COSE and JOSE Registrations for Post Quantum Signatures

draft-ietf-cose-post-quantum-signatures-01

Mike Prorock
IETF 115, London
November 2022

What's the deal with PQC?

- Why introduce new forms of cryptography?
  - Shor's Algorithm
- Why support existing standards / formats?
  - Easier path to developer adoption
  - Creates an upgrade path for standards compliant software
- What Algorithms and Why?
  - Signature and Key Representations are the building blocks for secure identifiers and credentials.
  - Stronger agility from supporting multiple primitives
    - Lattice schemes have the best security/size tradeoff
    - Hash schemes have well established security properties
- NIST has announced candidates to be standardized

What are our goals?

- SPHINCS+, Falcon, Dilithium
- Intuitive upgrade path for post quantum
  - Enable leapfrogging from RSA to PQ
- Minimum cryptographic agility
  - Anticipate potential exploits in emerging tech
- Set a path for future PQ algorithms
- IANA Registrations
  - Mitigate ambiguity / parameterization related faults

What is new with PQC?

- Keys and signatures are larger
  - trade off between signing and verification times
- Larger number of parameters for some algorithms
  - we need to keep optionality small based on expert feedback
- We need to be very clear about what parameters are in use with which signature schemes

Draft Updates

- We have completed out sections for Falcon and Sphincs+
- We have detailed parameter sets that will likely see use
- Utilizing kty & alg to identify algorithm family, specific algorithm, and parameters - e.g.

```
{
   “kty” : “HASH”,
   “alg” : “SPHINCS+128f”,
   “x”   : “eyJhbGciOiJQUzM4NC…”
}
```

Next Steps

- Split into 3 drafts?
  - `draft-ietf-cose-dilithium-01`
  - `draft-ietf-cose-falcon-01`
  - `draft-ietf-cose-sphincs-plus-01`

- Await finalization on parameter sets
- General guidance from the group

Resources

Work Item Repository (Issues, PRs, Details):
https://github.com/mesur-io/post-quantum-signatures

Datatracker:
https://datatracker.ietf.org/doc/draft-prorock-cose-post-quantum-signatures/

NIST PQC:
https://csrc.nist.gov/projects/post-quantum-cryptography/news
https://csrc.nist.gov/projects/post-quantum-cryptography

Relevant Signature Schemes:
https://pq-crystals.org/dilithium/
https://falcon-sign.info/
https://sphincs.org/