SPDM & Post Quantum Crypto (PQC)

October 2024
Jeff Hilland, HP Labs, DMTF President & SPDM co-chair

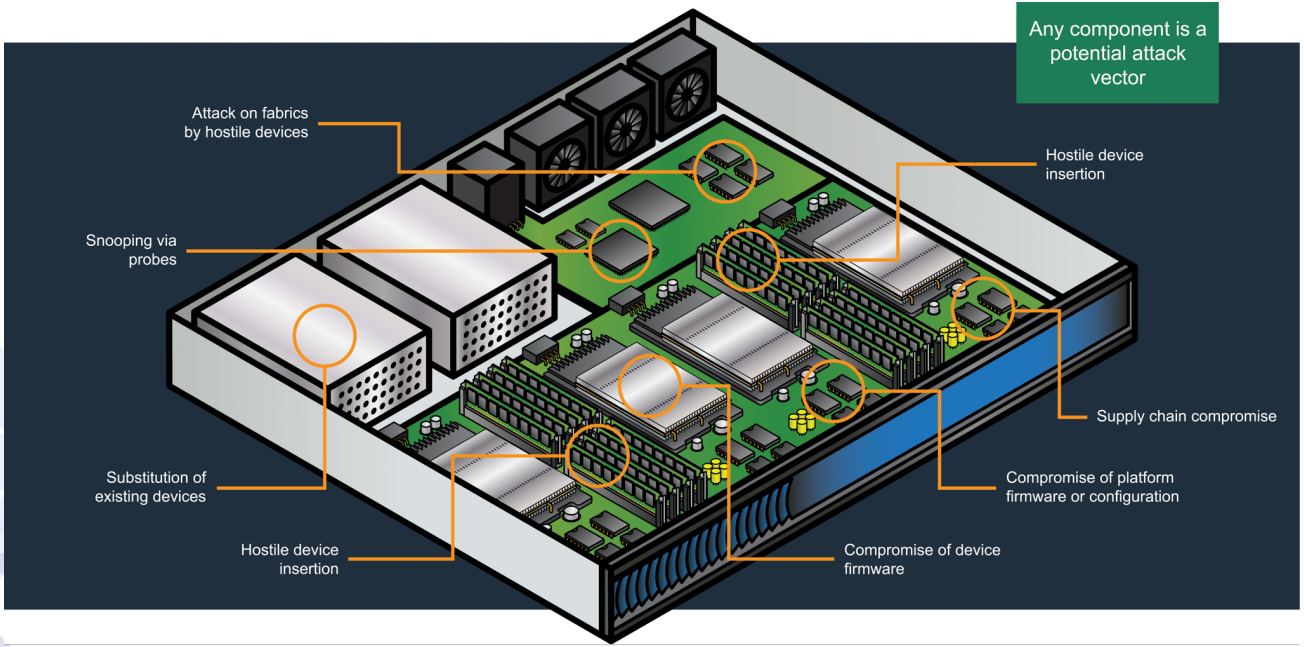
Disclaimer

- 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.

Agenda

- SPDM Background
- SPDM for Storage Binding
- SPDM PQC Update

Why Platform Security?



Why SPDM?

The industry needs a common solution that works for the control plane and data plane regardless of technology or protocol and integrates into the solutions being proposed by other open communities. This decreases costs while increasing security.

Having an open-source code base (DMTF's libspdm) that can be leveraged by both ends of the wire (Requester and Responder in SPDM language) helps seed the industry and allows researchers to validate the security of the standard.

SPDM's Overall Goals

- All SPDM features fall into at least one of these main goals:
  - Device Attestation and Authentication
  - Secure Communication over any transport
- Device Attestation and Authentication
  - The ability to attest various aspects of a device such as firmware integrity and device identity
- Secure Communication over any Transport
  - Provide the ability to secure communication of any data or management traffic over any transport
  - Work with industry partners to ensure data in-flight is secure for all parts of the infrastructure (e.g. storage, network fabrics, etc.)

