

# Certificates: Transition from Traditional Algorithms to PQC Algorithms

Russ Housley  
Founder  
Vigil Security, LLC

# 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:** upgrading existing PKI will take a long time

**Recognize:** security protocols need to be updated, which will also take a long time

# Two Possible Approaches

- 1) 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
- 2) One certificate:
  - 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

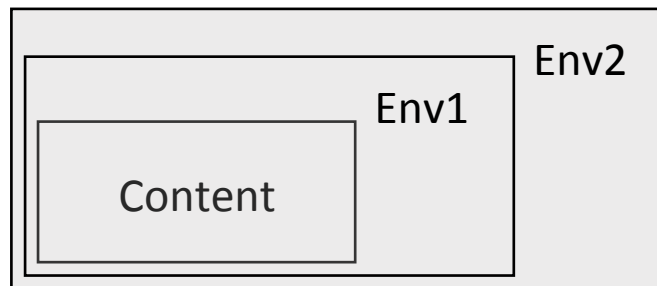
SEQUENCE OF	Traditional signature
	PQC signature

# In both cases ...

While people gain confidence in the PQC algorithms and their implementations, security protocols should mix traditional and PQC algorithms for confidentiality and authentication based on both IPsec and TLS, use a KDF to compute shared secret from two inputs:

$$SS = \text{KDF}( SS_T, SS_{\text{PQC}} )$$

S/MIME, could so the same OR use double encapsulation for confidentiality along with parallel signatures for authentication



# 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 ...
  - Traditional signature fails but PQC is good – do what?
- Has known pitfalls of the “jumbo” certificate, which carried a key agreement public key and a signature public key for the same user
  - The “jumbo” certificate had fewer corner cases since there was only one signature public key
- Certificate becomes huge

# 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 repeated in both
- At the end of the transition, just stop using the certificates with traditional algorithms

# My Recommendation

- Use separate certificates for traditional and PQC algorithms
- Begin the security protocol work now for mixing the two
- Plan for the day when only PQC algorithms are used

The logo for Vigil Security LLC is centered on a white rectangular background. The word "Vigil" is written in a red, serif font. Below it, the word "Security" is written in a black, serif font. Underneath "Security", the letters "LLC" are written in a smaller, black, sans-serif font.

Vigil  
Security  
LLC