P802.1ARce

Submitter Email: gparsons@ieee.org
Type of Project: Amendment to IEEE Standard 802.1AR-2009
PAR Request Date: 12-Jun-2014
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for an Amendment to an existing IEEE Standard

---

1.1 Project Number: P802.1ARce
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 Amendment 1: SHA-384 and P-384 Elliptic Curve

---

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: gparsons@ieee.org
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: 857.205.0050
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: 03/2015
4.3 Projected Completion Date for Submittal to RevCom: 10/2015

5.1 Approximate number of people expected to be actively involved in the development of this project: 10
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: Amendment 1 specifies the optional use of the secure hash algorithm SHA-384 and the P-384 elliptic curve for use in Elliptic Curve Digital Signature Algorithm (ECDSA), and SHA-384 for hashing by the DevID module.

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 cybersecurity community wants to take advantage of recent improvements in cryptographic technology to use a stronger digital signature algorithm with IEEE Std 802.1AR, and in particular to use 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. To promote interoperability and ensure cryptographic quality, IEEE Standard 802.1AR requires that the cryptography used while claiming conformance is limited to that which is specified in the standard. This project will add the support for SHA-384 hash and P-384 elliptic curve as options.

5.6 Stakeholders for the Standard: Developers and users of networking equipment.

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 (Item Number and Explanation):