**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **LB225/D03 comment resolution -- CID 41 and 44** |
| Date Submitted | Oct 15, 2025  |
| Sources | Alex Krebs (Apple)krebs @ apple.com |
| Re: |  |
| Abstract |  |
| Purpose | To propose resolution for MMS related comments for “P802.15.4ab™/D03 Draft Standard for Low-Rate Wireless Networks”. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ab Task Group. It represents only the views of the participants listed in the “Sources” field above.It is offered as a basis for discussion and is not binding on the contributing individuals. The material in this document is subject to change in form and content after further study. The contributors reserve the right to add, amend or withdraw material contained herein. |

# CID 41, 44 (Rejected)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Index #** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| 41 | 99 | 10.39.11.1.2.1 | 12 | My comment 94 was rejected because there was no alternative text. This comment will provide that alternative text.  | Remove 2nd sentence of 2nd paragraph of 10.39.11.1.2.1 (starting at line 12, ending at line 14. Replace it as follows: "The RPA Hash field value is calculated by doing an AEAD encryption operation (Section 2.1 of RFC 5116) with following parameters: secret key K=IdentityResolvingKey, nonce N = 0x00 ... 00, plaintext P = empty, and associated data A = RPA prand. The RPA Hash field value is then taken as bits 0 to 23 of the output ciphertext C. The AEAD algorithm used is specified by the macIrkAlgorithmId." |
| 44 | 152 | 10.39.12 | 6 | Add macIrkAlgorithmId.  | Add macIrkAlgorithmId with type of "Integer", Range "as defined in Table 9-9", and description of "The AEAD algorithm used when generating RPA Hash values from IRK". |

Discussion: The discussion on D02/CID 94 was that independent of the missing text change proposal the group does not see a need to introduce "algorithmic agility" for RPAs. Additionally it was discussed that the definitions in 802.15.4ab-D02 for generating the RPAs are specific to AES-128 and additional text changes in various sections would be needed to make RPA generation suitable for SHA-2 class hash algorithms. The newly proposed change includes specific text to change, but fails to resolve the issues mentioned. Additionally, it is unclear what is the benefit of replacing the existing definition of AES-128 in B.2.2 as referenced in D03 on page 99 with the AEAD encryption operation from RFC5116. RFC5116 only defines an interface to GCM and CCM stream cipher operation modes, but the operation described in D03 is a AES-128 block cipher operation of which the result is identical to the first 16 octets of the ECB stream cipher. Even if ECB was referenced, it would be unclear why devices would have to implement a stream cipher mode instead of simply using the AES-128 block operation as currently defined.

Proposed resolution: Rejected.

Disposition detail: Algorithmic agility is undesired and leads to implementation ambiguity.