Migration zu einer quantensicheren Verwaltungs-PKI

Dr. Kaveh Bashiri, Dr. Stavros Kousidis, OMNISECURE, 24. Mai 2023

Die Verwaltungs-PKI (V-PKI)

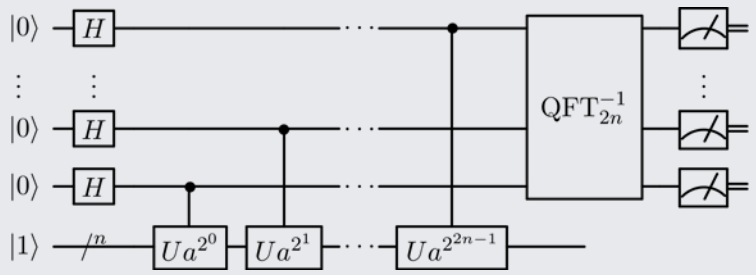
- Ziel: Bereitstellung vertrauenswürdiger Identitäten in der öffentlichen Verwaltung

- Größenordnung: 6 Sub-CAs, ca. 500.000 Subscriber
- Algorithmus: RSA
- Anwendungen: S/MIME, TLS und weitere Standardanwendungen

Quantencomputer und ihre kryptografischen Auswirkungen

Shor (1994)

Quantencomputer würden die heute verwendeten Public-Key-Verfahren (RSA, ECC,…) brechen.



Rechtzeitige Migration zu einer quantensicheren V-PKI notwendig!

Quantensichere V-PKI – Auswahl der Signaturverfahren

Kriterien bei der Auswahl:

- Sicherheit
- Performance
- Interoperabilität und Kompatibilität mit Standardanwendungen

Kandidaten:

Algorithmus	Pro	Contra
XMSS, LMS	• Gut verstandene Sicherheitseigenschaften • Performance (insb. Signatur- und PK-Größe)	• Verwaltung des Zustands (!)
SPHINCS+	• Gut verstandene Sicherheitseigenschaften	• Performance
CRYSTALS-Dilithium in Kombination mit ECDSA	• Bessere Performance als SPHINCS+ • Vsl.: Kompatibilität mit Standardanwendungen	• Strukturierte Gitter (?)

Quantensichere V-PKI – Zertifikatsgrößen im Vergleich

Algorithmus	(Signatur+PK)-Größe in Kilobyte
RSA4096	1
Dilithium3 & ECDSA-384	5.5
SPHINCS+-192s	14.5
SPHINCS+-192s (reduced)	8
LMS-H20-192-W8	1.1
HSS-H5/H15-192-W8	1.8

LMS-H20-192-W8 für die Root-CA-Ebene?

Quantensichere V-PKI – Weitere Kriterien

Zertifikatsgestaltung:

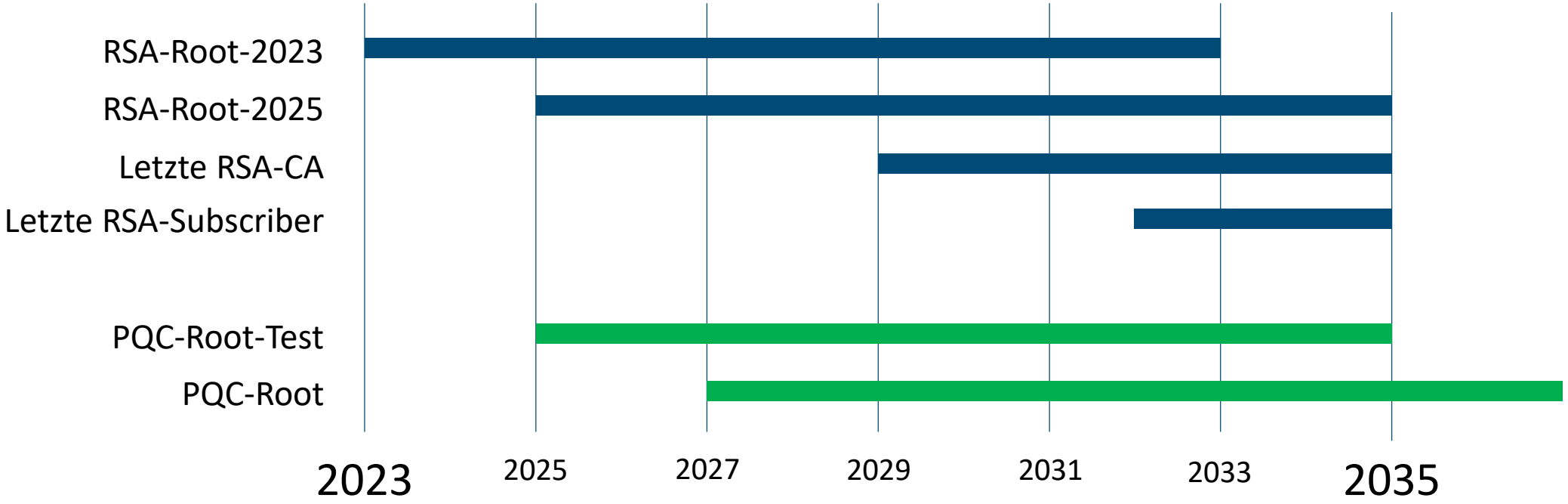
- Getrennte Signatur- und Verschlüsselungszertifikate
- Standardisierung der Post-Quanten-Verfahren in gängigen Zertifikatsformaten
  → Kooperation BSI & genua GmbH für X.509-Zertifikate

Migrationskonzept:

- *Paralleler Ansatz*:

→ Unterbrechungsfreier Übergang ohne Stichtagsumstellung

Beispielhafter Migrationsplan



(Die Balken stellen den Gültigkeitszeitraum des jeweiligen Zertifikats dar)

Zusammenfassung

- Wesentliche Kriterien bei der Auswahl der Post-Quanten-Verfahren:
  - ✓ Sicherheit
  - ✓ Performance (insb. Zertifikatsgröße)
  - ✓ Interoperabilität sowie Kompatibilität mit Standardanwendungen
- Hashbasierte Signaturverfahren:
  - \+ Hohes Vertrauen
  - – Einschränkungen müssen sorgfältig berücksichtigt werden
- Migrationsdauer für eine PKI (optimistisch): 15y
- Wann muss der Umstieg initiiert werden? **JETZT!**

→ Rahmenbedingungen für die Migration sind von allen Seiten zu schaffen!

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Dr. Kaveh Bashiri
Dr. Stavros Kousidis

Referat KM 21

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

E-Mail:
kaveh.bashiri@bsi.bund.de
stavros.kousidis@bsi.bund.de

https://bsi.bund.de/dok/997274