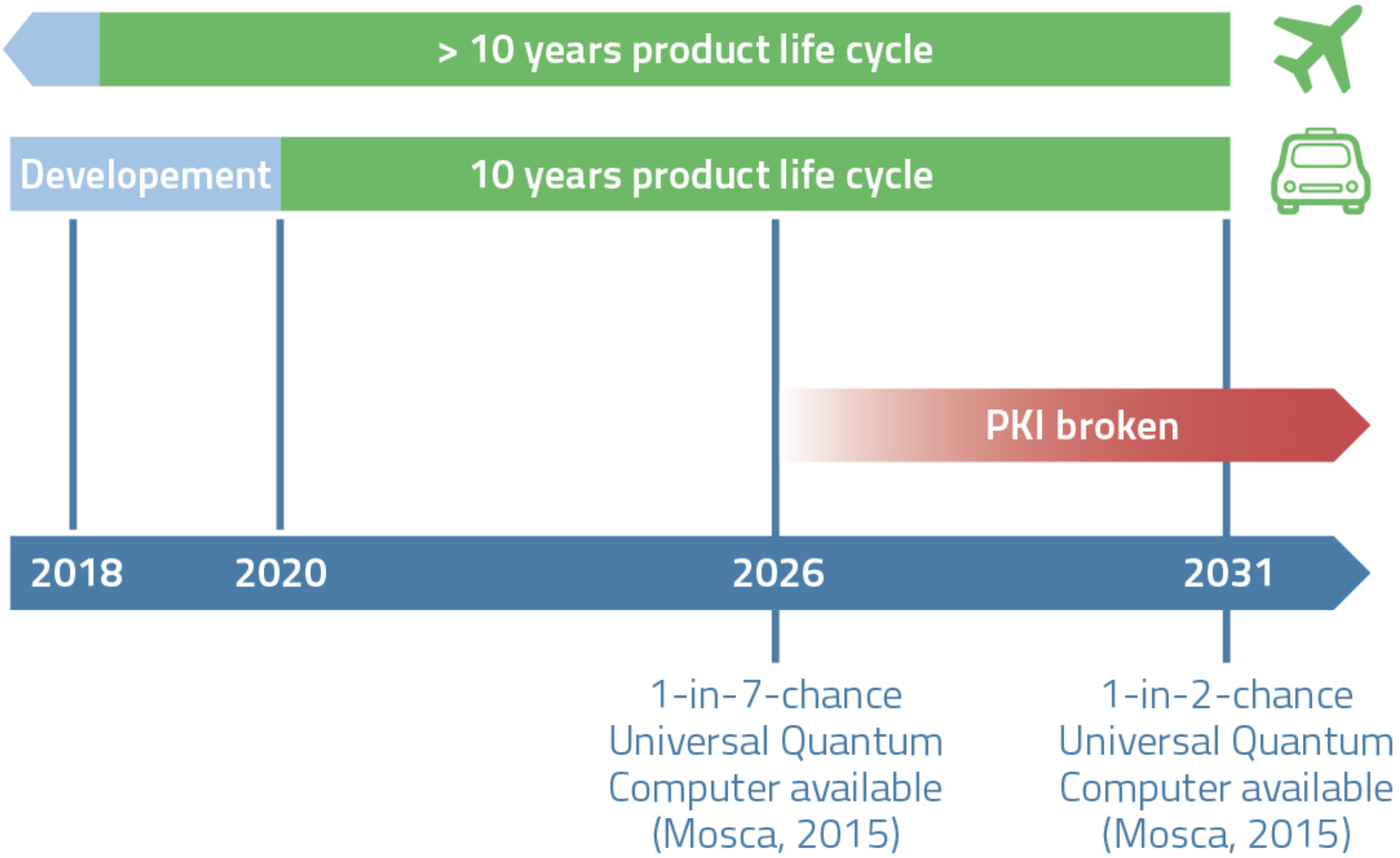
Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC256	128		
	ECC 521	256		
Symmetric	AES128	128	64	Grover's Algorithm
	AES 256	256	128	

Resource Estimates for Shor's Algorithm

Algorithm	#Qubits
RSA 1024	2050
RSA 2048	4098
ECC 256	2330
ECC 521	4719

Quelle: Roetteler, Martin et al. "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms." ASIACRYPT (2017).

