**IEEE P802.15**

**Wireless Specialty Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Specialty Networks (WSNs) | |
| Title | **TG 802.15.4ae List of changes to the IEEE Std 802.15.4** | |
| Date Submitted | 9th September 2024 | |
| Source | Tero Kivinen | E-Mail: kivinen@iki.fi |
| Abstract | List of changes needed in the IEEE Std 802.15.4 to add ASCON. | |
| Purpose | Getting ready for draft proposal. | |
| 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. | |

1. Changes to Clause 9

Add ASCON algorithm to Table 9-9.

1. New annex Ba for specifying how to use AEAD ciphers in general

The new annex would specify how to use AEAD just like the Annex B now specifies how to use AES-CCM\* and AES-CCM modes of operation. This might not be even needed if the text in Section 9.3.2 is enough. Or we might just update the text in 9.3.2 to be sufficient.

Ba.1 Introduction

Ba.2 Symmetric-key cryptographic building blocks

Ba.2.1 General

Ba.2.2 Block cipher

Ba.3 Specification of AEAD operations

Ba.3.1 AEAD encryption and authentication transform

Ba.3.2 AEAD decryption and authentication checking transformations

1. Create test vector document in mentor

Create document providing test vectors using ASCON and add reference to that in Table 9-9.