Post-Quantum

Cryptography Conference

Quantum-safe PKI for the German Administration

Kaveh Bashiri

The Federal Office for Information Security (BSI)

Federal Office
for Information Security

Quantum-safe PKI for the German administration

PKI Consortium, Amsterdam, November 8, 2023

Dr. Kaveh Bashiri, Dr. Stavros Kousidis, BSI

The public administration PKI ("Verwaltungs-PKI", V-PKI)

- Goal: Trustworthy identity management for the public administration

- Usage: S/MIME, TLS and other standard applications
- Scale: 6 Sub-CAs, approx. 500.000 subscribers
- Algorithm: RSA

Migration towards a quantum-safe V-PKI necessary!

Quantum-safe V-PKI – Choice of signature schemes

Important Criteria:

- Security
- Performance (especially: signature- and PK-size)
- Interoperability and compatibility with standard applications
- High Availability

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SPHINCS+ (SLH-DSA)	• Well-understood security properties	• Performance
Dilithium (ML-DSA) in combination with ECDSA	• Better performance than SPHINCS+ • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SPHINCS+ (SLH-DSA)	• Well-understood security properties	• Performance
Dilithium (ML-DSA) in combination with ECDSA	• Better performance than SPHINCS+ • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Comparison of certificate sizes

Algorithm	Signature-size in kB	PK-size in kB	(Signature + PK)-size in kB
RSA4096	0.5	0.5	1
Dilithium3 & ECDSA-384	3.4	2.1	5.5
SPHINCS+-192s	16	0.05	16
SPHINCS+-Few-192s	8	0.05	8
LMS-H20-192-W8	1.1	0.05	1.1
HSS-H5/H15-192-W8	1.8	0.05	1.8

LMS-H20-192-W8 (or HSS-H5/H15-192-W8)

on the Root-CA level?

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SPHINCS+ (SLH-DSA)	• Well-understood security properties	• Performance
Dilithium (ML-DSA) in combination with ECDSA	• Better performance than SPHINCS+ • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

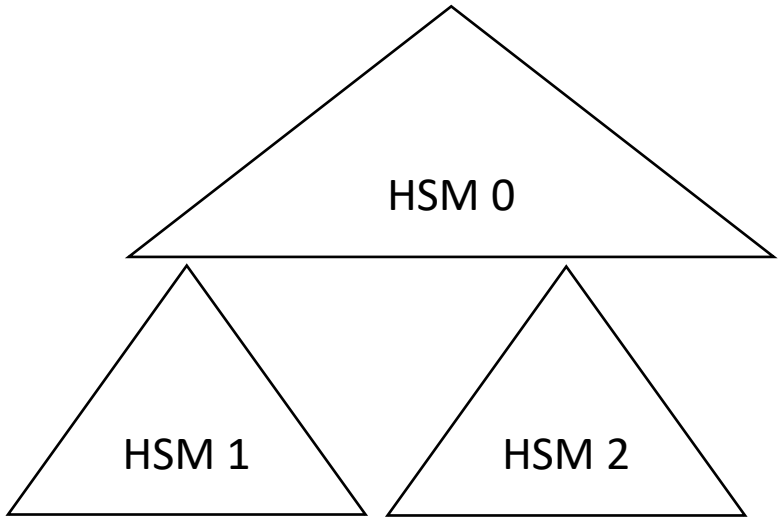
Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SPHINCS+ (SLH-DSA)	• Well-understood security properties	• Performance
Dilithium (ML-DSA) in combination with ECDSA	• Better performance than SPHINCS+ • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Backup management according to NIST SP 800-208, § 7

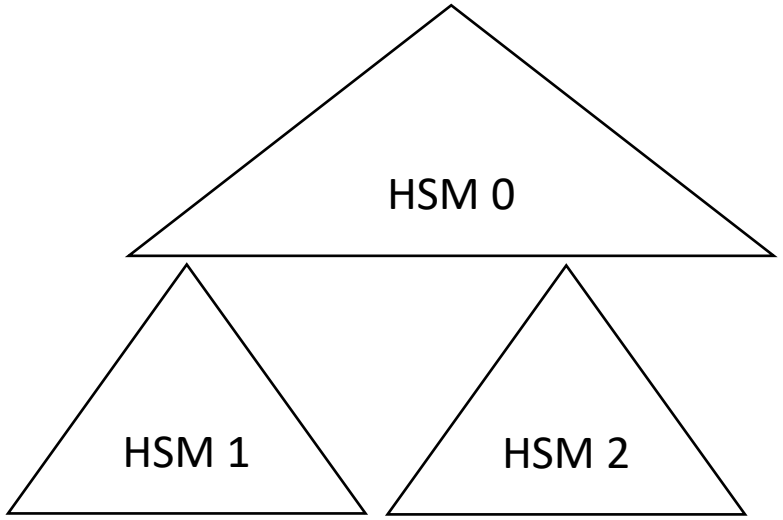
(Distributed multi-tree hash-based signatures)



- Create top-level Merkle-tree on HSM 0
- Create bottom-level Merkle-trees on HSM 1, HSM 2
- Sign roots of the bottom-level Merkle-trees with HSM 0
- Store copies of the corresponding signatures and auth. paths outside of the cryptographic modules
- Sign messages with HSM 1 (and then with HSM 2)
- Initiate new HSM 3 as long as HSM 0 is operational

