«VOI» TeleTrusT Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 22.09.2020

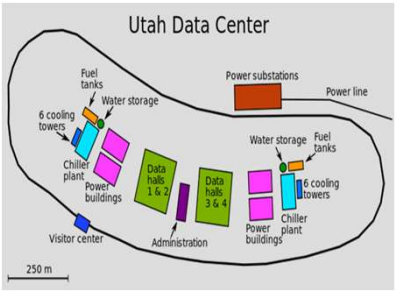
Krypto-Agilität

Christian Seegebarth

D-Trust GmbH

1. Quantum Impact

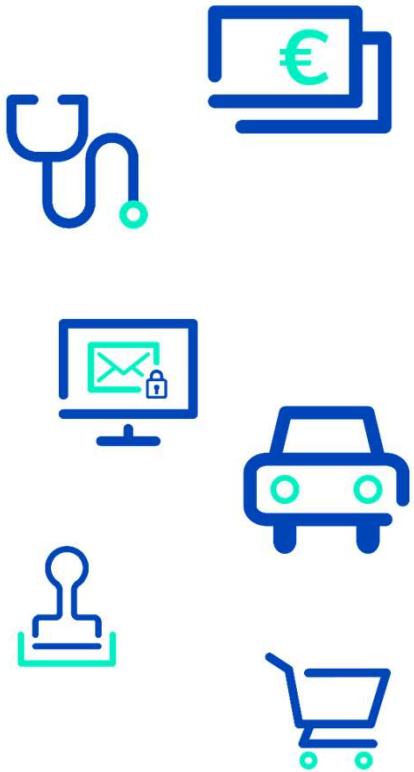
- Ein Quantencomputer genügender Stärke bricht heutige verbreitete asymmetrischen Algorithmen RSA, ECC, DH, ECDSA ….
- NSA baut in Utah eine Super Cloud 140 – 420 TB pro Person der Weltbevölkerung
- Symmetrische Algorithmen, wie AES sind nicht so stark betroffen, da hier eine möglicherweise eine Verdoppelung der Schlüssellänge ausreicht und die nötige Sicherheit wieder herzustellen



2. Welche Geschäftsprozesse sind betroffen

- TLS (z.B. Browserkommunikation)
- VPN Installationen (Telematik Infrastruktur, Behördennetzte, …)
- Mailverschlüsselung, DE-Mail, BeA, EGVP, eANV, …
- Reisepass, Personalausweis und andere notifizierte eIDAS Systeme
- Zeitstempel
- Qualifizierte Signaturen, qualifizierte Siegel
- Archive zur Beweiskraftbewahrung (TR-ESOR)

