**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | **Resolution proposal regarding MMS MAC-public part 3 for P802.15.4ab™/Draft (pre-ballot) C** | |
| Date Submitted | Mar 2024 | |
| Sources | Hong Won Lee, Insun Jang, Jinsoo Choi, HanGyu Cho (LG Electronics) |  |
| Re: | Contribution to IEEE 802.15.4ab | |
| Abstract |  | |
| Purpose | To propose comments and proposed changes to “P802.15.4ab™/ Draft (pre-ballot) C 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. | |

|  |
| --- |
| **Abstract**  This submission contains the proposed comment resolutions for the CIDs 166, 510 and 511  R0: initial document |

***This document aims to propose a resolution proposal regarding MMS comments for P802.15.4ab™/*** ***Draft (pre-ballot) C Draft Standard***

***Comment index #510 in 15-24-0010-14-04ab-tg4ab-consolidated-comments-draft-c.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Pg** | **Sub-clause** | **Ln** | **Comment** | **Proposed change** | **Disposition** |
| Tero Kivinen | 510 | 55 | 10.38.7.2 | 6 | What is this IRK generation for public addresses trying to do? The entropy of the key is only 48 bits, thus is it is trivial to brute force the key. | Describe what the security properties of the useless IRK generation is, and include note, that it is completely unsecure as it will be trivially brute forced. Remove the whole compact frame format and the public/private addresses defined by it, and use standard frames, and privacy defined by the 4ac. | Revised |

**Discussion:**

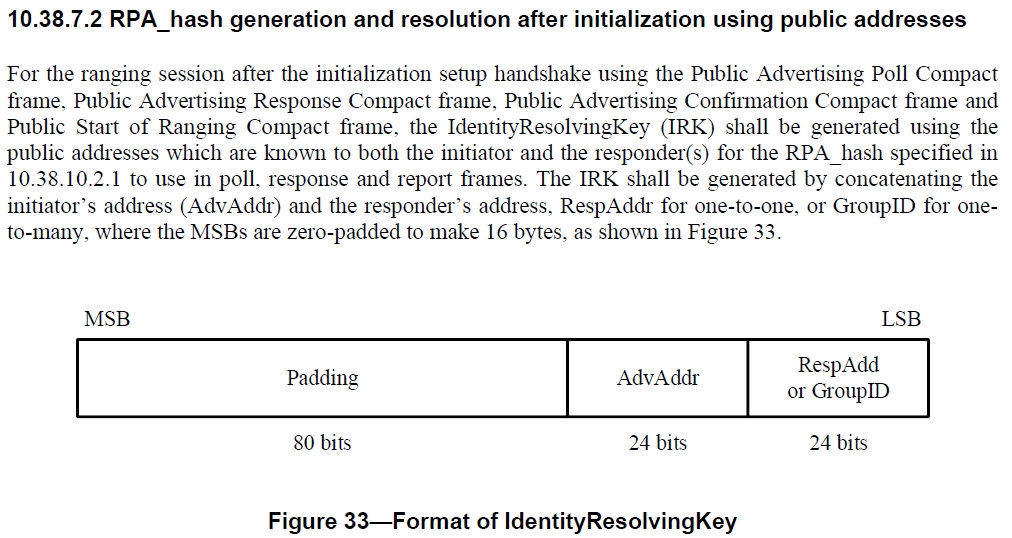
Regarding describing the security properties of the public IRK generation, the note describing the purpose of the public IRK usage is added. Regarding remove the whole compact frame format, it was discussed, however the conclusion is not made yet. Disposition should be aligned with CIDs 497 and 507 in 15-24-0223-01-04ab-draftc-comment-resolution-compact-frames-rpa-cids-497-507-508-509. This resolution proposal is focused on the security properties of the public IRK generation

