**IEEE P802.15**

**Wireless Specialty Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Specialty Networks (WSNs) |
| Title | **TG 802.15.4ae comments to NIST SP 800-232 initial public draft** |
| Date Submitted | 11th November 2024 |
| Source | Tero Kivinen | E-Mail: kivinen@iki.fi |
| Abstract | Comments relating to the NIST SP 800-232 initial public draft related to the ASCON Tag generation requirement R3 |
| Purpose | Propose changes to NIST SP 800-232 initial public draft so that it can be used with current IEEE Std 802.15.4. |
| 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. |

##

IEEE 802 comments to the NIST SP 800-232 initial public draft

NIST SP 800-232 initial public draft in section 4.3 has requirement R3 as follows:

R3. Minimum length of truncated tag. When an application uses truncated tags, the bit length of the truncated tags shall be at least 64 bits, and the tag length shall be the same across the life-span of the key.

**Comments:**

1. In the IEEE Std 802.15.4™ there is three possible tag lengths MIC-32, MIC-64, and MIC-128. The current text in R3 does not allow using 32-bit tag lengths.
2. IEEE Std 802.15.4™ allows using different tag lengths for the same key, and encodes the tag length inside the Nonce, so each tag length will be using different Nonce value. The current text in R3 does not allow this construct to be used.

**Background:**

Nonce in IEEE Std 802.15.4 is generated as follows:

|  |  |  |
| --- | --- | --- |
| **Octets: 8** | **4** | **1** |
| Source Address | Frame Counter | Nonce Security Level |

Where the Nonce Security Level contains the security level of the frame as integer, and that defines the tag length to be used:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security level** | **Security attributes** | **Data confidentiality** | **Data authenticity** | **MIC length (octets)** |
| 0 | None | OFF | NO | 0 |
| 1 | MIC-32 | OFF | YES | 4 |
| 2 | MIC-64 | OFF | YES | 8 |
| 3 | MIC-128 | OFF | YES | 16 |
| 4 | Reserved |
| 5 | ENC-MIC-32 | ON | YES | 4 |
| 6 | ENC-MIC-64 | ON | YES | 8 |
| 7 | ENC-MIC-128 | ON | YES | 16 |

**Request:**

To allow future IEEE Std 802.15.4™ implementations to use NIST approved Ascon cipher, the R3 requirement would need to be changed to allow 32-bit tags, and allowing using different tag lengths with same key provided that nonce for each tag length is generated in such way that no same nonce can be used with two different tag lengths.