TeleTrusT
Pioneers in IT security.

TeleTrusT-Konferenz 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 28.11.2019

Kryptoagilität

Dr. Kim Nguyen,

Managing Director (CEO) - D-Trust GmbH

Fellow – Bundesdruckerei GmbH

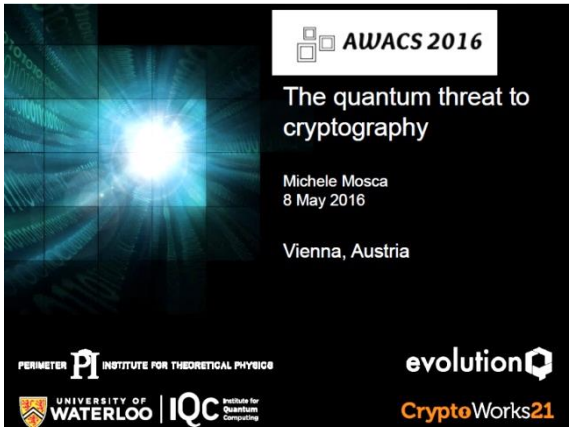
Aktuelle Entwicklungen in der praktischen Kryptographie

- RSA immer längere Schlüssel
- 3072 Bit → ROCA
- Entwicklung zu ECC hat 20 Jahre gedauert
- Neue Technologie: Quantencomputer
- Die Entwicklung der Quantencomputer entspricht heute nicht Moore‘s Law, stattdessen Verdoppelung alle 12 Monate
- Seit 1994 Shor‘s Algorithmus

Wann wird es kritisch?

- x – Lebensdauer kryptografischer Schlüssel
- y – Zeitspanne zur Einführung neuer Algorithmen
- z – Zeit bis zur Verfügbarkeit von Quantencomputern mit nötiger Qubit-Breite

- Mosca‘s Theorem:
  „If *x* + *y* > *z*, then worry.“



- Beispiel: CN = csca-germany, SN = 103
  Gültigkeit 23. August 2016 - 24. Februar 2030 -> x > 15 Jahre
- Standardisierung Kryptografie + ICAO + Implementierung: -> y >= 5 Jahre ?
- Mosca [NIST April 2015, ISACA September 2015]:
  “1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031” -> *z* < 13 Jahre

Derzeit ist Kryptographie sehr statisch

- Minimale Änderungen benötigen zu viel Zeit
- Neue Algorithmen waren lange standardisiert
  - MD5 wurde 1991 veröffentlicht → 1993 erste Angriffe → 2004 Tool MD5CRK → wird in Teilen jedoch heute noch verwendet
  - SHA1 wird bis heute abgelöst, obwohl spätestens seit 2006 gebrochen

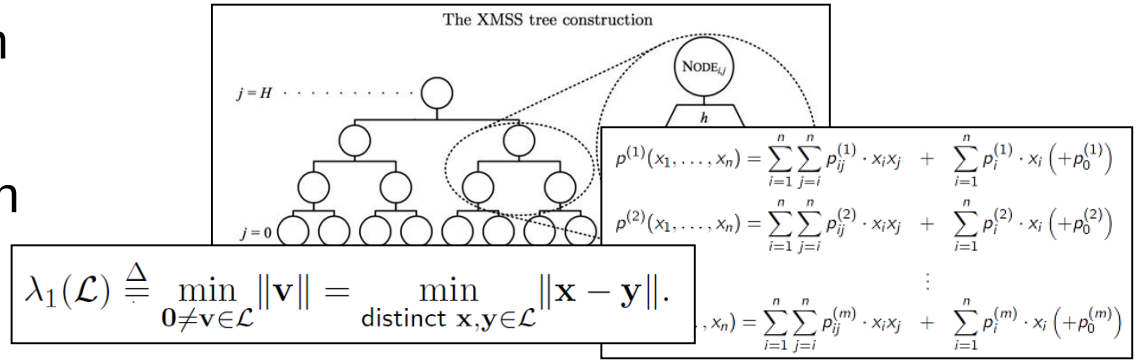
Reicht die Annahme y = 5Jahre? Also z = 13 Jahre?

