

P802.1AR

Type of Project: Revision to IEEE Standard 802.1AR-2018

Project Request Type: Initiation / Revision

PAR Request Date:

PAR Approval Date:

PAR Expiration Date:

PAR Status: Draft

Root Project: 802.1AR-2018

1.1 Project Number: P802.1AR

1.2 Type of Document: Standard

1.3 Life Cycle: Full Use

2.1 Project Title: Standard for Local and Metropolitan Area Networks - Secure Device Identity

Change to Title: ~~IEEE~~ Standard for Local and Metropolitan Area Networks - Secure Device Identity

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:

Mar 2027

4.3 Projected Completion Date for Submittal to RevCom: Nov 2027

5.1 Approximate number of people expected to be actively involved in the development of this project: 15

5.2 Scope of proposed 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.

5.3 Is the completion of this standard contingent upon the completion of another standard? No

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: Revision of this successful and widely used standard, published in 2018, is timely. This project will include editorial and technical corrections to existing functionality, and corrigenda and amendments approved at the time of completion.

Change to Need for the Project: ~~The secure device identity standardized by IEEE Std 802.1AR facilitates secure authentication of devices attached to a network, using (for example) IEEE Std 802.1X, successful and can be widely used as standard, an published enabling component in of 2018, security is solutions timely. This revision project will take include advantage editorial of and improvements technical in cryptographic technology corrections to add a stronger digital signature algorithm as existing an option functionality, using SHA-384 and the P-384 elliptic corrigenda curve~~

~~and to amendments align approved with at the Suite time B Certificate Profile (IETF RFC 5759). of~~
~~The project will also resolve any maintenance items submitted on IEEE Std 802.1AR completion.~~

5.6 Stakeholders for the Standard: Manufacturers, distributors, 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?

No

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: