P802.1AEef

Type of Project: Amendment to IEEE Standard 802.1AE-2018
Project Request Type: Initiation / Amendment
PAR Request Date:
PAR Approval Date:
PAR Expiration Date:
PAR Status: Draft
Root Project: 802.1AE-2018

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

2.1 Project Title: IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security Amendment: Ascon Cipher Suite

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: Apr 2027
4.3 Projected Completion Date for Submittal to RevCom: Apr 2028

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 optional use of the Ascon-AEAD128 authenticated encryption with associated data scheme, as specified in National Institute of Standards and Technology (NIST) SP 800-232, as a ~~MACsec (~~Media Access Control ~~s~~Security~~)~~ (MACsec) Cipher Suite.

5.3 Is the completion of this standard contingent upon the completion of another standard? No
5.4 Purpose: This document will not include a purpose clause.
Change to 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: To promote interoperability and ensure Cipher Suite quality, IEEE Standard 802.1AE requires that the Cipher Suites used while claiming conformance are limited to those specified in the standard. ~~There is a growing awareness for the need for~~ Network security requires data integrity, confidentiality, and origin authenticity for all network communication. NIST has selected the Ascon family of symmetric-key cryptographic primitives as ideal for resource-constrained environments, such as Internet of Things (IoT) devices, embedded systems, and low-powered sensors. This project adds support for an optional Ascon-AEAD128 based Cipher Suite, specifying the necessary mapping between protected frame fields and

parameters and the Key, Nonce~~, Tag~~, Associated Data, Plaintext, Ciphertext, and Tag parameters specified in NIST SP 800-232.

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

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?
Yes

Explanation: Registration Authority Committee (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 Is it the intent to develop this document jointly with another organization? No

---

8.1 Additional Explanatory Notes: #2.1 "Ascon" is a name, not an acronym, in the NIST (National Institute of Standards and Technology) SP 800-232 publication and is nowhere expanded in that publication.

#5.2.b "Ascon" and "Ascon-AEAD128" are names, not acronyms, in ~~the~~ NIST SP 800-232~~publication~~, although Ascon-AEAD128 is described as nonce-based authenticated encryption with associated data providing 128-bit security strength in the single-key setting.

#5.2.b NIST is the National Institute of Standards and Technology (U.S. Department of Commerce).

#5.2.b The full title of NIST SP 800-232 is:
"NIST Special Publication 800
NIST SP 800-232
Ascon-Based Lightweight Cryptography Standards for Constrained Devices
Authenticated Encryption, Hash, and Extendable Output Functions".