1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031

Post Quantum Cryptography

- beschäftigt sich mit asymmetrische Kryptoalgorithmen, die (vermutlich) Angriffen mit Quantencomputern widerstehen
- Algorithmen für
  - Verschlüsselung,
  - Schlüsselvereinbarung und/oder
  - Signatur

- Klassifizierung nach mathematischen Problemen
  - Hash-basierte Signaturen
  - Gitterbasierte Probleme
  - Multivariante Gleichungen
  - Codingtheorie
  - Isogenien



Stand NIST Wettbewerb: Ziel und Zeitplan

- Start: 03.01.2017
- Deadline of Submisson: 30.11.2017

- Ziel: Quanten-Computer resistente kryptografische Algorithmen (PQC) als Federal Information Processing Standards Publication (FIPS) oder Special Publications (SPs).
- Methode: Evaluierung via multiple Runden über 3-5 Jahre
- Beteiligung: 69 Kandidaten

Kann man in der PKI RSA/ECDSA dann einfach ersetzen?

- Herausforderungen, u.a.:
- Oft: Entweder Signaturen oder Verschlüsselung
- Stateful Hash-based signatures: Nicht mit heutigen Smartcards, Nicht in loadbalanced Systems
- Smartcards und HSMs für PQC: Verfügbarkeit noch nicht da

Einschätzung:

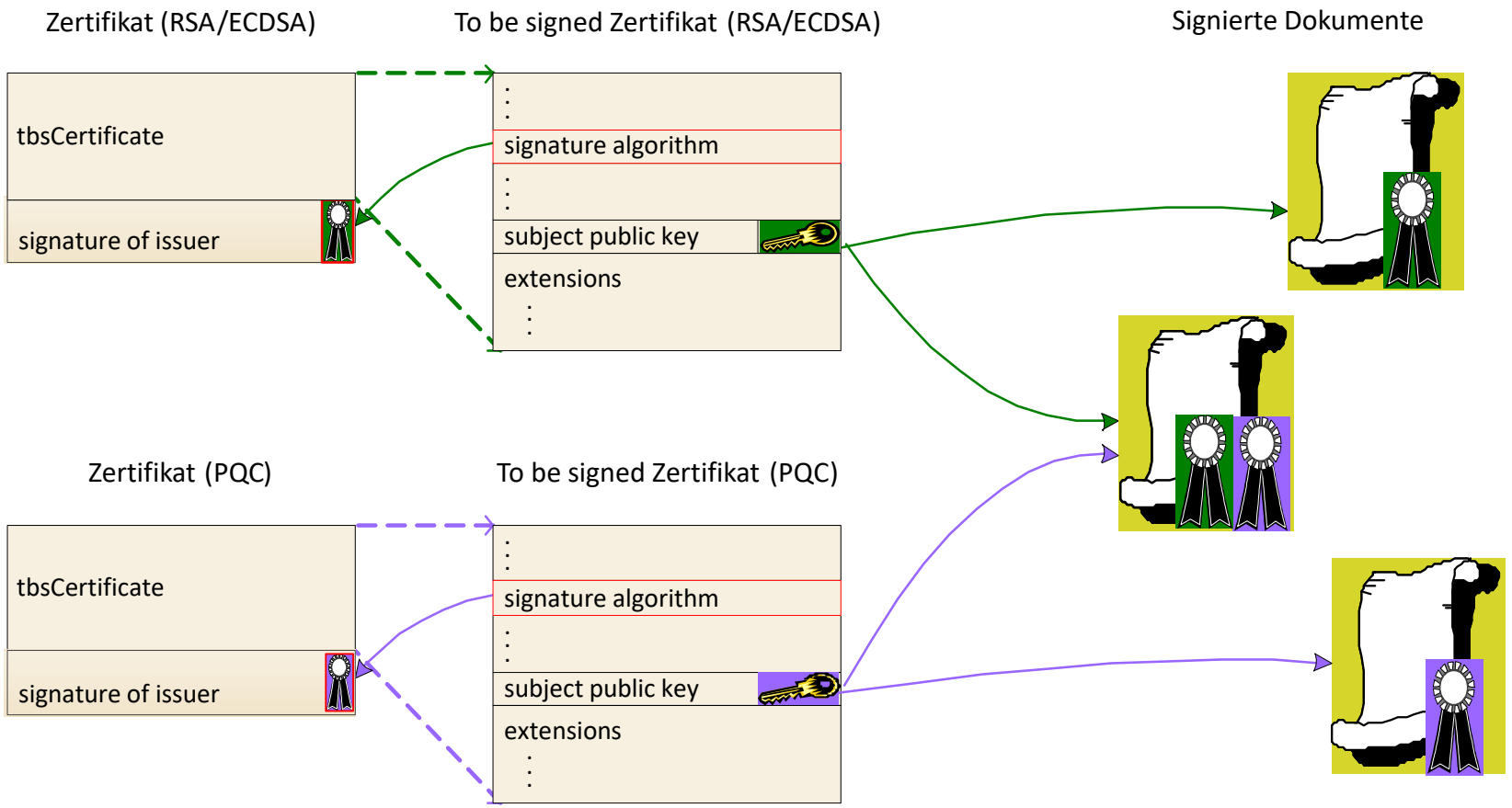
- „private“ Anwendungen: JA
  Anwendungen unter Kontrolle des PKI-Betreibers, z.B. SW-Updates
- „öffentliche“ Anwendungen: Erst nach Standardisierung
  Das dauert vielleicht zu lange!

