P802.1AEdk

Submitter Email: mick_seaman@ieee.org
Type of Project: Amendment to IEEE Standard 802.1AE-2018
PAR Request Date: 20-May-2019
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for an Amendment to an existing IEEE Standard

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

2.1 Title: Standard for Local and metropolitan area networks-Media Access Control (MAC) Security
Amendment 4: MAC Privacy protection

3.1 Working Group: Higher Layer LAN Protocols Working Group (C/LM/WG802.1)
Contact Information for Working Group Chair
  Name: John Messenger
  Email Address: j.l.messenger@ieee.org
  Phone: +441904699309
Contact Information for Working Group Vice-Chair
  Name: Jessy Rouyer
  Email Address: jessy.rouyer@nokia.com
  Phone: +1 469 661 2093

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: 05/2023
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 10/2023

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: The scope of this standard is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients.

5.2.b. Scope of the project: This amendment specifies privacy enhancements that complement existing IEEE Std 802.1AE MAC Security capabilities, and reduce the ability of external observers to correlate user data frames, their sizes, transmission timing and transmission frequency with users identities and activities. It specifies an encapsulation format that allows one or more user data frames and padding octets to be carried within the confidentiality protected data of consolidating frames, hiding the users MAC addresses and original frame sizes. The transmitter can balance the privacy improvement against the loss of efficiency and delay by controlling the sizes of consolidating frames and when they are transmitted. YANG configuration and operational state models are defined both for the existing functionality of IEEE Std 802.1AE and for the functionality to be added by this project. An SNMP MIB will be defined for the added functionality. This amendment also describes privacy considerations for the use, design, and deployment of bridged networks. This project includes technical and editorial corrections to existing functionality.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This standard will facilitate secure communication over publicly accessible LAN/MAN media for which security has not already been defined, and allow the use of IEEE Std 802.1X, already widespread and supported by multiple vendors, in additional applications.

5.5 Need for the Project: Even when data confidentiality protection is provided, unauthorized observers can correlate MAC addresses, frame sizes, and frame transmission timing with user identities, the applications being used, and with the content or purpose of LAN communications. Proprietary solutions to enhance privacy, guarding against such network traffic analysis have been developed. Vendors and users have expressed a desire for a standard interoperable solution for use in conjunction with IEEE Std 802.1AE MAC Security.

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?: Yes
If yes please explain: RAC review of previously reviewed text that may be included in this amendment is appropriate to assure terminology and descriptions of usage are correct and up to date.

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: #5.2B YANG is not an acronym, but a name. It has no useful expansion. SNMP is the commonly used distinguishing name for the management protocol with the trivial expansion Simple Network Management Protocol. MIB is the commonly used name for management objects, formally the Management Information Base, for that protocol.
#7.3 Adoption as an ISO/IEC Standard under the ISO/IEEE PSDO agreement. Refer to Jodi Haasz of IEEE Staff.