**IEEE P802.15**

**Wireless Specialty Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Specialty Networks (WSNs) |
| Title | Miscellaneous Comments, Part 1 |
| Date Submitted | 14-Novemner-2024 |
| Source | [Benjamin Rolfe][Blind Creek Associates][Benjamin A. Rolfe][BCA] | E-mail: [ben.rolfe @ ieee.org ]  |
| Re: | Resolving comments form LB207 |
| Abstract | Proposed resolutions to CIDs 1026, 457, 1388, 512, 513 |
| Purpose | Make the world better by encouraging adoption and productive use of 802.15 standards based on accurate information |
| 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. |

# Introduction

This document addresses the following comments: 1026, 457, 1388, 512, 513

Comments:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Sub-clause** | **Line #** | **Comment** | **Proposed Change** |
| 1026 | 19 | 7.4.4 | 6 | In Table 7-9 the "Use Description" reference for these new IEs is not present. If they don't have a described use then they should be removed.  | Determine the most relevant clause reference for each of these IEs and insert it into the table. |
| 457 | 72 | 10.38.7.4.3 | 19 | PRNG usually generates sequence of integers, in case of using AES-128 this is not really a case. It generates sequence of blocks which consists of sequence of bits and/or octets. Using term least significant will cause confusing as it would assume that the AES function wound return integer, which it does not.  | Change to leftmost 32 bits, which matches how section 4.4 defines the strings. |
| 1388 | 72 | 10.38.7.4.3  | 21 | As pointed out similarly for RPA\_hash calculation before, modulo operation is not defined for AES-128 block output. We can use similar language here to fix. | Replace lines 19-21 by:The *PrngValue* is thengiven by bits 0 to 31 of *NbaPrng(macMmsPrngSeed, RangingBlockIndex)*Also change line 24 to:where MOD is the integer modulus operator, ~~and~~ n is the length of macMmsNbChannelAllowList, and input/outputs of *NbaPrng* are MSB zero-padded unsigned integers. |
| 512 | 85 | 10.38.9.3.11 | 4 | The table 14 defines more than just the valid range.  | Change text to say that Number of RSF values are defined in table 14. |
| 513 | 85 | 10.38.9.3.11 | 8 | The table 15 defines more than just the valid range.  | Change text to say that table defines the values, not range. |

# Resolutions

## CID 512

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 512 | 85 | 10.38.9.3.11 | 4 | The table 14 defines more than just the valid range.  | Change text to say that Number of RSF values are defined in table 14. |

Resolution detail: change text to:

The Number of RSF field specifies the number of RSF segments in the UWB MMS packet and shall be set to one of the non-reserved values in Table 14.

## CID 513

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 513 | 85 | 10.38.9.3.11 | 8 | The table 15 defines more than just the valid range.  | Change text to say that table defines the values, not range. |

The Number of RIF field specifies the number of RIF segments in the UWB MMS packet and shall be set to one of the non-reserved values in Table 15.

## CID 1388

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1388 | 72 | 10.38.7.4.3  | 21 | As pointed out similarly for RPA\_hash calculation before, modulo operation is not defined for AES-128 block output. We can use similar language here to fix. | Replace lines 19-21 by:The *PrngValue* is thengiven by bits 0 to 31 of *NbaPrng(macMmsPrngSeed, RangingBlockIndex)*Also change line 24 to:where MOD is the integer modulus operator, ~~and~~ n is the length of macMmsNbChannelAllowList, and input/outputs of *NbaPrng* are MSB zero-padded unsigned integers. |

Recommended resolution: Accepted

Discussion: The proposed change removes ambiguity of which bits of a block of bits are intended and clarifies that it is the input to the PRNG (both integers) that are being padded.

## CID 457

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 457 | 72 | 10.38.7.4.3 | 19 | PRNG usually generates sequence of integers, in case of using AES-128 this is not really a case. It generates sequence of blocks which consists of sequence of bits and/or octets. Using term least significant will cause confusing as it would assume that the AES function wound return integer, which it does not.  | Change to leftmost 32 bits, which matches how section 4.4 defines the strings. |

Recommended resolution: Revised

Resolution Detail:

Replace lines 19-21 by:

The PrngValue is then

given by bits 0 to 31 of NbaPrng(macMmsPrngSeed, RangingBlockIndex)

Also change line 24 to:

where MOD is the integer modulus operator, and n is the length of macMmsNbChannelAllowList, and input/outputs of NbaPrng are MSB zero-padded unsigned integers.

Discussion: This is the resolution proposed in comment 1388 which is technically correct.

## CID 1026

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1026 | 19 | 7.4.4 | 6 | In Table 7-9 the "Use Description" reference for these new IEs is not present. If they don't have a described use then they should be removed.  | Determine the most relevant clause reference for each of these IEs and insert it into the table. |

Proposed resolution: Revised

Resolution detail: Add the references to **Use description column** as shown:

|  |  |
| --- | --- |
| **Name** | **Use description** |
| Scheduling IE  | 10.3210.39 |
| Enhanced Ranging Round IE (ERR IE) | 10.32.3.5 10.32.8.110.32.9.4 |
| Hyper Block Structure IE (HBS IE)  | 10.32.3.510.38.9.6  |
| Application Control IE (AC IE)  | 10.39.4.310.39.4.610.39.5.310.40.210.40.4 |
| CIR Report IE  | 10.39.4.610.39.5.310.39.6.1 |
| SBP Request IE  | 10.39.5.210.39.6.5 |
| SBP Response IE  | 10.39.5.210.39.6.5 |
| SBP Termination  | 10.39.5.4 |
| Processed Target Feature Report IE | 10.39.4.5 |
| Dynamic Data Mode Negotiation IE (DDMN IE) | 10.41.210.41.3 |
| NB Allocation IE | 10.43.210.43.3 |

Discussion: non required.