Einsatz von PQ-Algorithmen

- X.509-Zertifikate mit PQ-Algorithmen grundsätzlich möglich
  - Aber: Größe der Schlüssel
  - Aber: Größe der Signaturen
- Grundsätzliche Gestaltung der PKIen könnte erhalten bleiben
  - Organisation der Schlüssel bei „Einmal-Schlüsseln“ ist zu lösen
- Geschäftsmodelle könnten grundsätzlich fortgeführt werden
  - Aber: Zeitpunkt der Verfügbarkeit von Smartcards mit PQ-Algorithmen nicht klar
- Sicherung bestehender Daten
  - PQ-Zeitstempel
  - Sicherung der eigenen Archive und der Archive Dritter

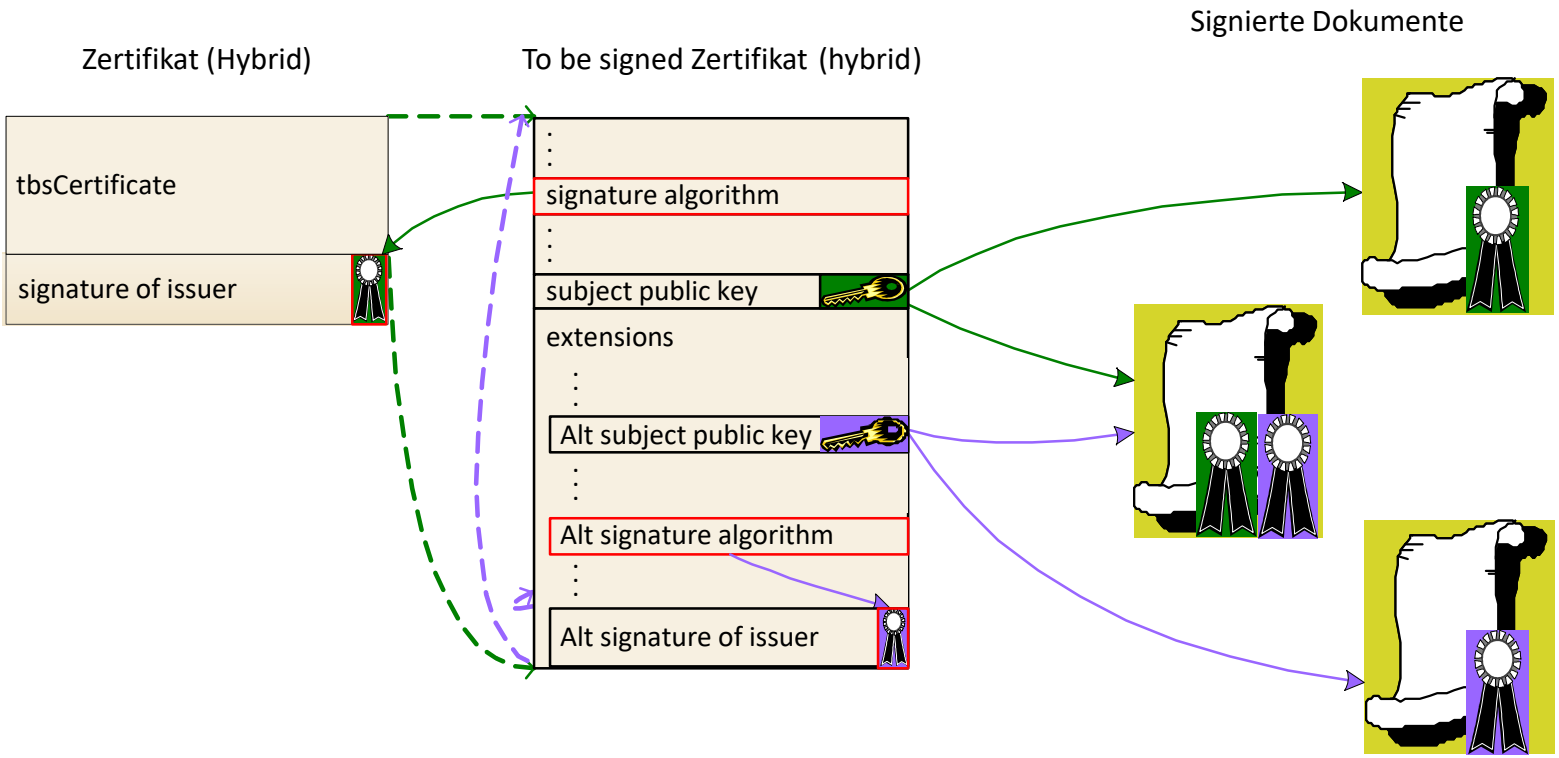
Migration zur quantum-resistenten PKI

1. Ansatz - Zwei oder mehr PKI parallel betreiben



Migration zur quantum-resistenten PKI

2. Ansatz - Hybridansatz



Quantencomputer - Was wird aus der PKI?

Ansatz paralleler PKI-en und Hybridansatz können allgemein für **Kryptoagilität** benutzt werden.

- Dokument wird als echt und unverfälscht akzeptiert, wenn wenigstens eine Verifikationskette vertrauenswürdig ist.
- Vertraulichkeit wird durch Doppelverschlüsselung erreicht,
  z.B. im klassischen TLS-Kanal werden PQC-Verschlüsselte Daten übertragen.

Neue Use Cases benötigen sehr viel Agilität

- nach eIDAS werden Algorithmen in verschiedenen EU-Ländern zwar unterschiedlich bewertet – gültig ist immer die Bewertung des Herkunftslandes einer Signatur
  - Frage: RSA 2048 wird in Schweden & Deutschland wie lange als gut bewertet? (insgesamt 28 Mitgliedstaaten)
