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 the Module-Lattice-Based Digital Signature Algorithm

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 adds support for unique per-device identifiers utilizing cryptographic binding based on the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) with the ML-DSA-87, ML-DSA-65, and ML-DSA-44 parameter sets.

5.3 Is the completion of this standard contingent upon the completion of another standard? ~~Yes~~ No
Explanation: ~~This standard relies on work which is currently in the RFC Editor's queue 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).~~
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 asymmetric keyed cryptographic algorithms used for device identification. The need is for the inclusion of cryptographic algorithms as part of IEEE Std 802.1AR-2018 Secure Device Identify, including identifiers for the algorithms, that are believed to secure devices against attacks from both classical and quantum

computers. ~~This amendment provides cryptographic algorithms which can secure devices against both classical and quantum computer attacks.~~ Post Quantum Cryptography supported DevIDs are expected to become a requirement for many governments in their procurements. ~~Post Quantum Cryptography supported DevIDs are expected to become a requirement for government procurements in January 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 computers and devices.

6.1 Intellectual Property

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

Explanation: The amendment is expected to include a fragment of Abstract Syntax Notation 1 (ASN.1) quoted from IETF RFC 9881. Copyright permission will be sought from the IETF Trust if needed~~The amendment will include a fragment of Abstract Syntax Notation 1 (ASN.1) quoted from an IETF RFC. Copyright permission will be sought from the IETF Trust~~.

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: #5.2.b: ML-DSA parameter sets are specified in National Institute of Standards and Technology (NIST—U.S. Department of Commerce) Federal Information Processing Standards (FIPS) 204 and in other national and international standards.~~#5.2.b: ML-DSA parameter sets are specified in National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 204 and in other national and international standards.~~

#4.2: This date is selected to meet the timeline expressed in the Need For the Project.

#5.5: Examples of procurements: In January 2027 in the United States of America, with a full transition by 2031, as prescribed in US Quantum Computing Cybersecurity Preparedness Act (US 117-260); Europe (Federal Office for Information Security's (BSI) TR-02102-1) and UK National Cyber Security Centre (NCSC—Timelines for migration to post-quantum cryptography) timelines are essentially aligned with U.S. mandates.