P802.1AR

Submitter Email: mick_seaman@ieee.org
Type of Project: Revision to IEEE Standard 802.1AR-2009
PAR Request Date: 23-Jul-2016
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for a Revision to an existing IEEE Standard

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

2.1 Title: Standard for Local and metropolitan area networks - Secure Device Identity

Changes in title: ~~IEEE~~ Standard for Local and metropolitan area networks - Secure Device Identity

3.1 Working Group: Higher Layer LAN Protocols Working Group (C/LM/WG802.1)
Contact Information for Working Group Chair
Name: Glenn Parsons
Email Address: glenn.parsons@ericsson.com
Phone: 613-963-8141
Contact Information for Working Group Vice-Chair
Name: John Messenger
Email Address: jmessenger@advaoptical.com
Phone: +441904699309

3.2 Sponsoring Society and Committee: IEEE Computer Society/LAN/MAN Standards Committee (C/LM)
Contact Information for Sponsor Chair
Name: Paul Nikolich
Email Address: p.nikolich@ieee.org
Phone: 8572050050
Contact Information for Standards Representative
Name: James Gilb
Email Address: gilb@ieee.org
Phone: 858-229-4822

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 08/2017
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 02/2018

5.1 Approximate number of people expected to be actively involved in the development of this project: 15
5.2 Scope: 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 dependent 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. A verifiable unique device identity allows establishment of the trustworthiness of devices. This facilitates secure device provisioning.

5.5 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, and can be used to simplify security management as an enabling component of security solutions. This revision project will take advantage of improvements in cryptographic technology to add a stronger digital signature algorithm as an option, using SHA-384 and the P-384 elliptic curve to align with the Suite B Certificate Profile (IETF RFC 5759) and with expected updates to the TPM 2.0 specification in the Trusted Computing Group. The project will also resolve any maintenance items submitted on IEEE Std 802.1AR.

5.6 Stakeholders for the Standard: Manufacturers, distributors, and users of network-attached devices.

Intellectual Property
6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No
6.1.b. Is the Sponsor 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 Joint Development
Is it the intent to develop this document jointly with another organization?: No

8.1 Additional Explanatory Notes: #5.5 The extent of the changes required by an existing amendment project, P802.1ARce SHA-384 and P-384 Elliptic Curve, together with those required to update references and maintain consistency are more appropriate to a revision. This revision project will adopt the changes developed under P802.1ARce, and the P802.1ARce project will be withdrawn.