**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **LB214/D01 comment resolution -- Proposed change to add support for ad-hoc extended privacy addresses** |
| Date Submitted | April 8, 2025 |
| Sources | Alex Krebs (Apple)krebs @ apple.com |
| Re: |   |
| Abstract |  |
| Purpose | Supportive material for comments submitted to 802.15.4ac letter ballot 214. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ac 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. |

---- Start of change 1 ----

Instructions to editor: On p.17, at the end of l. 15 insert

The privacy network ID may be used to generate ad-hoc extended privacy addresses as defined in 10.9a.2.5.

---- End of change 1 ----

---- Start of change 2 ----

Instruction to editor: On p.19, after l.15, insert

For some applications it may not be suitable to request a list of extended privacy addresses as described in 10.9a.3.1. Instead, an adhoc extended privacy addresses may be generated by means of the privacy network ID as the result of AES-128(key, data), where key is the MSB-wise zero padded privacy network ID, data is a 128-bit MSB-wise zero padded 24-bit value, and AES-128 is the 128-bit output of the block cipher from [B.2.2]. The extended privacy address is given by the data and the output of the AES-128 operation as shown in Figure 10-124x.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| RMO-->LMO | Octet 8 RMO | Octet 7 | Octet 6 | Octet 5 | Octet 4 | Octet 3 | Octet 2 | Octet 1 LMO |
| LSB --> MSB | 00000000 | data Bits-16-23 | data Bits 8-15 | data Bits 0-7 | Output of AES-128 Bits 15-23 | Output of AES-128 Bits 8-15 | Output of AES-128 Bits 0-7 | 01110000 MXYZST.. |

Figure 10-124x—Generation of an ad-hoc extended privacy address key from privacy network ID

---- End of change 2 ----