Post-Quantum

Cryptography Conference

The PQC Landscape: Protocols and Standards

David Hook
VP Software Engineering at Keyfactor

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

KEYFACTOR

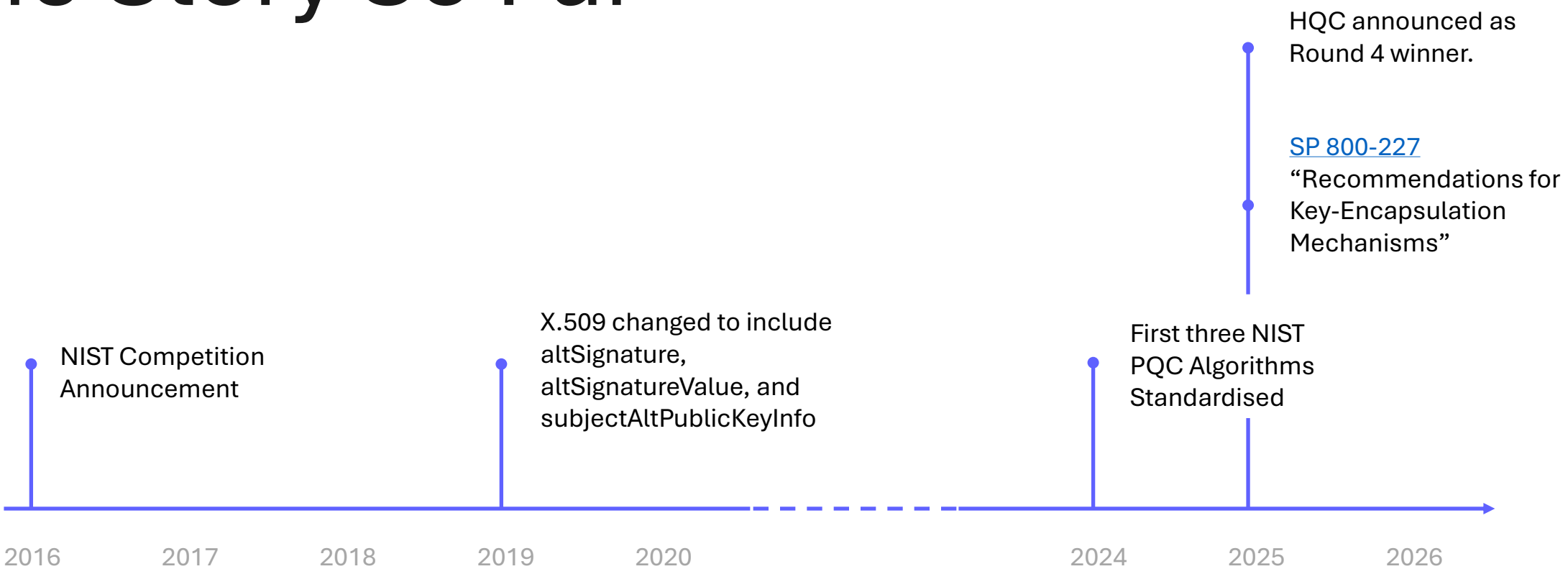
KEYFACTOR

The PQC Landscape: protocols and standards.

David Hook

VP Software Engineering, Keyfactor

The Story So Far



Other Algorithms

- FN-DSA (Falcon) Initial Public Draft coming (FIPS PUB 206).
- HQC KEM continues to evolve.
- Still no clear “front runners” with the PQC signature process.
- FrodoKEM - BSI TR-02102-1, ISO.
- Classic McElliece – IETF draft-josefsson-mceliece, BSI TR-02102-1, ISO.
- NTRU – IEEE 1636.1-2008, IETF draft-fluhrer-cfrg-ntru Nippon Telecom
- SNTRUPrime – IETF draft-ietf-sshm-ntruprime-ssh