SPDM Feature Summary

- Version 1.0:
  - Measurements
  - Device Attestation and Authentication
- Version 1.1:
  - Secure Session
    - Public Key Exchange
    - Symmetric Key Exchange
  - Mutual Authentication
- Version 1.2:
  - Installation of certificates
  - Allows for alias certificates derived from device certificates
  - Send and receive large SPDM messages (chunks)
  - Added SM2, SM3, SM4 algorithms to supported list
  - New OIDs added
  - Deprecated basic mutual authentication in CHALLENGE and CHALLENGE_AUTH
- Version 1.3
  - Eventing
  - Multi-Key
  - Generic Certificates
  - MEL & HEM
  - Endpoint Info
- Bindings
  - MCTP to SPDM
  - MCTP to Secure Messages
  - Secure Messages to SPDM
  - SPDM over TCP
  - SPDM over Storage (NVMe, SAS, SATA)

SPDM PQC SUPPORT

Background

- In August 2023, NIST published drafts of PQC contest winning algorithms.
  - (FIPS 203) "Module-Lattice-Based Key-Encapsulation Mechanism Standard" (ML-KEM); replacing Diffie-Hellman (aka Kyber).
  - (FIPS 204) "Module-Lattice-Based Digital Signature Standard" (ML-DSA); replacing RSA and ECDSA (aka Dilithium).
  - (FIPS 205) "Stateless Hash-Based Digital Signature Standard"; replacing RSA and ECDSA (aka SPHINCS+)
  - Final specifications[1] published August 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.
- CNSA specs are expected that will make these required.
  - While not every country will follow CNSA requirements, many will

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Proposed Plan - Core Messages Adopting PQC

- Immediate Need is Signatures
  - Adopt PQC for the scenario where the public key is pre-provisioned to peer.
  - Adopt PQC signatures after X.509 cert supports PQC (RFC expected by end of 2024).
  - Adopt PQC key encapsulation after SP 800-227, which indicates requirements for ML-KEM in protocol implementations, is published.
  - This is planned to be SPDM 1.4, released on or after 4Q24.
    - Any changes/features that happen to be ready and merged will also be included.
- Consider adopting PQ/T (hybrid) signature and key encapsulation schemes.
  - Once the industry has general agreement on how.
  - This addition may be captured in a later SPDM release.
- libspdm support
  - lbspdm is likely to work on 1.3 through 4Q24.
  - Plan of record will be to add PQC subsequent to being feature complete for 1.3.
    - Given that SPDM doesn't implement any algorithms and instead references libraries, this is not expected to be burdensome.

Impact of PQC on SPDM

- SPDM message length is 2 bytes (64K)
  - In order to support SPINCS+, length needs to be extended.
  - Kyber & Dilithium can fit within 64K packet length
- Extend data structures
  - Handle larger lengths without reformatting the packet
    - In most cases, a bit will indicate whether to use the old length field or a new, larger field in the packet.
  - New Algorithm Structures
    - Separation of the traditional algorithms from PQC in the algorithm negotiation structures.
    - Leave room for the newer algorithms expected.
  - Hybrid solution will depend on the industry
- May need additional commands to support PQC algorithms
  - Examination of impact of algorithms for any semantic changes

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 Oct. 31, 2024

Call to Action

- Understand what SPDM means to your ecosystem.
- Get ready for SPDM for storage
  - See sessions tomorrow in Security Track
- Get ready for PQC!
  - I2C is insufficient for PQC
  - Realize the space constraints for PQC
  - Implement algorithms in silicon
  - Give us feedback: https://www.dmtf.org/standards/feedback