Quantum impact

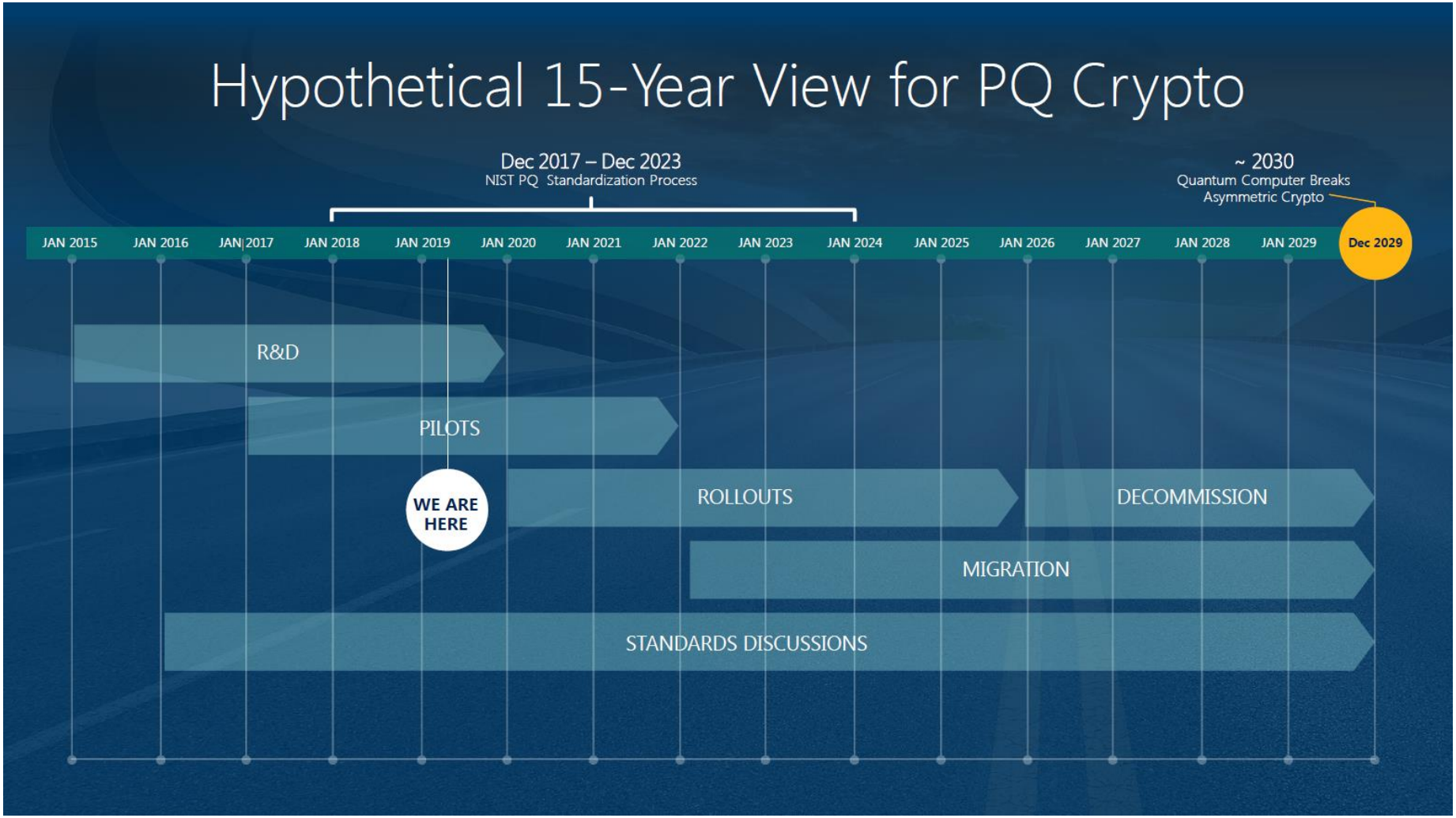


Post Quantum Cryptography (PQC) to the Rescue!

