**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **IEEE 802.15.4y Draft CSD** |
| Date Submitted | [18 January 2018] |
| Source | [Don Sturek][Itron][address] | Voice: [ ]Fax: [ ]E-mail: [ ] |
| Re: |  |
| Abstract | [CSD for 802.15.4y SECN] |
| Purpose | [CSD for 802.15.4y SECN] |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

CRITERIA FOR STANDARDS DEVELOPMENT (CSD)

Based on IEEE 802 LMSC Operations Manuals approved 13 November 2015

Last edited 3 December 2015

 **Title:**

Amendment defining security extensions to IEEE Std. 802.15.4 adding at a minimum Advanced Encryption Standard (AES)-256

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

###  Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (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) No
2. If not, explain why the CA document is not applicable. This project defines extensions to the IEEE Std 802.15.4 MAC security to support additional encryption modes and key lengths.

## 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.

IEEE Std 802.15.4 was originally designed for constrained devices with a single encryption method using AES-128. Since inception, IEEE Std. 802.15.4 has been deployed in mission critical applications for industries like building automation and utility distribution automation where long deployment life is now requiring future support for AES-256 and further extensibility for Quantum Computing attacks.

1. Multiple vendors and numerous users.

There are many silicon and system vendors already producing devices and systems using IEEE Std 802.15.4 for use in IoT applications. This includes things like 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? While the Security Next Generation (SECN) extensions to IEEE Std 802.15.4 shall comply with IEEE Std 802, it cannot comply with IEEE Std 802.1Q and IEEE Std 802.1AC because IEEE Std 802.15.4 uses 64-bit MAC addresses.

b) If the answer to a) is no, supply the response from the IEEE 802.1 WG. As stated earlier, the SECN extensions apply to the existing standard (IEEE Std 802.15.4) for which it has been previously determined that compliance with IEEE Std 802.1Q and IEEE Std 802.1AC is not possible due to IEEE Std 802.15.4 using 64-bit MAC addresses

* + 1. 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 specifically to optimally address the needs of IoT networks and is broadly used in that application. It remains unique in that regard. The SECN extensions serve to meet current User demand and to help increase the competitive edge of the 802.15.4 standard. The SECN extensions are unique in the existing standard which is currently limited to AES-128 encryption or no security.

### 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.

AES-256 is an existing security mode identified by the National Institute of Standards and Technology (NIST) [Federal Information Processing Standards](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standards) (FIPS) 197 for use in Smart Grid and related critical infrastructure deployments.

1. Proven similar technology via testing, modeling, simulation, etc.

The AES-128 standard is already used in IEEE 802.15.4. The addition of AES-256 is the same standard with a longer key length.

### 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 (infrastructure versus attached stations).

Implementing the SECN amendment will be a firmware implementation on today’s faster and already cheaper devices. The proposed project does not affect the balance of costs between the infrastructure and attached stations.

1. Known cost factors.

Devices of similar functionality are in high volume shipment today, so cost factors are well known and acceptable

1. Consideration of installation costs.

No special manufacturing requirements for use of these devices are needed; additionally use of this amendment may reduce installation costs of IEEE Std. 802.15.4 devices due to more automated configuration.

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

These are low energy consumption components which are part of a larger product. Additionally, the cost of the increased overhead of the SECN amendment is significantly outweighed by the benefits it provides to the use of IEEE Std. 802.15.4 devices in various internet protocol applications.

1. Other areas, as appropriate.