Backup management according to NIST SP 800-208, § 7

(Distributed multi-tree hash-based signatures)



Problem:

- Cryptographic modules may be operational for < 10y
- All HSMs might break at the same time
- Root-CA needs to be able to generate signatures for 10y

Quantum-safe V-PKI – Choice of signature scheme

Candidates:

Algorithm	Pros	Cons
XMSS, LMS	• Well-understood security properties • Performance (especially: signature- and PK-size)	• Statefulness (!) • Backup management
SPHINCS+ (SLH-DSA)	• Well-understood security properties	• Performance
Dilithium (ML-DSA) in combination with ECDSA	• Better performance than SPHINCS+ • Presumably: compatibility with standard applications	• Structured lattice (?) • Compatibility of hybrid mode (?)

Hybrid Digital Signatures

- Independent signatures, e.g. PQC & ECC
- Signature is valid if and only if all (independent) signatures verify
- Concrete proposals @IETF:
  - draft-ounsworth-pq-composite-sig
  - draft-wussler-openpgp-pqc
  - Composite construction, e.g. identifier for „ML-DSA-65 + ECDSA-brainpoolP256r1“

Quantum-safe V-PKI – Further Criteria

Quantum-safe V-PKI – Further criteria

Design of certificates:

- Separate signature- and encryption certificates
- Standardisation of post-quantum schemes in common certificate formats

  → Cooperation BSI & genua GmbH for X.509 certificates: draft-gazdag-x509-hash-sigs

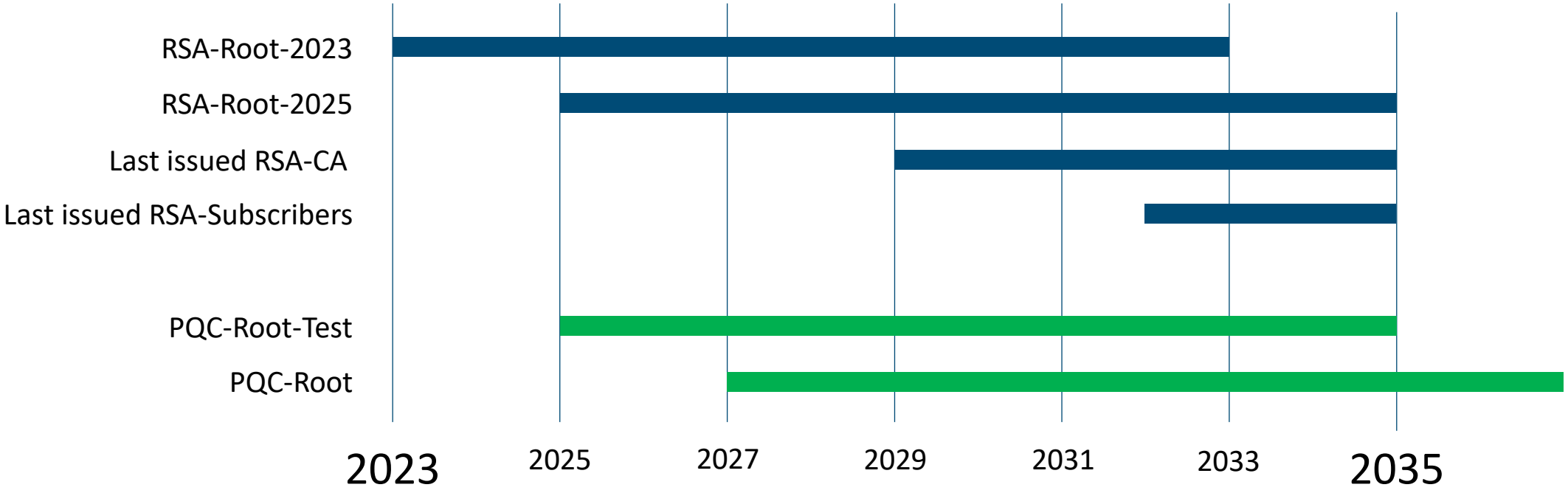
Quantum-safe V-PKI – Further criteria

Migration concept:

- *Parallel approach*:

→ Smooth transition in order to guarantee business continuity

Migration – What it looks like in validity periods



(The bars represent the validity periods of the corresponding certificates)

Summary

- Crucial criteria for the choice of the post-quantum schemes:
  - ✓ Security
  - ✓ Performance (especially, certificate size)
  - ✓ Interoperability and compatibility with standard applications
  - ✓ High Availability
- Hash-based signature schemes:
  - \+ High confidence
  - – Restrictions need to be carefully considered
- Migration timeline for a complex PKI (optimistic): 15y
- When do we have to initiate the transition? **NOW!**

→ Need commitment to PQC-migration from all involved parties!

Thank you for your attention!

Dr. Kaveh Bashiri
Dr. Stavros Kousidis

Federal Office for Information Security
Godesberger Allee 185-189
53175 Bonn

Email:
kaveh.bashiri@bsi.bund.de
stavros.kousidis@bsi.bund.de

www.bsi.bund.de/dok/pqmigration-en

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia