Postquantum Certificates

- People will create a practical Quantum Computer sometime
  - They would be able to break current certificates.
- Upgrading the PKI infrastructure (and everything that uses certificates) will take a long time.
- We need to start on a solution now.

Two problems and how we address them

We don’t fully trust postquantum algorithms

- Solution: composite signatures (which combine multiple algorithms)

Backwards compatibility

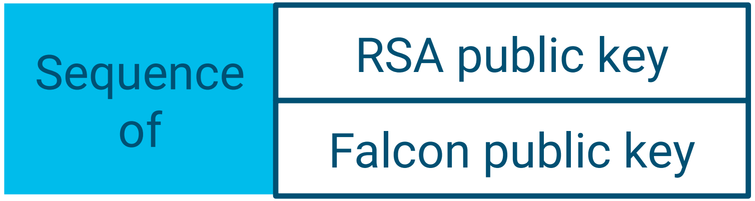
- Solution: Have parallel certificates, with one certificate with a traditional algorithm, and one with the postquantum algorithms

Our draft addresses the first solution

How our draft works

We treat the combination of signature algorithms as a single larger algorithm

Public Key

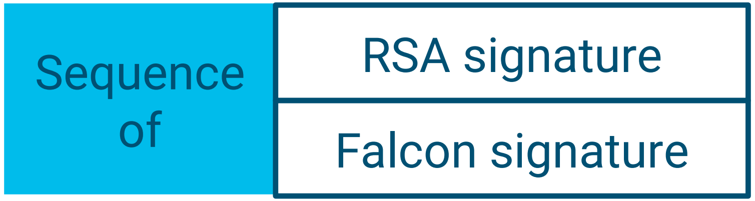


Sequence of

RSA public key

Falcon public key

Signature



Sequence of

RSA signature

Falcon signature

When the certificate includes a public key or signature, we insert the composite version

Advantages of this approach

Simplicity

No need to modify certificate architecture

Hybrid signatures can be used outside of certificates

IPR Free

Comments?