➔ gesamte Vertrauensinfrastruktur der Digitalisierung gefährdet



3. Was kann man dagegen tun

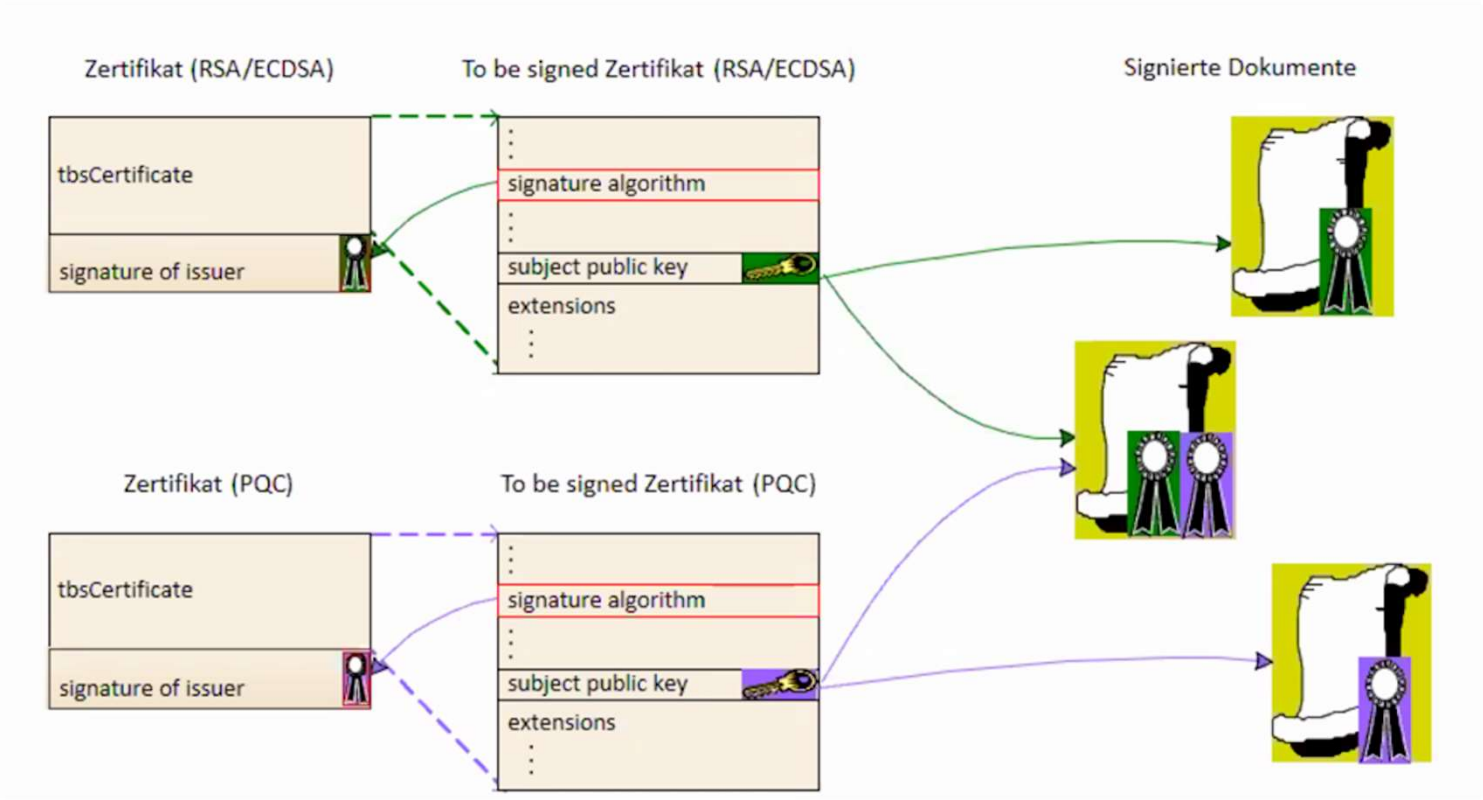
- Entwicklung neuer Algorithmen, Verwendung von schon bekannten Quanten resistenten Algorithmen
  McEliece, SPHINCS(+), XMSS (rfc 8391), NewHope u.a.

- Anforderungen sind je nach Use Case zu betrachten
  - große/kleine Schlüssel,
  - Robustheit/Geschwindigkeit der Implementation

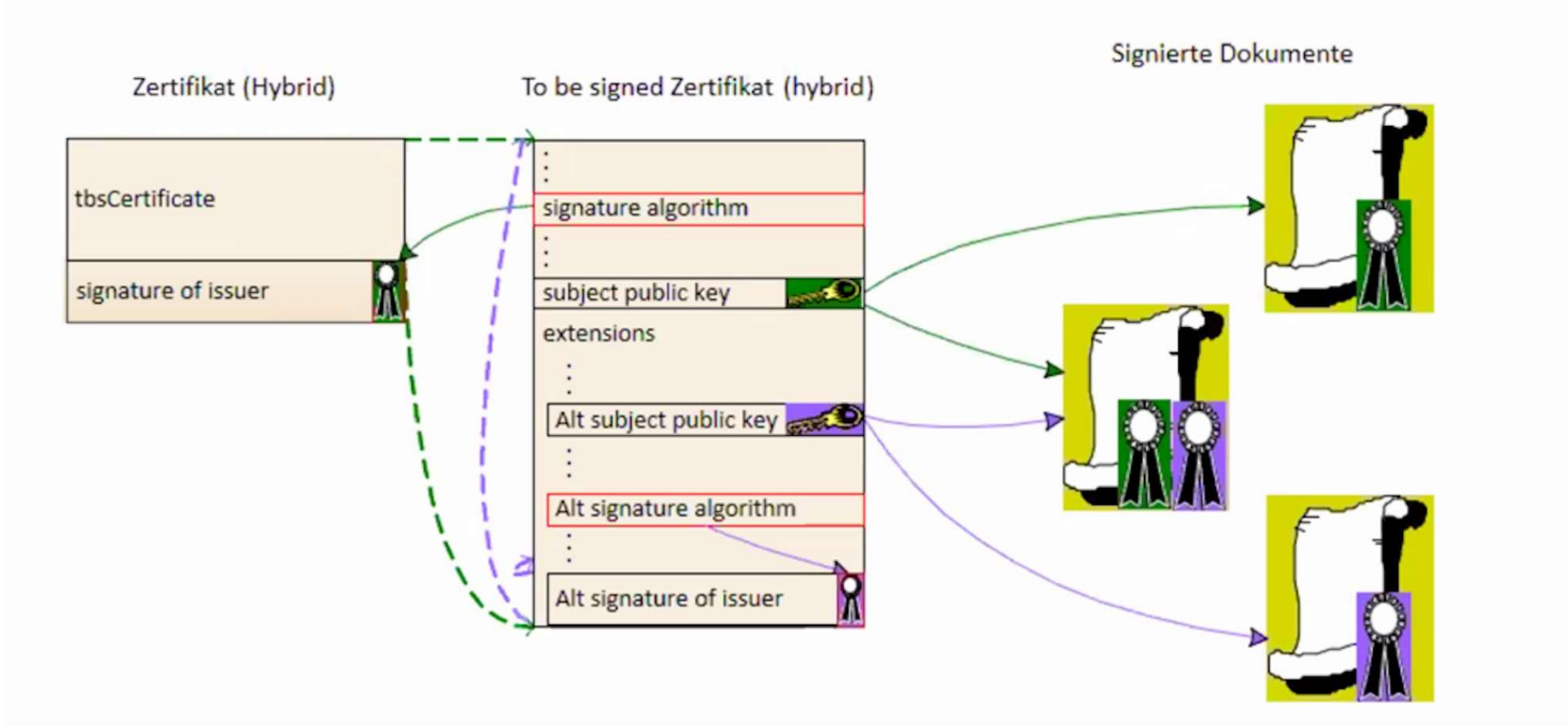
- Wichtig ist die Standardisierung
  z.B. rfc 8391 (XMSS) oder NIST (post-quatum crypto project)