MTG

- NIST Post-Quantum Standardization Project
- Goal: find algorithms based on different mathematical problems that are not vulnerable to known quantum attacks
- Started on Nov 30, 2017 → finish in 2023
- ~ 70 submissions from around the world
- Primitives used:
  - code-based
  - lattice-based
  - hash-based
  - Multivariate
  - super singular elliptic-curve isogenies
- NIST & crypto community now engaged in cryptanalysis
- NIST expected to pick multiple “winning” algorithms

- Current Status: Round 2
  - 17 key encipherment (encryption) algorithms
  - 9 digital signature algorithms



https://hsm.utimaco.com/wp-content/uploads/2019/05/20190516-Utimaco-webinar-Post-Quantum-Cryptography_The-Perspective-of-Brian-LaMacchia_Microsoft-slides.pdf

Crypto Agility

„The ability for an IT system to gracefully and securely exchange crypto primitives, with minimum down-time, no migration periods, and complete visibility on used primitives.“

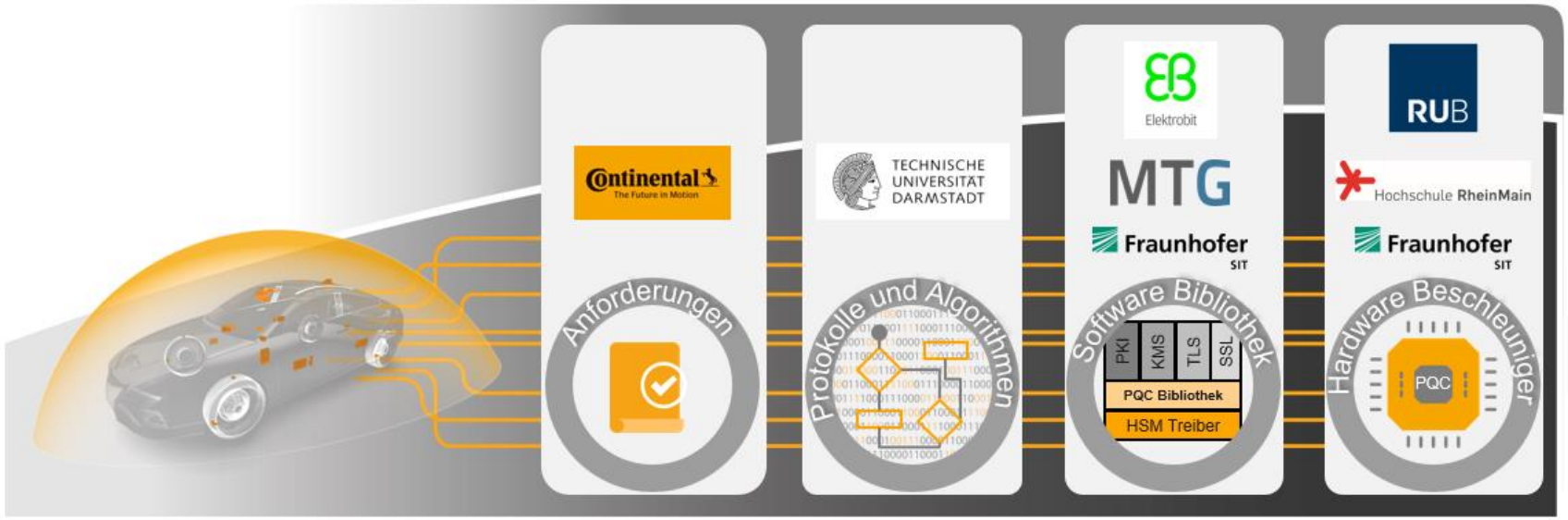
https://cloakable.irdeto.com/2018/06/21/cryptographic-agility/

Why?

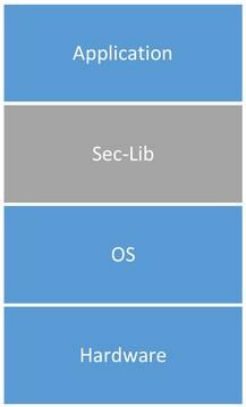
- Different PQC algorithms for different use cases
- Algorithms can be proven insecure
- New more effective/secure algorithms can be developed