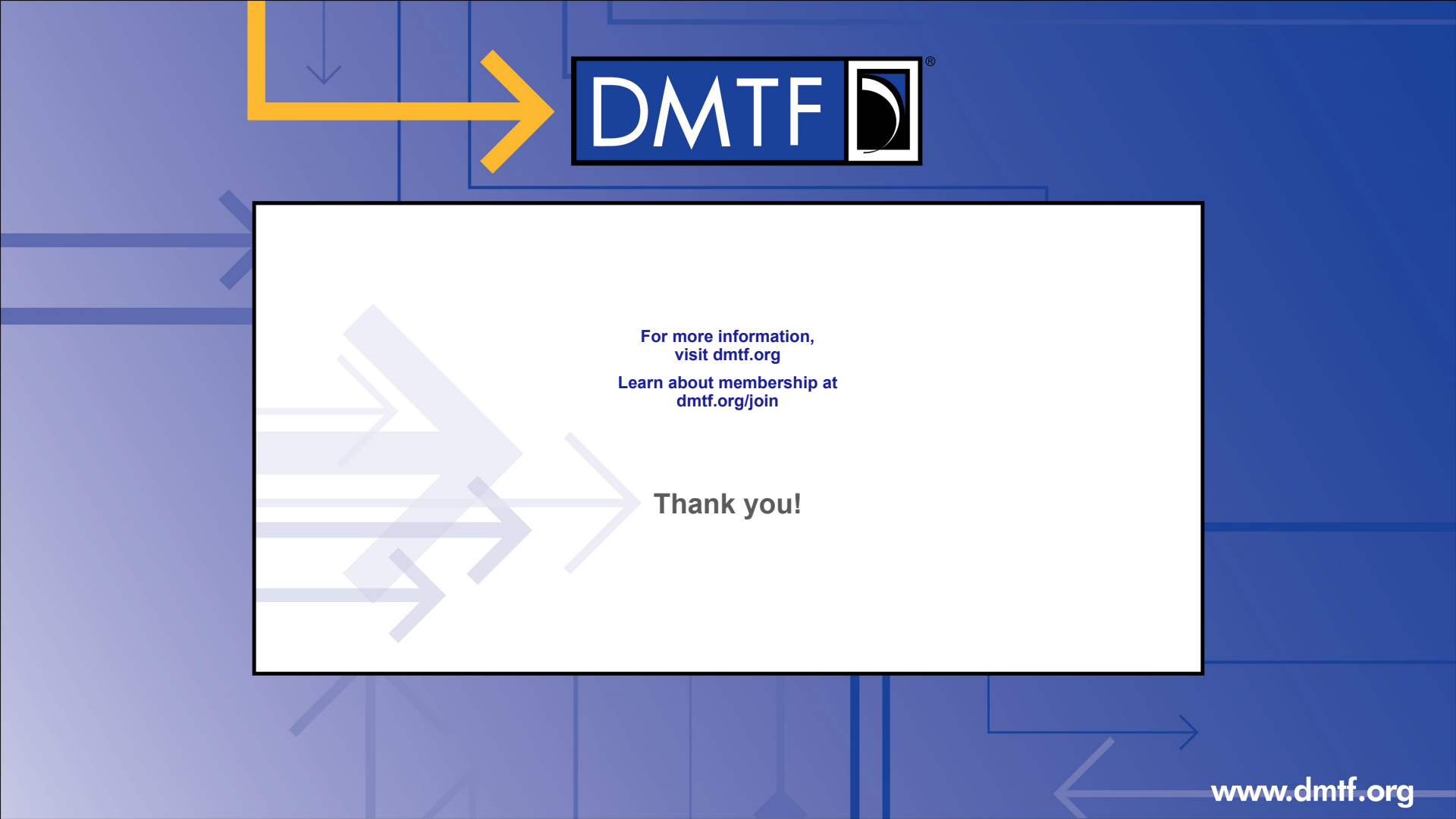
Thank you!

www.dmtf.org

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]


DMTF
For more information,
visit dmtf.org
Learn about membership at
dmtf.org/join
Thank you!
www.dmtf.org