ML-KEM

- FIPS: NIST FIPS PUB 203
- IETF: draft-ietf-lamps-kyber-certificates-11
- Key Encodings provide options with private keys

```
ML-KEM-512/768/1024-PublicKey ::= OCTET STRING (SIZE (800/1184/1568))

ML-KEM-512/768/1024-PrivateKey ::= CHOICE {
      seed [0] OCTET STRING (SIZE (64)),
      expandedKey OCTET STRING (SIZE (1632/2400/3168)),
      both SEQUENCE {
        seed OCTET STRING (SIZE (64)),
        expandedKey OCTET STRING (SIZE (1632/2400/3168))
        }
      }
```

ML-DSA

- FIPS: NIST FIPS PUB 204
- IETF: draft-ietf-lamps-dilithium-certificates
- Key Encodings provide options with private keys

```
ML-DSA-44/65/87-PublicKey ::= OCTET STRING (SIZE (800/1952/2592))

ML-DSA-44/65/87-PrivateKey ::= CHOICE {
      seed [0] OCTET STRING (SIZE (32)),
      expandedKey OCTET STRING (SIZE (2560/4032/4896)),
      both SEQUENCE {
        seed OCTET STRING (SIZE (32)),
        expandedKey OCTET STRING (SIZE (2560/4032/4896))
        }
      }
```

SLH-DSA

- FIPS: NIST FIPS PUB 205
- IETF: draft-ietf-lamps-x509-slhdsa
- Also NIST: SP 800-230 - Alternative Parameter Sets.
- Key Encodings simple octet strings in both cases.

SLH-DSA-???-PublicKey ::= OCTET STRING (SIZE (32...64))

SLH-???-PrivateKey ::= OCTET STRING (SIZE (64...128))

Certification Requests

ML-DSA and SLH-DSA

- PKCS#10
- CRMF.

ML-KEM

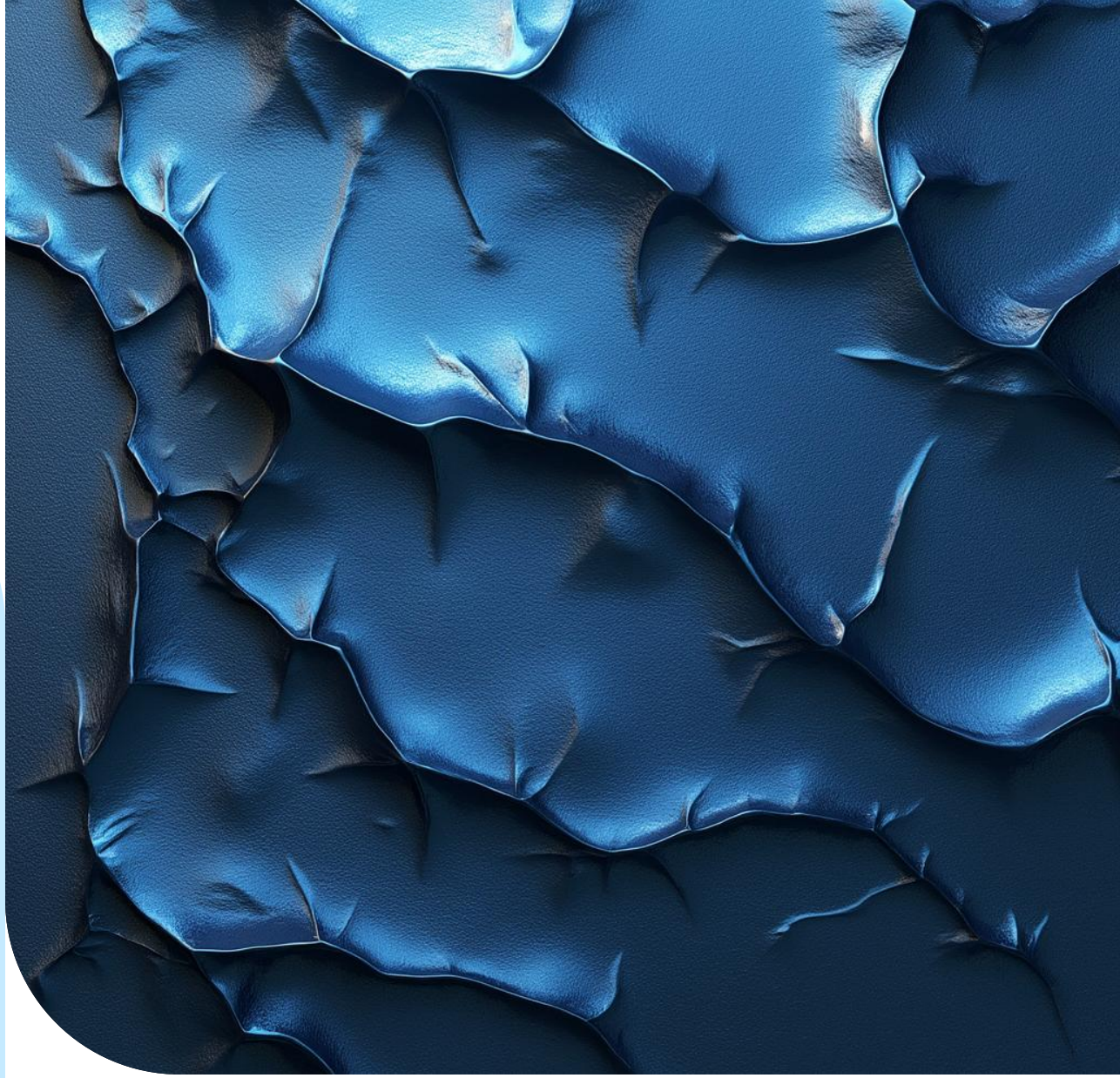
- CRMF only (POP requires use of certEncr)
- Proposals for Dual Key PKCS10, even Dual Usage PKCS10

