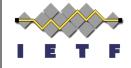
QSC

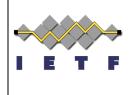
Key Identification and Serialization

draft-uni-qsckeys



Mike Osborne IETF 114 Philadelphia July 27, 2022

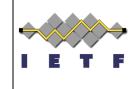
Draft update 01



https://datatracker.ietf.org/doc/html/draft-uni-qsckeys-00.html

- We refrain from assigning any preliminary OIDs for the algorithms. The goal is to use a single OID for each algorithm and to align with NIST on the assigned OIDs.
- Revision of the ASN.1 syntax.
- Revision of the private key encoding of Kyber. The parameters now have the same order as the raw keys.
- Updated references.

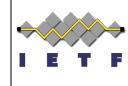
PQC Update



- NIST has selected the PQC algorithms to standardize :
 - CRYSTALS-Kyber as primary KEM
 - CRYSTALS-Dilithium as primary Signature
 - FALCON as backup signature
 - SPHINCS+ as backup signature
- NIST will evaluate the following KEM algorithms in a fourth round :
 - SIKE
 BIKE
 HQC
 Classic McEliece

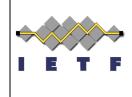
 At most two selected
- NIST will hold a 4th NIST PQC Standardization Conference on Nov. 29 Dec. 1, 2022.
- NIST also plans to issue a new Call for Proposals for public-key digital signature algorithms by the end of summer 2022 (Deadline June 1st 2023)

Next Steps



- Work underway to update the document
 - Remove non finalist algorithms to a separate document
 - Restructure according to NIST decision
 - Add SPHINCS+ algorithm
 - Decided to wait before adding the Round 4 candidates to the draft
- Debate parsing complexity tradeoff for structure definitions
 - The use of CHOICE ASN syntax for partially populated keys.
 - The definition of PKCS#8 v2 syntax (with optional public key).
 - A separate document being created for distribution/discussion
- Align with NIST on algorithm OIDs
- Resolve issues around multi key modes (IP, key serialization)
- Encouraged format for migration

Resources



Work Item Repository (Issues, PRs, Details):

https://github.com/Quantum-Safe-Collaboration/qsc-key-rfc

Datatracker: https://datatracker.ietf.org/doc/html/draft-uni-qsckeys-00.html

NIST PQC:

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

Relevant KEM Schemes:

https://pq-crystals.org/kyber/

Relevant Signature Schemes:

https://pq-crystals.org/dilithium/ https://falcon-sign.info/

https://sphincs.org/