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

# 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.

## Project process requirements

### Managed objects

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

1. The definitions will be part of this project.

Yes, the definition will be part of the project.

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

### Coexistence

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

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

No CA document is needed, as this amendment only adds new cryptographic algorithms to existing IEEE Std 802.15.4.

## 5C requirements

### Broad market potential

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

1. Broad sets of applicability.
2. Multiple vendors and numerous users.

IEEE Std 802.15.4 was designed using advanced encryption standard extension of counter mode encryption and cipher block chaining message authentication code (AES-CCM\*). Adding the more efficient drop in replacement cipher Ascon-128 and/or Ascon-128a will make more lightweight implementations available. The Ascon family has been selected as the US National Institute of Standards and Technology (NIST) lightweight cryptographic algorithm, making its use in the future more widespread.

There are many silicon and system vendors already producing devices and systems using IEEE Std 802.15.4 for use in Internet of Things (IoT) applications. This includes consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community.

### 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.

1. Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?

No.

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

This project is an amendment to an existing standard for which it has been previously determined that compliance with IEEE Std 802.1Q is not possible. The project will comply with IEEE Std 802 using either local or global MAC addresses.

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.

### 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 802.15.4 was developed to address the needs of IoT networks and is used in those areas. Adding Ascon-128 and/or Ascon-128a to the standard will allow devices to use more lightweight cryptographic algorithms. Ascon-128 and Ascon-128a offer functionality not available in AES, like hashing and key material extraction, so it can be used in more cases than AES.

### 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:

1. Demonstrated system feasibility.
2. Proven similar technology via testing, modeling, simulation, etc.

Ascon was announced as winner of the NISTs lightweight cryptographic standard competition. During the competition it received a large number of third party reviews, and verifications.

There are multiple existing implementations of it. It uses the same authenticated encryption with associated data (AEAD) framework as used in the IEEE Std 802.15.4, thus dropping it in to the existing IEEE Std 802.15.4 security framework should be straightforward.

### 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:

1. Balanced costs.
2. Consideration of installation costs.
3. Consideration of operational costs (e.g., energy consumption).
4. Other areas, as appropriate.

Ascon provides a smaller footprint than AES for hardware implementations, and it is faster on pure software implementations, thus it allows making lower cost implementations than currently possible. The cost of the implementation should be same in both coordinators and devices, and there is no special installation or operational costs.