**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Standard for Transport of Key Management Protocol (KMP) Datagrams | |
| Date Submitted | [14 May 2019] | |
| Source | [Tero Kivinen] [] [] | Voice: [ ] Fax: [ ] E-mail: [ ] |
| Re: |  | |
| Abstract | [CSD for 802.15.9 revision] | |
| Purpose | [CSD for 802.15.9 revision] | |
| 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:**

IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams

# 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 is about the transport of the key management protocol datagrams. There is no impact on coexistence.

## 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.

Security is a key aspect of current Internet of Things (IoT) applications, remote controls, sensor networks, as well as many other applications that utilize IEEE Std 802.15.4. IEEE Std 802.15.9 Recommended Practice currently provides the methodology for key management for IEEE Std 802.15.4. While the existing combination is widely used, it is reaching its limits. The conversion of the Recommended Practice to a Standard and the addition of additional security key management protocols is required for continued broad application deployments in this rapidly growing market.

1. Multiple vendors and numerous users.

There are many silicon and system vendors already producing devices and systems using IEEE Std 802.15.4 and IEEE Std 802.15.9 for use in IoT and many other 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? Yes.

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

* + 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 802.15.9 was developed specifically to optimally address the KMP needs of IoT and other networks utilizing IEEE Std 802.15.4, and is broadly used in those applications. It remains unique in that regard. The security KMP extensions serve to meet current user demand and to help increase the competitive edge of the IEEE Std 802.15.4. The proposed security KMP extensions are unique from features in the existing Recommended Practice which does not address key lengths other than 128-bits or security algorithm selection.

### 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.

IEEE Std 802.15.9 provides encapsulation of existing, mature key management protocols to address the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57 part 1 for IEEE Std 802.15.4 devices.

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

The IEEE Recommended Practice 802.15.9 provides an encapsulation for existing key management protocols like IEEE 802.1X for IEEE 802.15.4 devices. The addition of session key derivation text for security keys of different sizes (for support of IEEE P802.15.4y), broadcast/multicast key generation and security algorithm selection (again supporting IEEE P802.15.4y), will permit additional support of existing security key management protocols. These protocols are already in wide use in other market sectors and are just being brought in to the IEEE Std 802.15.4 application space

### 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 IEEE Std 802.15.9 is 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.

Existing equipment may be upgradable via firmware. Installation costs would not vary from current products implementing the standard.

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 IEEE Std 802.15.9 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.