**IEEE 802.15**

**Wireless Specialty Networks (WSN)**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Specialty Networks (WSN) |
| Title | **802.15 Standing Committee Maintenance – Response to comment received from ISO/IEC JTC1/SC6 for IEEE Std 802.15.7**  |
| Date Submitted | [November 14, 2024]  |
| Source | [Phil Beecher][Wi-SUN Alliance] | email: [pbeecher@wi-sun.org] |
| Re: | [November 2024, 802.15 Session] |
| Abstract | [IEEE 802.15 SCM contribution] |
| Purpose | [IEEE 802.15 SCM contribution] |
| Notice | This document has been prepared to assist the IEEE 802.15. 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 802.15. |

**Thursday 14 November 2024**

**Comment received from China National Body w.r.t. submission of IEEE Std 802.15.7:**

CCM\* are mandatorily based on AES encryption algorithm without other options.

Actually, a cryptographic algorithm is one module of a security protocol, and it is usually used in the

security protocol. The security protocol and cryptographic algorithm is relatively independent, and the security protocol is applicable to multiple different cryptographic algorithms. Cryptographic algorithms are only adoptable modules, and which algorithm to be applied is subject to the user’s

requirement and national/regional laws and regulations.

But in this proposal, only AES is specified. That’s to say, the compliance to the proposal is being bound by using AES. It causes the neglect of other nations’ interests and makes the proposal not applicable in different nations.

**Planned response:**

“IEEE Std 802.15.7 specifies AES CCM\* as a mandatory cipher suite.  There is nothing to prevent additional, optional cipher suites being implemented to meet specific national interests”

Approved by unanimous consent.