**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 802.15.9** | |
| Date Submitted | [January 18, 2024] | |
| Source | [Phil Beecher]  [Wi-SUN Alliance] | email: [pbeecher@wi-sun.org] |
| Re: | [January 2024, 802.15 Session] | |
| Abstract | [IEEE 802.15 TG4me Minutes] | |
| Purpose | [IEEE 802.15 TG4me Minutes] | |
| 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. | |

**Monday 15 January 2024**

**Comment received from China National Body w.r.t. submission of IEEE Std 802.15.9:**

The KMP protocol includes 802.1X MKA as a protocol option in 8.2. However, China NB have voted against IEEE 802.1X and submitted technical comments pointing out the security flaws during its pre-ballot and FDIS ballot as described in 6N15555 and 6N15771, such as “cannot achieve the real mutual authentication between the Supplicant and Authenticator”, but those comments have not been disposed reasonably. KMP will inherit the security flaws of 802.1X by including 802.1X MKA as a protocol option.

**Planned response:**

(Note, this response is identical to a previous response from 802.1 to ISO/IEC JTC1/SC6 - 802.1Qcz-2023)

The documents referenced in the China NB ballot comment (i.e., 6N15555 and 6N15771) are the Summary of Voting on IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) documents which date from 2013; IEEE 802 responses to these comments were submitted to ISO/IEC JTC1 SC6 at the time. The general assertions raised in the China NB’s ballots were discussed at length in 2013 at the IEEE 802 meeting in Geneva (with IEEE 802 and Switzerland NB representatives in attendance) and in both 2013 and 2014 at SC6 meetings in Seoul and Ottawa (with IEEE 802, China NB, and Switzerland NB representatives in attendance). During those meetings, IEEE 802 fully responded to all claims made by both the China NB and Switzerland NB representatives and presented additional information about the design and specification of IEEE 802 technologies. Additionally, at the SC6 meeting in Ottawa in early 2014, the China NB and Switzerland NB representatives committed to providing technical details to justify their concerns. There have been no submissions from the China NB or Switzerland NB and there has been no detailed technical information or discussion shared since that time.

IEEE 802 has supplied a number of communications about the security technology specified in the IEEE 802 security standards: explaining why attacks referenced in China NB contributions are not effective (and will fail); illustrating the use of certificates in IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) and describing how the use of the mutual authentication methods specified in IEEE Std 802.1X does not expose the public network or its user to (unspecified) security problems.

The China NB has repeatedly claimed there are “security problems”; however, these assertions have not been substantiated, despite requests for further information from IEEE 802. The invitation for a representative of the China NB (as well as representative from other interested SC6 NBs) to attend an IEEE 802 Plenary meeting remains open.

 IEEE 802 believes that the “security defects” in IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) described by the China NB have all been shown to be not valid but continues to invite the China NB to submit any additional technical details for consideration. IEEE 802 welcomes the opportunity to discuss further the details of any new concerns about IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) from the China NB. In the absence of any technical substantiation of the claims, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.

Approved by unanimous consent.