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: Media Access Control (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 MACsec 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 a consolidating frame, 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. This amendment 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 MACsec.

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: #7.3 Adoption as an International Standard under the existing PSDO agreement. Refer to Jodi Haasz of IEEE Staff.

myProject™ >> Submit a PAR

PAR for an Amendment to an existing IEEE Standard - P802.1AEdk

Section 1

1.1 AMENDMENT LETTER(S): dk

The IEEE myProject PAR input form provides a Download as PDF option, and the two pages above were created using that form and option. Unfortunately the downloaded PDF does not capture all the information on the form. I have found to this a nuisance in the past when trying to recall what was actually input, so the next three pages capture the form as set of screen shots.

The downloaded PDF is also inaccurate in one repect. There is a box that can be ticked to show that a Purpose clause is not included in the base standard (802.1AE-2018 does not include a Purpose clause) and once the box has been ticked no text for purpose appears. However the downloaded PDF does include an old and historic Purpose statement. It's probably harmless.
Mick

1.2 TYPE OF DOCUMENT: Standard

1.3 LIFE CYCLE: Full Use

Section 2

2.1 PROJECT TITLE: Standard for Local and metropolitan area networks-Media Access Control (MAC) Security

AMENDMENT TITLE: Amendment 4: Media Access Control (MAC) Privacy protection

Section 3

3.1 WORKING GROUP: Higher Layer LAN Protocols Working Group (C/LM/WG802.1)

3.2 SPONSORING SOCIETY AND COMMITTEE: IEEE Computer Society/LAN/MAN Standards Committee (C/LM)

3.3 JOINT SPONSOR:

Section 4

4.1 SPONSOR BALLOTING INFORMATION: Individual

4.2 EXPECTED DATE OF SUBMISSION OF DRAFT TO THE IEEE-SA FOR INITIAL SPONSOR BALLOT: May / 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.: Oct / 2023

Section 5

5.1 APPROXIMATE NUMBER OF PEOPLE EXPECTED TO BE ACTIVELY INVOLVED IN THE DEVELOPMENT OF THIS PROJECT:

15

5.2A SCOPE OF THE COMPLETE STANDARD:

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

5.2B SCOPE OF THE PROJECT:

This amendment specifies privacy enhancements that comple ment existing MACsec capabilities, and reduce the ability of ex ternal observers to correlate user data frames, their sizes, tra nsmission timing and transmission frequency with users identi ties and activities. It specifies an encapsulation format that all

5.3 IS THE COMPLETION OF THIS STANDARD CONTINGENT UPON THE COMPLETION OF ANOTHER STANDARD?:

○ Yes ⊙ No

5.4 WILL THE COMPLETE DOCUMENT (BASE + AMENDMENT) CONTAIN A PURPOSE CLAUSE?:

○ Yes ⊙ No

5.5 NEED FOR THE PROJECT:

Even when data confidentiality protection is provided, unautho rized observers can correlate MAC addresses, frame sizes, and frame transmission timing with user identities, the application s being used, and with the content or purpose of LAN commun ications. Proprietary solutions to enhance privacy, guarding ag

5.6 STAKEHOLDERS FOR THE STANDARD:

Developers and users of networking equipment.

Section 6

6.1 Intellectual Property:

A. IS THE SPONSOR AWARE OF ANY COPYRIGHT PERMISSIONS NEEDED FOR THIS PROJECT?:

○ Yes ⦿ No

B. IS THE SPONSOR AWARE OF POSSIBLE REGISTRATION ACTIVITY RELATED TO THIS PROJECT?:

⦿ Yes ○ No

If yes, please explain below:

RAC review of previously reviewed text that may be included i n this amendment is appropriate to assure terminology and d escriptions of usage are correct and up to date.

Section 7

7.1 ARE THERE OTHER STANDARDS OR PROJECTS WITH A SIMILAR SCOPE?: ○ Yes ● No ⓘ

7.2 JOINT DEVELOPMENT – IS IT THE INTENT TO DEVELOP THIS DOCUMENT JOINTLY WITH ANOTHER ORGANIZATION?: ○ Yes ● No ⓘ

Information from 7.3 - 7.4 is captured for potential follow up and coordination but will not appear on the final PAR view.

7.3 International Standards Activities

A. ADOPTIONS – IS THERE POTENTIAL FOR THIS STANDARD TO BE ADOPTED BY ANOTHER ORGANIZATION?: ● Yes ○ No ⓘ

If yes, please indicate the organization, technical committee name/number and contact person within external organization

ORGANIZATION: ISO/IEC JTC1 ▼

TECHNICAL COMMITTEE NAME:

TECHNICAL COMMITTEE NUMBER:

CONTACT NAME:

PHONE:

EMAIL:

B. HARMONIZATION – ARE YOU AWARE OF ANOTHER ORGANIZATION THAT MAY BE INTERESTED IN PORTIONS OF THIS DOCUMENT IN THEIR STANDARDIZATION DEVELOPMENT EFFORTS?: ○ Yes ● No ⓘ

7.4 DOES THE SPONSOR FORESEE A LONGER TERM NEED FOR TESTING AND/OR CERTIFICATION SERVICES TO ASSURE CONFORMITY TO THE STANDARD?: ○ Yes ● No

ADDITIONALLY, IS IT ANTICIPATED THAT TESTING METHODOLOGIES WILL BE SPECIFIED IN THE STANDARD TO ASSURE CONSISTENCY IN EVALUATING CONFORMANCE TO THE CRITERIA SPECIFIED IN THE STANDARD?: ○ Yes ● No

7.5 INDICATE IF YOU WOULD LIKE IEEE-SA STAFF TO SUBMIT YOUR PROJECT TO THE AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI) FOR APPROVAL CONSIDERATION AS AN AMERICAN NATIONAL STANDARD: ○ Yes ● No

Section 8

8.1 ADDITIONAL EXPLANATORY NOTES NOTE: IF APPLICABLE, INCLUDE SECTION/ ITEM # ABOVE WITH EXPLANATION:

#7.3 Adoption as an International Standard under the existing PSDO agreement. Refer to Jodi Haasz of IEEE Staff. ⓘ

Include the Item # in front of each explanation to distinguish which PAR field it is referring to.