P802.1AReg

Type of Project: Amendment to IEEE Standard 802.1AR-2018
Project Request Type: Initiation / Amendment
PAR Request Date:
PAR Approval Date:
PAR Expiration Date:
PAR Status: Draft
Root Project: 802.1AR-2018

1.1 Project Number: P802.1AReg
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Project Title: IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity Amendment: Support for Module-Lattice-Based Digital Signatures

3.1 Working Group: Higher Layer LAN Protocols Working Group(C/LAN/MAN/802.1 WG)
3.1.1 Contact Information for Working Group Chair:
Name: Glenn Parsons
Email Address: glenn.parsons@ericsson.com
3.1.2 Contact Information for Working Group Vice Chair:
Name: Jessy Rouyer
Email Address: jessy.rouyer@nokia.com
3.2 Society and Committee: IEEE Computer Society/LAN/MAN Standards Committee(C/LAN/MAN)
3.2.1 Contact Information for Standards Committee Chair:
Name: James Gilb
Email Address: gilb_ieee@tuta.com
3.2.2 Contact Information for Standards Committee Vice Chair:
Name: David Halasz
Email Address: dave.halasz@ieee.org
3.2.3 Contact Information for Standards Representative:
Name: George Zimmerman
Email Address: george@cmephyconsulting.com

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot: Dec 2026
4.3 Projected Completion Date for Submittal to RevCom: Jul 2027

5.1 Approximate number of people expected to be actively involved in the development of this project: 15
5.2.a Scope of the complete standard: This standard specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device to its identifiers, the relationship between an initially installed identity and subsequent locally significant identities, and interfaces and methods for use of DevIDs with existing and new provisioning and authentication protocols.
5.2.b Scope of the project: This amendment to IEEE Std 802.1AR-2018 provides unique per-device identifiers (DevIDs) and their management, utilizing cryptographic binding based on Module-Lattice-Based Digital Signatures (ML-DSA). The amendment will include support for DevIDs bound by the three algorithms ML-DSA-87, ML-DSA-65, and ML-DSA-44. In addition, the amendment will provide necessary changes to IEEE Std 802.1AR-2018 management modules for support of the ML-DSA algorithms.

5.3 Is the completion of this standard contingent upon the completion of another standard? Yes
Explanation: This standard uses work currently in draft at IETF as draft-ietf-lamps-dilithium-certificates titled Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA). The IETF work is essential since it provides the object identifiers which will be used in the amendment to identify ML-DSA. The IETF work is at a mature state in the IETF and is expected to be published as an RFC prior to completion of this amendment.
5.4 Purpose: This standard defines a standard identifier for IEEE 802 devices that is cryptographically bound to that device, and defines a standard mechanism to authenticate a device's identity. This facilitates secure device provisioning.

5.5 Need for the Project: Quantum computing may provide sufficient compute power to break the current set of cryptographic algorithms used for device identification. This amendment provides cryptographic algorithms which can secure devices against both classical and quantum computer attacks. PQC supported DevIDs are expected to become a requirement for governments in 2027 with a full transition required by 2031.

5.6 Stakeholders for the Standard: Government organizations, manufacturers, distributors, telecom, cloud providers, Internet providers, utilities, large businesses, and users of network-attached devices.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project? Yes

Explanation: ASCII use

6.1.2 Is the Standards Committee aware of possible registration activity related to this project? No

---

7.1 Are there other standards or projects with a similar scope? No

7.2 Is it the intent to develop this document jointly with another organization? No

---

8.1 Additional Explanatory Notes: