SPDM WG

Plan of Support for Post Quantum Crypto (PQC) in SPDM

June 2024

Disclaimer

- The information in this presentation represents a snapshot of work in progress within the DMTF SPDM WG.
- This information is subject to change without notice. The standard specifications remain the normative reference for all information.
- For additional information, see the DMTF website.
- This information is a summary of the information that will appear in the specifications. See the specifications for further details.

Background

- In August 2023, NIST published drafts of PQC contest winning algorithms.
    - (FIPS 203) "Kyber: Module-Lattice-Based Key-Encapsulation Mechanism Standard"; replacing Diffie-Hellman
    - (FIPS 204) "Dilithium: Module-Lattice-Based Digital Signature Standard"; replacing RSA and ECDSA
    - (FIPS 205) "SPHINCS+: Stateless Hash-Based Digital Signature Standard"; replacing RSA and ECDSA
- Final specifications[1] expected in summer 2024
- Another PQC signature winner but no public draft yet: Falcon
- NIST is still looking for more digital signature schemes, preferably not based on Module-Lattice.

[1]: https://csrc.nist.gov/Presentations/2024/update-on-the-nist-pqc-standardization-project

PQC's Impact to SPDM – Signature and Key Exchange

Message	Digital Signature	Key Exchange
("core" messages)		
CERTIFICATES	Yes	No
CHALLENGE_AUTH	Yes	No
ENDPOINT_INFO	Yes	No
MEASUREMENTS	Yes	No
KEY_EXCHANGE_RSP	Yes	Yes
FINISH	Yes	No
("supporting" messages)		
NEGOTIATE_ / ALGORITHMS	Yes	No
SET_CERTIFICATE / _RSP	Yes	No
SET_KEY_PAIR_INFO / _ACK	Yes	No
GET_ / KEY_PAIR_INFO	Yes	No
(others)	No	No

Dependency on Industry Standards

“Core” messages	FIPS 203	FIPS 204 and/or 205	X.509 cert	TLS
CERTIFICATES	No	Yes	Yes	No
CHALLENGE_AUTH	No	Yes	Yes or No*	No
ENDPOINT_INFO	No	Yes	Yes or No*	No
MEASUREMENTS	No	Yes	Yes or No*	No
KEY_EXCHANGE_RSP	Yes	Yes	Yes or No*	Yes
FINISH	Yes	Yes	No	Yes

* When the public key is pre-provisioned to peer (instead of sent in CERTIFICATES).

Yes = Need this standard to support PQC before this SPDM message can support PQC.
No = This SPDM message may support PQC even if this standard does not support PQC.

Proposed Plan - Core Messages Adopting PQC

- Upon NIST Publishing FIPS 203/204/205
- Step 1: Adopt PQC for the scenario where the public key is pre-provisioned to peer. Benefits these messages:
  - CHALLENGE_AUTH
  - ENDPOINT_INFO
  - MEASUREMENTS
- Step 2: Further adopt PQC after X.509 cert supports PQC (RFC expected by end of 2024). Benefits these messages:
  - CERTIFICATES
  - CHALLENGE_AUTH
  - ENDPOINT_INFO
  - MEASUREMENTS
- Step 3: Further adopt PQC after TLS support PQC. Benefits all core messages.
- Proposal: SPDM 1.4 will be a PQC-focused revision that supports Steps 1 & 2. A later SPDM revision will add support for Step 3.

Request for Industry Feedback

1. Among NIST's selected PQC algorithms, which algorithms and which parameters sets is your company planning to support?
2. Is your company considering support for Post-Quantum / Traditional (PQ/T) hybrid key and signature schemes? If yes, which combinations?
3. What are your thoughts on the proposed plan for PQC and/or hybrid schemes in SPDM?
4. When does your company need PQC and/or hybrid schemes in SPDM?

Please provide feedback to your SPDM WG representative or the DMTF Feedback Portal at https://www.dmtf.org/standards/feedback by August 2024

References

All are internet drafts; nothing finalized

- Hybrid key exchange in TLS 1.3 [link]
- Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA [link]
- Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) [link]
- Composite ML-DSA for use in Internet PKI [link]
- A Mechanism for Encoding Different Paired Certificates [link]
- Related Certificates for Use in Multiple Authentications within a Protocol [link]