PQC Research Projects

QuantumRISC



Use-A-PQClib

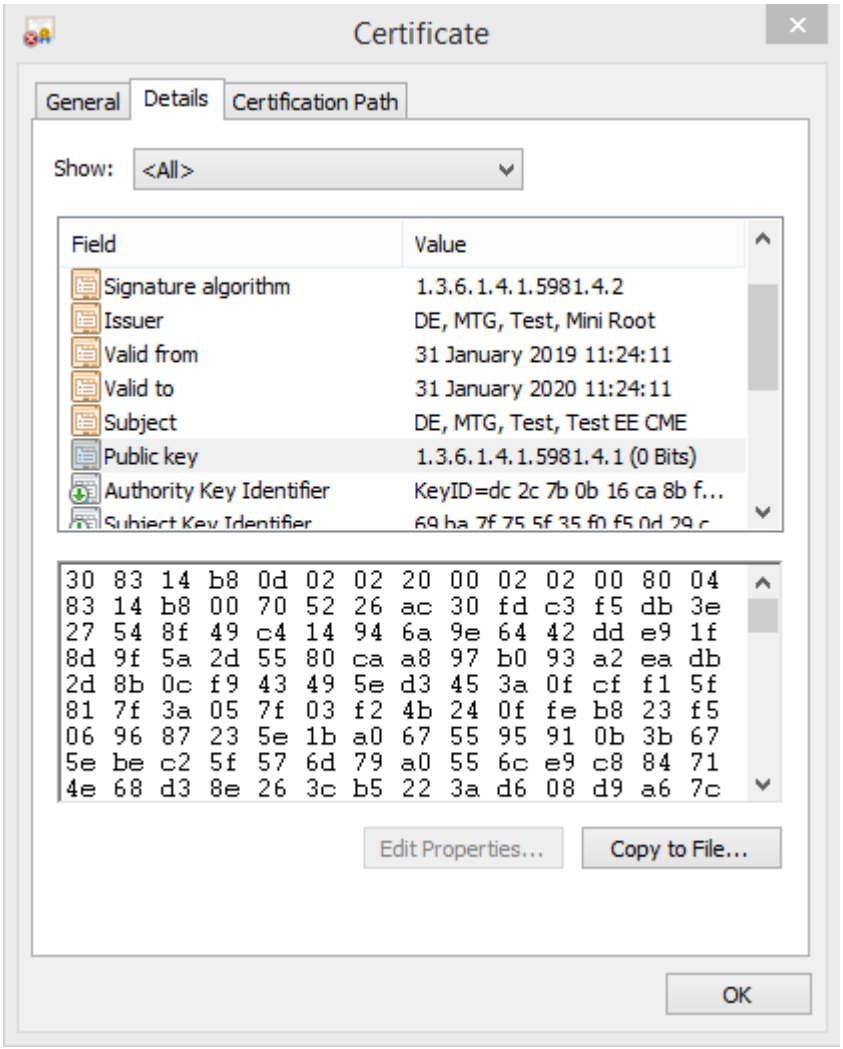


h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Integrate Post-Quantum Cryptography now!

