IEEE 802 LAN/MAN STANDARDS COMMITTEE (LMSC)

CRITERIA FOR STANDARDS DEVELOPMENT (CSD)

Based on IEEE 802 LMSC Operations Manuals approved 4 August 2020
Last edited 31 August 2020

P802.1AEef Standard for Local and metropolitan area networks—
Media Access Control (MAC) Security
Amendment: Ascon Cipher Suite

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 1.1, and the 5C requirements, 1.2.

1.1 Project process requirements

1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

a) The definitions will be part of this project.
b) The definitions will be part of a different project and provide the plan for that project or anticipated future project.
c) The definitions will not be developed and explain why such definitions are not needed.

Item c) is applicable to this project. The existing MIB and YANG modules were designed to support additional Cipher Suites without further change.

1.1.2 Coexistence

A WG proposing a wireless project shall prepare a Coexistence Assessment (CA) document unless it is not applicable.

a) Will the WG create a CA document as part of the WG balloting process as described in Clause 13? (yes/no)
b) If not, explain why the CA document is not applicable.

This project is not a wireless project; therefore, the CA document is not applicable.

1.2 5C requirements

1.2.1 Broad market potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

a) Broad sets of applicability.

The proposed amendment will facilitate the use of the Ascon Cipher Suite recently (August 2025) published as NIST SP 800-232 Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. Publication of this document marked the culmination of an international competitive effort begun in 2013 to provide efficient cryptographic solutions for resource-constrained environments, such as Internet of Things (IoT) devices, embedded systems, and low-power sensors. Further information is available at: https://csrc.nist.gov/pubs/sp/800/232/final

b) Multiple vendors and numerous users.

Multiple implementations of the Ascon-AEAD128 (Authenticated Encryption with Auxiliary Data) function needed for the proposed IEEE Std 802.1AE use, covering processors used in resource constrained environments, exist and include freely available and open-source implementations. The need to secure communication to wired (typically using 802.3) resource constrained devices is widely appreciated.

1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?

b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The project will be in conformance with IEEE Std 802, IEEE Std 802.1AC, and IEEE Std 802.1Q.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one describe why the proposed project is substantially different.

IEEE Std 802.1AE has an established and widely used distinct identity as a solution for securing wired network connectivity. The proposed project will increase its applicability, but is not expected to materially reduce the use of existing Cipher Suites.

1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.

Multiple implementations of the Ascon-AEAD128 cryptographic function to be used have been developed and analyzed.

b) Proven similar technology via testing, modeling, simulation, etc.

The use of Ascon-AEAD128 is expected to follow the blueprint established for existing widely deployed Cipher Suites

1.2.5 Economic Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Known cost factors.

The cost factors of Ascon implementations have been extensively analyzed as part of its selection by the NIST organized competition for secure communication support for resource constrained devices.

b) Balanced costs.

The proposed project does not change the cost characteristics of bridges and end stations.

c) Consideration of installation costs.

Installation costs for use of this technology are believed to be acceptable given the need for communication security, and have been an important consideration throughout its development.

d) Consideration of operational costs (e.g., energy consumption).

The use of the Ascon Cipher Suite should reduce energy consumption as compared to existing alternatives. The administrative costs associated with its use should not be materially different to those for existing deployed alternatives.

e) Other areas, as appropriate.

No other areas have been identified.