  - Frage: Wer bewertet im Prüf-Land eine Signatur nach Maßgabe des Herkunftslandes bzw Herkunftsländer
- Roll over: Migration von Einer zur anderen PKI mit Algorithmuswechsel
  - Link Zertifikate zu verschiedenen PKIen mit verschiedenen Algorithmen (1 zu N Beziehung)
  - Akzeptanz in anderen Ländern
- Verifikation: das Ergebnis kann je nach Algorithmus verschieden sein
  - Beispiel: an einer Datei ist die RSA Signatur gut, Dilithium schlecht
  - Wird ein Ranking von Algorithmen benötigt?

Neue Use Cases benötigen Agilität

- Flexibilität: Algorithmuswechsel innerhalb einer PKI
  - Für unterschiedliche Anwendungen z.B. Nutzung für die Root (lange Laufzeit), im Bereich IoT (kleine Schlüssel) und TLS (viele Schlüssel)
  - Unterschiedliche Infrastrukturen wie LAN-HSM oder Sensor
- Laufzeiten von Algorithmen: in einem Bewahrungsdienst müssen Signaturen, Zeitstempel, Hash-Trees/Chains parallelisiert und getrennt von Content gespeichert werden
- Verschlüsselung als „Matroschka-Anwendung“
  - Tunnel im Tunnel (HTTPS, VPN)
  - ECC verschlüsselter AES Schlüssel → mit SIKE nochmal verschlüsselt

Fazit

- Kryptoagilität ist wesentlich für die Zukunftssicherheit von kryptographischen Anwendungen
- Quantencomputer und PQC sind nur ein weiterer Aspekt, der dies verdeutlicht
- Kryptoagilität muss ein verpflichtendes Element von zukunftssicheren SW Architekturen sein/werden!