Chimera Certificates

- Standardized in X.509 2019.
- Allows for 2 keys and 2 signatures in a certificate.
- Early IPR issues held up usage.
- Second key and signature appear in extension block.
- Requires “preTBSCertificate” calculation for dealing second signature.
- Proposal for CSR message currently being discussed in X9.

Composite Certificates

- IETF: draft-ietf-lamps-pq-composite-sigs
- Dual Signature format using ML-DSA and an associated classical algorithm.
- Requires evaluation of both signatures.
- Not so much a migration thing as a “hedge your bets” thing.
- Driven by IETF, now in final call.



Chameleon Certificates

- IETF: draft-bonnell-lamps-chameleon-certs
- Allows nesting of a template for a second certificate within the extension block of a carrier certificate.
- Other than processing of extension, no extra certificate processing required.
- Can be used for forward migration, with the nested certificate replacing the carrier one.

Dual Usage Certificates

- Another approach which provides a signing and KEM key in a single certificate.
- Main certificate key is a signing key.
- KEM key associated with holder of the signing key provided in an extension.
- Allows for a PKCS#10 CSR to be used, with a certEncr style response to allow POP for both signing and KEM key.

Unsigned X.509 Certificates

- Written up in draft-ietf-lamps-x509-alg-none
- For trust anchors – theory is they're self-signed, signature usually ignored
- Deals with the increase in signature size nicely, by leaving it out
- Now in last call, so likely coming to a trust store near you soon.

CMS

RFC 9629

Using Key Encapsulation Mechanism (KEM) Algorithms in the Cryptographic Message Syntax (CMS)

draft-ietf-lamps-cms-ml-dsa

Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)

RFC 9814:

Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)