Real World PQC Applications

PQC Certificates

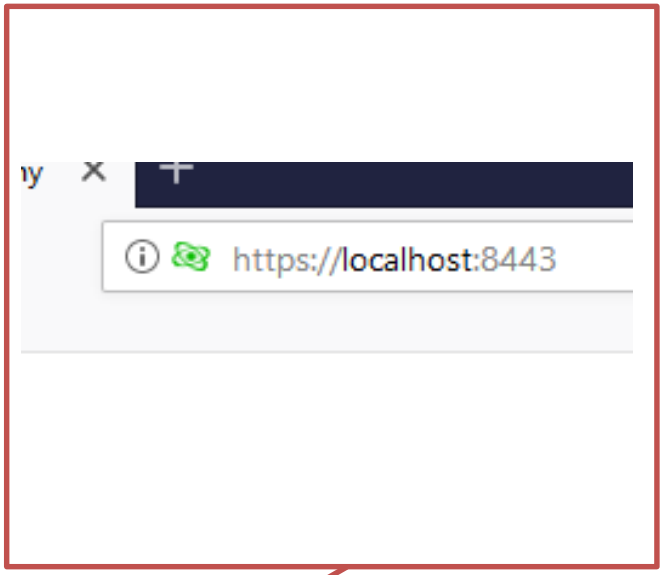


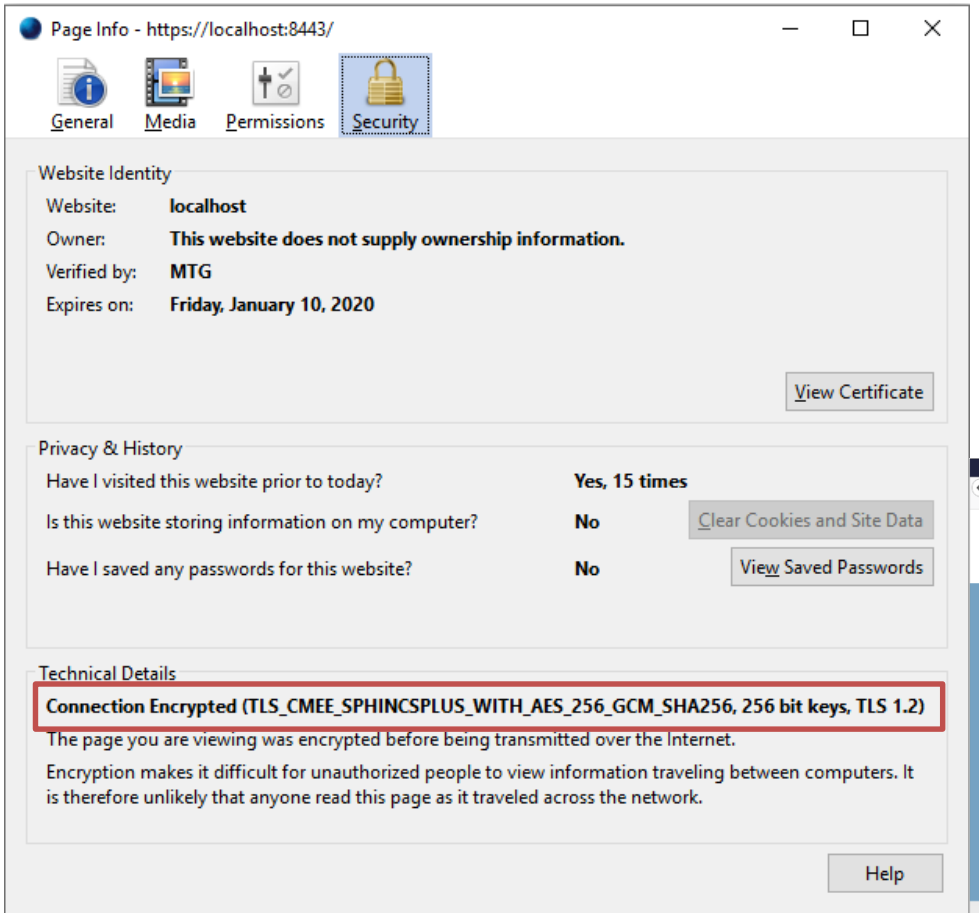
- Classic McEliece Public Key
- Sphincs Plus Signature
- No standardized OIDs
- No standardized ASN1 Structures
- Most applications cannot handle:
  - Large key sizes (1,4 MB)
  - Large signature sizes (50 KB)

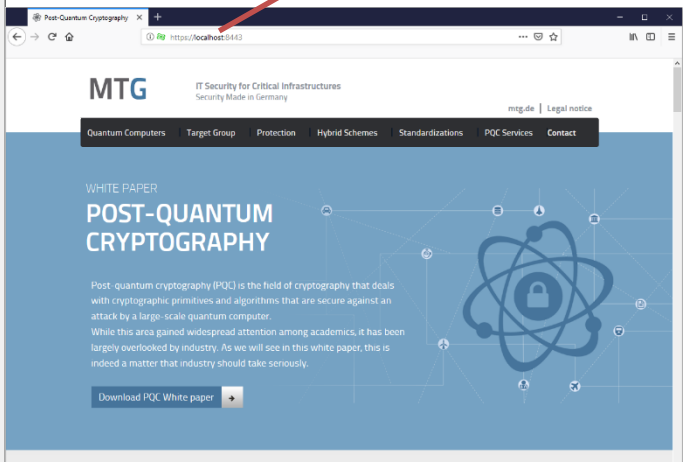
Challenges for a Real World PQC PKI

- No standardized PQC Algorithms
- No standardized encoding for keys and algorithm parameters
- Large key sizes (1,4 MB)
- Large signature sizes (50 KB)
- Keys and Certificates stored in databases...
- Existing software written with no flexibility in mind
- Restrictions through variable types…
- Communication overhead for large keys and certificates
- The whole system needs to use PQC (Webserver, Web browser, HSM, etc.)
- Many existing tools and solutions decide to wait for standards…