- Wie kann eine Migration aussehen
  hybride Zertifikate oder parallele PKIen

Parallele PKI Systeme



Hybride Zertifikate



Initiativen

- **Wer engagiert sich heute im Bereich Quantum Computing / Post-Quantum Kryptographie**
  - NIST Wettbewerb (Request for Post-Quantum Cryptography Standardization)
  - ETSI (TC Cyber)
  - EC (Flagschiffprojekt 1 Mrd. EUR in 10 Jahren),
    - quantum communication
    - quantum simulation
    - quantum computing
    - quantum metrology and sensing
  - Bundesrepublik (650 Mio)
  - …
- **Was machen wir (Bundesdruckerei Konzern)**
  - PQ Crypto
  - squareUP Hash-Basierte Signaturen -> rfc 8391
  - QuaSiModO (Quanten-Sichere VPN-Module und - Operationsmodi)
  - FLOQI (Full- Lifecycle Post Quantum PKI)

FLOQI - Full Lifecycle Post-Quantum PKI

Projekt Rahmen

Bundesanzeiger vom 22.08.2018: "Post-Quanten-Kryptografie" im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit "Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020".

Inhalt

Im Projekt FLOQI werden neuartige Konzepte, wie hybrid und parallel betriebene PKIen hinsichtlich quantenresistenter Verfahren und Krypto-Agilität für die Absicherung von zukünftigen Produktionsanlagen, Finanznetzwerken und Fahrzeug-Kommunikation erforscht und an Demonstratoren der Verbundpartner erprobt.

FLOQI –
Full Lifecycle
Post-Quantum PKI

FLOQI - Full Lifecycle Post-Quantum PKI

- **Schwerpunkte: Bundesdruckerei/D-Trust GmbH**
- Betreiben und Migrieren von PKIen, um sie flexibel und Quantencomputer-Sicher zu betreiben
- Untersuchung der möglichen Algorithmenkombinationen in PKIen
  - Beachtung der spezifischen Anforderungen aus den einzelnen Use Cases unserer Partner
  - Performance-Untersuchungen
- Aufbau und Bereitstellung aller PKIen
- Spezifikation paralleler & hybrider Zertifikatsstrukturen/PKIen

FLOQI - Full Lifecycle Post-Quantum PKI

- **Status Ende 2020**
- Algorithmen untersucht auf Performance, Speicherplatzbedarf– meist embedded
  (NIST 3. Runde Finalisten + XMSS)

- DTR untersucht PKI Betriebserhaltung PKI
  Ziel Austausch Algorithmen im laufenden Betrieb) – Krypto-Agilität
  Zertifkate (root, subCA ,Endbenutzer) z.B Root mit XMSS, SubCA (ongoing)

- Untersuchung Hybride PKI (ongoing) Kooperation mit QuantumRISC
  - Verhalten von verschiedenartigen Algorithmen innerhalb einer PKI
  - Laufzeitverhalten der PKI Ebenen in verschiedenen Use Case (TLS, Signatur)

FLOQI - Full Lifecycle Post-Quantum PKI

- **Ausblicke (in Planung)**
- Praktische Umsetzung der PKI
- Botan (lib) update, wolfSSL update
- Unterstützung der Standardisierung IETF (RFC erstellen), ETSI

Christian Seegebarth
Senior Expert Trusted Solutions
E-Mail: c.seegebarth@d-trust.net
Telefon:+49 (30) 25 98-3942

D-TRUST
Ein Unternehmen der Bundesdruckerei

Vielen Dank.