TLS

ML-KEM

draft-ietf-tls-mlkem ML-KEM Post-Quantum Key Agreement for TLS 1.3

draft-ietf-tls-ecdhe-mlkem Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3

ML-DSA

draft-ietf-tls-mldsa Use of ML-DSA in TLS 1.3

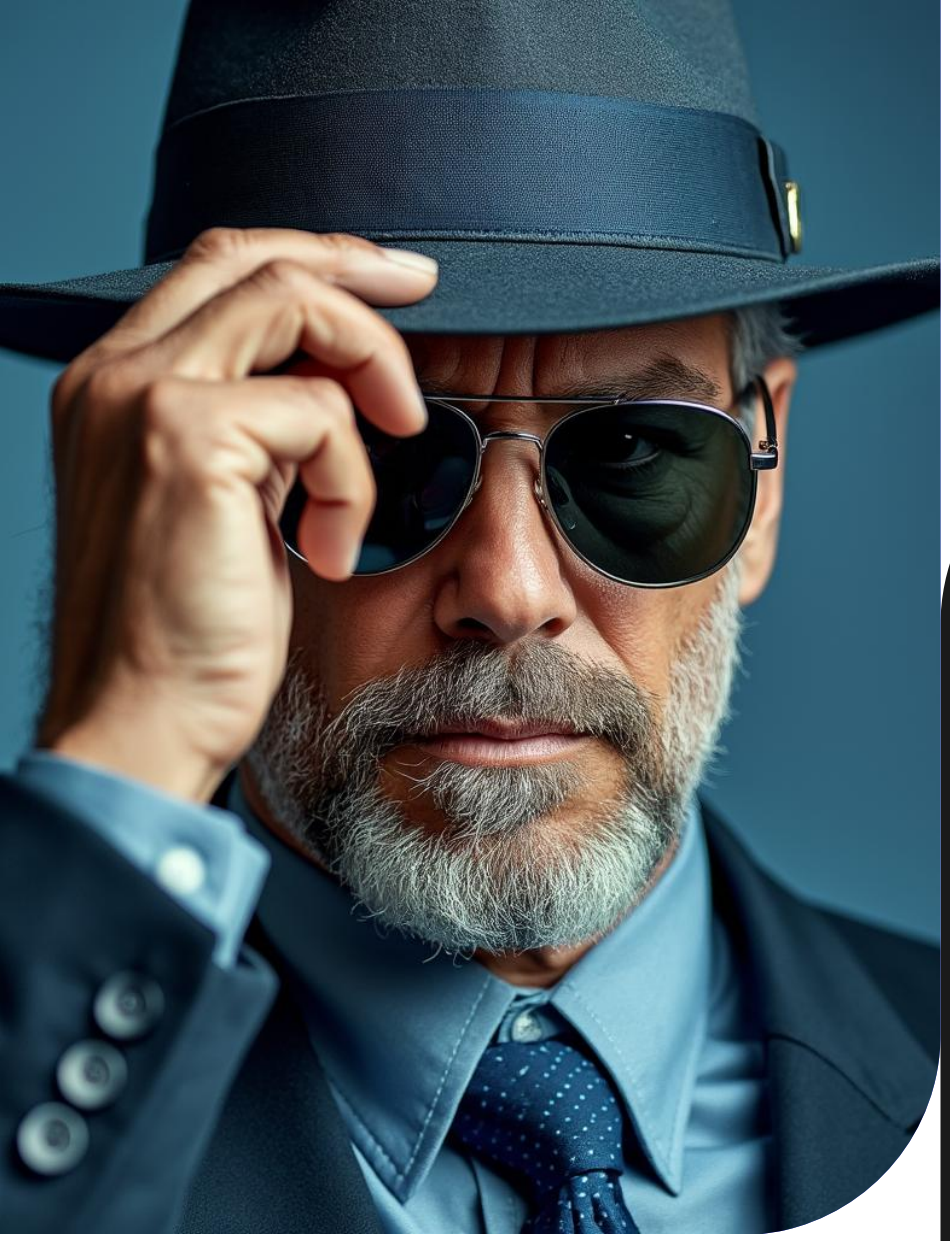
SLH-DSA

draft-reddy-tls-slhdsa Use of SLH-DSA in TLS 1.3

KEYFACTOR

General references

- draft-ietf-pquip-pqc-engineers Post-Quantum Cryptography for Engineers
- RFC 9794: Terminology for Post-Quantum Traditional Hybrid Schemes
- PQC Almanac For C# and Java
- ACSC: Planning for PQC
- BSI: Quantum-Safe Cryptography
- ETSI: Quantum Safe Cryptography
- NIST: Post-Quantum Cryptography



Thanks for Listening

Any Questions?

KEYFACTOR