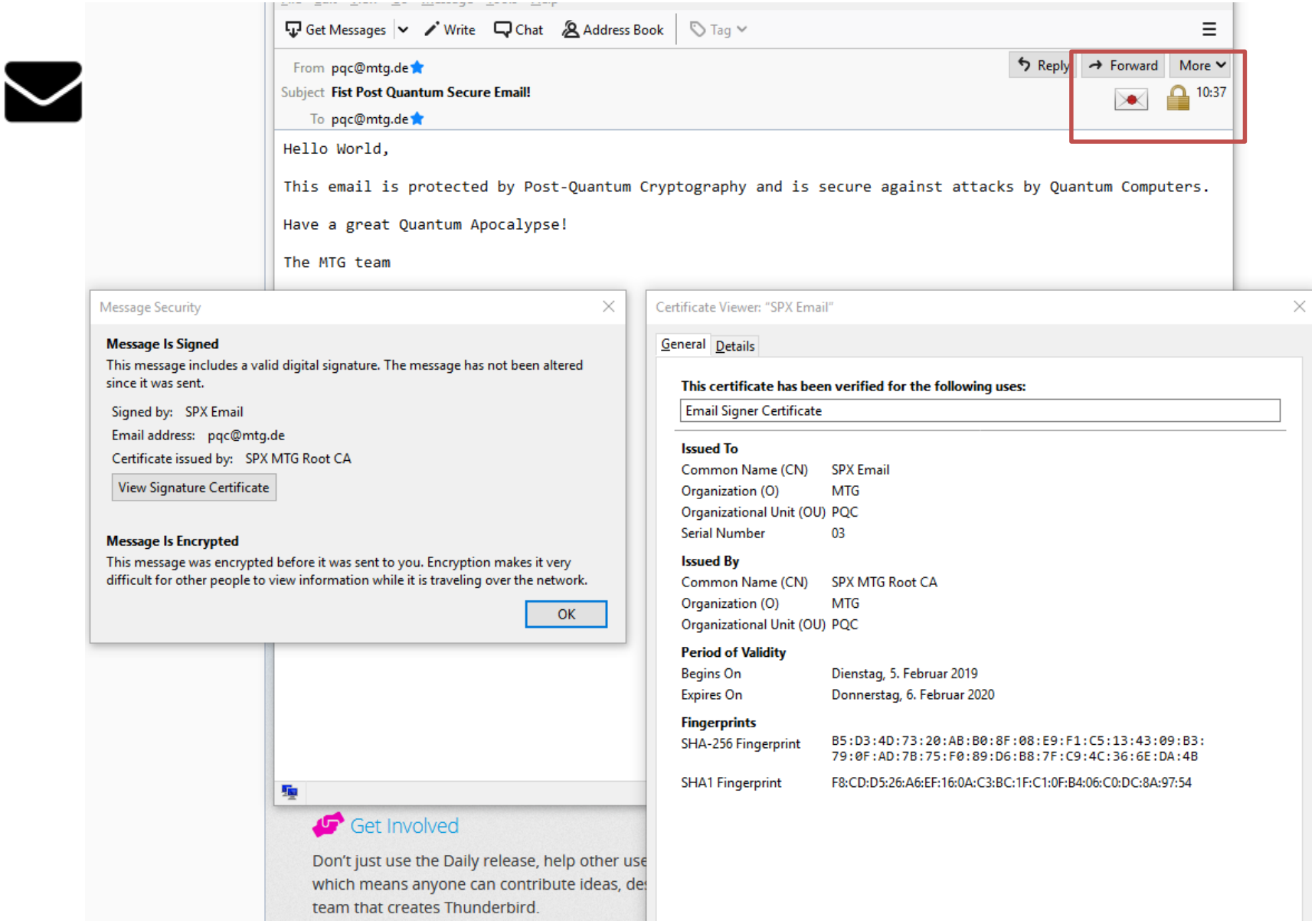
Use Case: PQC Web Browser & Web Server







Use Case: PQC Email Client



Conclusion

- PQC transition must start today!
- There are new challenges and requirements!
- Most of today's IT infrastructures and systems are able to use PQC!
- What role could the European Bridge CA play in the adaptation of PQC?

Contact

Stathis Deligeorgopoulos

sdeligeorgopoulos@mtg.de

+ 49 6151 8000 40