802.1AR Amendment Proposal to Add ML-DSA Algorithms

Paul Bottorff
paul.Bottorff@hpe.com

Guy Fedorkow
gfedorkow@juniper.net

Kevin Micciche
kevin.Micciche@hpe.com

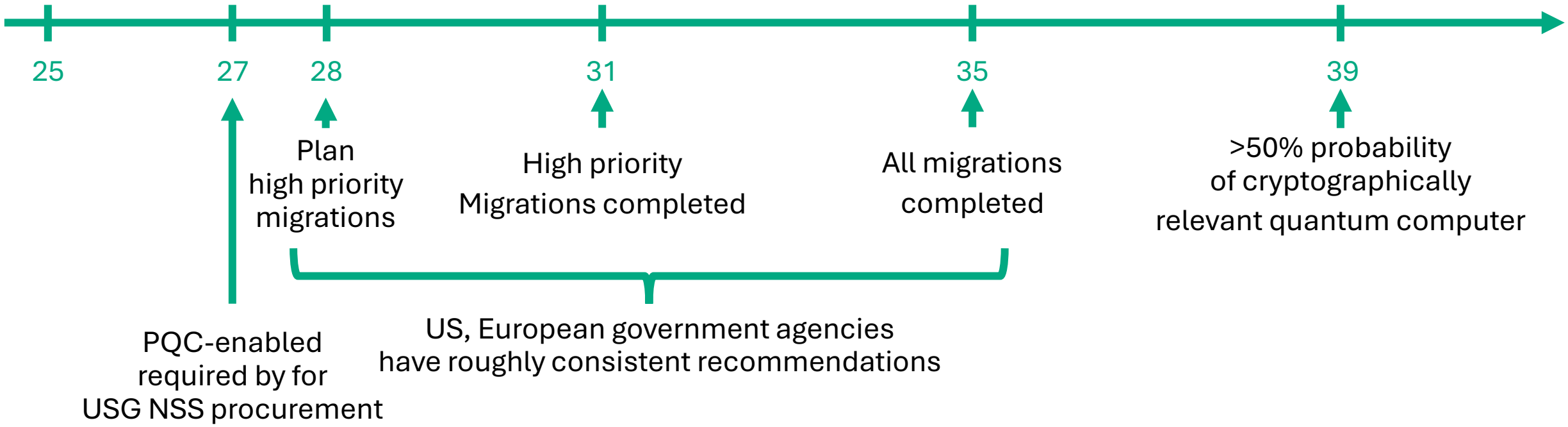
Maik Seewald
maseewald@cisco.com

July 28, 2025

Updating 802.1AR-2018 to support Post Quantum Cryptography (PQC)

- The US Quantum Computing Cybersecurity Preparedness Act (US 117-260) outlines a timelines for federal agency migration to post-quantum cryptography.
  - Transition starting in 2025 – this year
  - New equipment acquisitions supporting PQC by 2027
  - Full compliance to PQC support by the end of 2031
- US Commercial National Security Algorithm Suite 2.0 (CSNA 2.0, https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF) specifies requirements and recommended guidance for:
  - National Security Systems (NSS)
  - Department of Defense (DoD)
  - Defense Industrial Base (DIB)
- European and Asian governments have similar recommendations to US

The PQC timeline, must get started now



- Must get standards started now to enable silicon availability by 2028 for new equipment!
  - Government agencies need time to make a complete transition before 2039
- Though the probability of quantum computers is not likely until 2039 it could be sooner
- Governments are concerned about the threat of storing sensitive information today, then cracking it in the future

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) digital signatures

- The general purpose asymmetric algorithm required for digital signatures in any use case, including signing firmware and software by the CNSA 2.0 is the:
  - Module-Lattice-Based Digital Signature Algorithm (ML-DSA, previously CRYSTALS-Dilithium)
  - Use of high strength ML-DSA-87 for all classification levels
- Though not recommended for National Security Systems two lower strength ML-DSA algorithms are available for supporting less critical applications. These are:
  - ML-DSA-44 and ML-DSA-65
  - We recommend including these lower strength options

ML-DSA is both a must and the most desirable algorithm for device identity

- NIST has identified ML-DSA-87 as the only general algorithm accepted in CNSA 2.0
- ML-DSA key sizes are reasonable (though larger than RSA/ECC) and the computational requirements seem tractable for small devices like Trusted Platform Modules (TPMs)
- SPHINCS+ alternative requires substantially larger keys making it unattractive for small devices like TPMs
- LMS/XMSS can issue only a limited number of signatures until its state is exhausted rendering it unattractive for long-lived applications like DevID

Propose amendment to IEEE Std 802.1AR-2018 supporting Module-Lattice-Based Digital Signatures (ML-DSA)

- ML-DSA cryptographic algorithms (also called dilithium) are specified by the National Institute of Standards and Technology (NIST) in FIPS 204 https://csrc.nist.gov/pubs/fips/204/final
- Contribution with proposed changes in 802.1 public folder
  - https://www.ieee802.org/1/files/public/docs2025/new-bottorff-pqc-AR-amendment-proposal-0725-v04.pdf
  - The proposal relies on the IEFT draft in progress https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/ which specifies X.509 public key infrastructure algorithm identifiers for the ML-DSA algorithms

Stakeholders (some possible ones)

- government organizations,
- telecom,
- cloud providers,
- content providers,
- internet providers,
- utilities,
- any large business

Proposed Changes to 802.1AR-2018

- Clause 9 additions to include ML-DSA in signature suites (one page, see https://www.ieee802.org/1/files/public/docs2025/new-bottorff-pqc-AR-amendment-proposal-0725-v03.pdf
- Clause 5 additions for ML-DSA conformance requirements and Annex A PICS
- Clause 10 additions to include ML-DSA in SNMP MIB
- Miscellaneous references to NIST and TPG documents

- Note: IEEE Std 802.1AR-2018 does not include a YANG module
  - Our disposition is the development of a YANG module should be done as a separate amendment at a future time
  - Should be clarified in the project scope

Proposed Motion

- 802.1 authorizes the Security TG to generate a PAR and CSD at the September 2025 interim session for precirculation to the LMSC for an amendment to IEEE Std 802.1AR providing support for Device IDs utilizing cryptographic binding based on Module-Lattice-Based Digital Signatures (ML-DSA) as specified by the National Institute of Standards and Technology (NIST) in FIPS 204. .

Proposed Project Title

Standard for

Local and Metropolitan Area Networks –

Secure Device Identity

Amendment: Support for Module-Lattice-Based Digital Signatures

Proposed Project Scope

This amendment to IEEE Std 802.1AR-2018 introduces unique per-device identifiers (DevIDs) and their management, utilizing cryptographic binding based on Module-Lattice-Based Digital Signatures (ML-DSA) as specified by the National Institute of Standards and Technology (NIST) in FIPS 204. This enhancement aims to future-proof device authentication and management against quantum computing threats, ensuring robust security and interoperability across various network environments.

Proposed Project Purpose

This amendment incorporates the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) post-quantum cryptographic algorithms for device identification, ensuring robust security against both classical and quantum computer attacks. PQC supported DevIDs is expected to become a requirement for governments in 2027 with a full transition by 2031.

Proposed Need for the project

This amendment provides cryptographic algorithms which can secure devices against both classical and quantum computer attacks. These enhancements are needed in the next few year to support government procurements worldwide.

Thank You