Planning for Post-Quantum Cryptography: Evolution of the Internet PKI

Second X.509 Day – Session 2

Vigil Security LLC

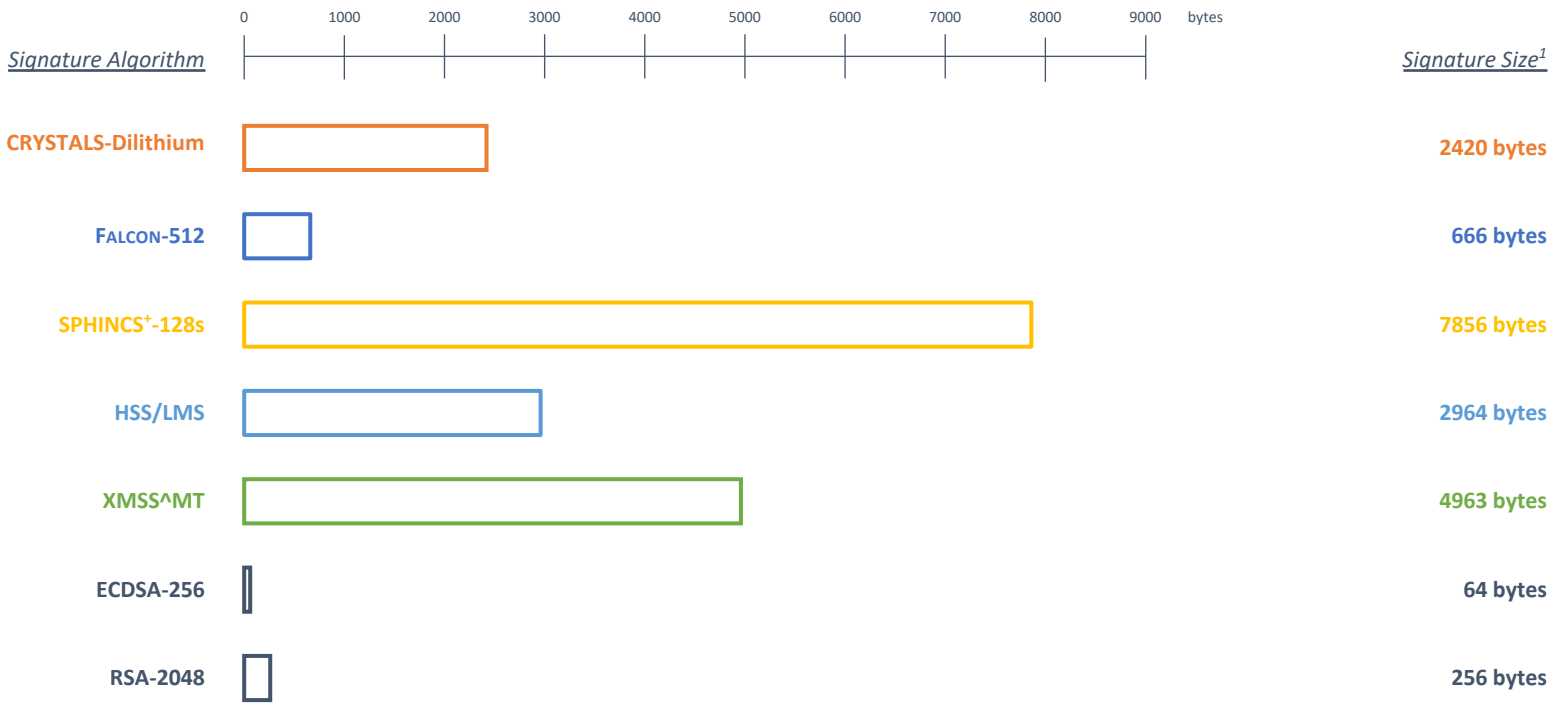
Russ Housley

9 May 2023

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 large-scale quantum computers.
- 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.

PQC: Large Public Key and Signature Size



[1] *with example parameters*

Vigil Security LLC

Two Possible Certificate Approaches

Goal – Deploy PQC algorithms before there is a large-scale quantum computer.

Assumption – First steps will mix traditional algorithms and PQC algorithms.

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, containing multiple public keys and multiple signatures:

Public Key

SEQUENCE OF	Traditional public key
	PQC public key

Signature

SEQUENCE OF	Traditional signature
	PQC signature

Vigil Security LLC