Planning for Post-Quantum Cryptography (PQC)

Russ Housley

Past IETF Chair

Current IETF LAMPS WG Chair

Vigil Security LLC

9 May 2022

Motivation

- If large-scale quantum computers are ever built, these computers will be able to break the public key cryptosystems currently in use.
- A post-quantum cryptosystem (PQC) is secure against quantum.
- It is open to conjecture when it will be feasible to build such computers; however, RSA, DSA, DH, ECDH, ECDSA, and EdDSA are all vulnerable if a large-scale quantum computer is developed.

Certificates and PQC Algorithms

Goal

Deploy PQC algorithms before there is a large-scale quantum computer that is able to break public key algorithms in widespread use today

Assumption

While people gain confidence in the PQC algorithms and their implementations, security protocols will use a mix traditional and PQC algorithms

Recognize

Such transitions take a long time—at least a decade

Two Possible Approaches

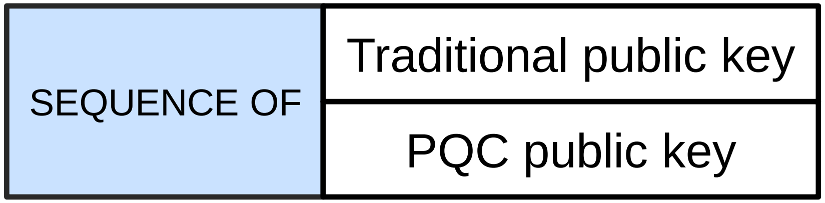
Two certificates, each with one public key and one signature:

- one certificate traditional algorithm, signed with traditional algorithm
- one certificate PQC algorithm, signed with PQC algorithm

One certificate:

- contains multiple public keys – mix of traditional and PQC public keys
- Multiple signatures – mix of traditional and PQC signatures

Public Key

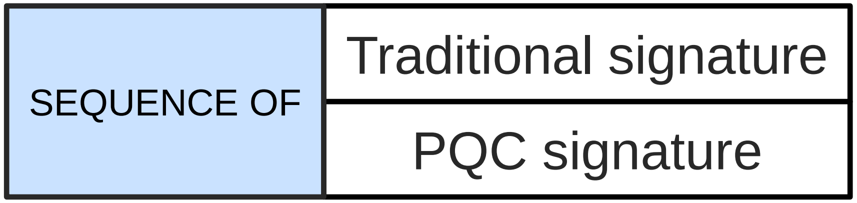


SEQUENCE OF

Traditional public key

PQC public key

Signature



SEQUENCE OF

Traditional signature

PQC signature

One Certificate

- Security protocols **do not need** any new fields
  - Additional public keys are in one certificate
  - Security protocols still need to be updated for the PQC algorithms
- No need to modify certificate architecture, but validation needs additional complexity to handle new corner cases …
- Has known pitfalls of the “jumbo” certificate, which carried a key agreement public key and a signature public key for the same user
- Certificate becomes huge
- Yet, the desire for just one certificate for a device like a cable modem makes this a very attractive approach

One Certificate, but Two Flavors

COMPOSITE

Composite encryption uses all of the public keys in the certificate separately

Composite decryption can be performed with *any* of the private keys associated with one of the certified public keys (OR)

COMBINED

Combined encryption uses all the keys in a nested way

Combined decryption must be performed with *all* of the private keys associated with all of the certified public keys (AND)

Two Certificates

- Security protocols need new field for the additional certificates
- No need to modify certificate architecture, and validation works exactly as it does today
- Avoid known pitfalls of the “jumbo” certificate
- Two certificates are slightly bigger than one, just because the subject, issuer, and other metadata are carried in both
- At the end of the transition, just stop using the certificates with traditional algorithms, which is the ultimate goal state

IETF LAMPS

Specification for both the two certificate approach and the one certificate approach:

- specify the use of the new PQC public key algorithms
- specify formats, identifiers, enrollment, and operational practices for “hybrid key establishment”
- specify formats, identifiers, enrollment, and operational practices for “dual signature”

Thank you!

Russ Housley
housley@vigilsec.com
+1 703 435 1775