**Resolution: Revised**

**Proposed text change on P802.15.4ab™/Draft (pre-ballot) C:**

**10.38.7.2 RPA\_hash generation and resolution after initialization using public addresses**

**- Original Text**

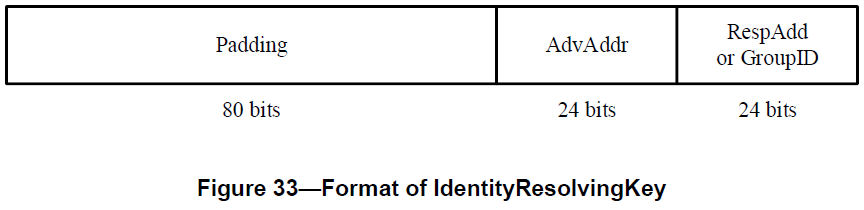


**- Proposed change**

***Revise the sub-clause 10.38.7.2 RPA\_hash generation and resolution after initialization using public addresses in IEEE P802.15.4ab/Draft (pre-ballot) C as follows:***

***pp. 55 L15***

For the ranging session after the initialization setup handshake using the Public Advertising Poll Compact frame, Public Advertising Response Compact frame, Public Advertising Confirmation Compact frame and Public Start of Ranging Compact frame, the IdentityResolvingKey (IRK) shall be generated using the public addresses which are known to both the initiator and the responder(s) for the RPA\_hash specified in 10.38.10.2.1 to use in poll, response and report frames. The IRK shall be generated by concatenating the initiator’s address (AdvAddr) and the responder’s address, RespAddr for one-to-one, or GroupID for one-to-many, where the MSBs are zero-padded to make 16 bytes, as shown in Figure 33.



Note - Generating an IRK using public addresses is not intended to protect the privacy of a device. The primary purpose of using the IRK is to generate RPA\_Hash for reuse in poll, response and report frames

***Comment index #511 in 15-24-0010-14-04ab-tg4ab-consolidated-comments-draft-c.xlsx***

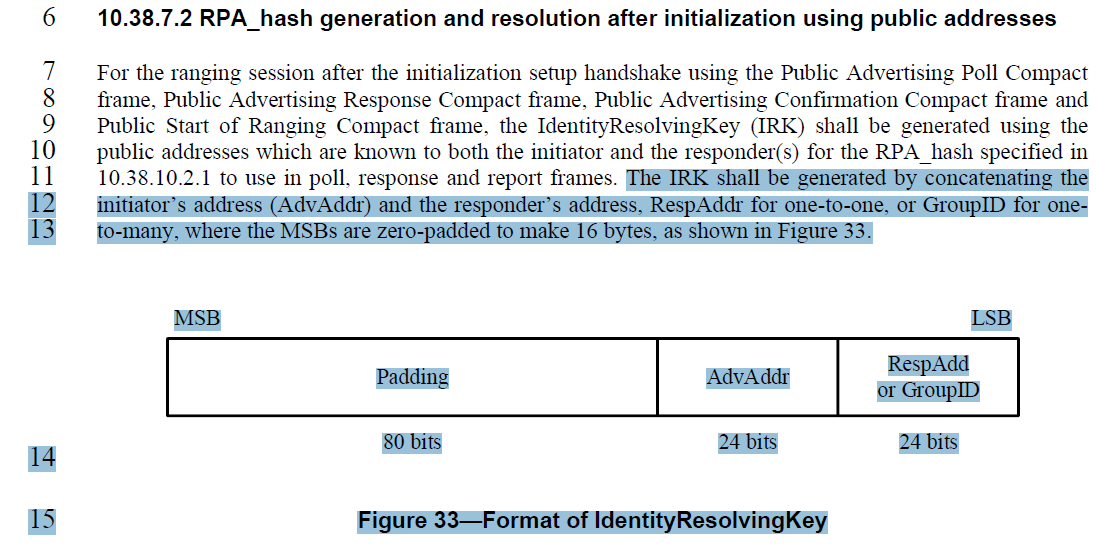
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Pg** | **Sub-clause** | **Ln** | **Comment** | **Proposed change** | **Disposition** |
| Tero Kivinen | 511 | 55 | 10.38.7.2 | 14 | The MSB and LSB are not meaningfull when talking about the key, as keys are not integers, they are bit strings, so you most likely want to define concatenation function like is defined in the Annex B of the IEEE Std 802.15.4, and use it by saying "padding || AdvAddr || RespAdd or GroupID". Then you nee to define how the addresses are converted to the bit strings. Also note, that some ciphers take keys longer than 128 bits, i.e., AES-256 takes 256 bit key, so this should be defined so it can use any cipher that is defined for IEEE Std 802.15.4. | Define it using concationation not using integers. | Revised |

**Discussion:**

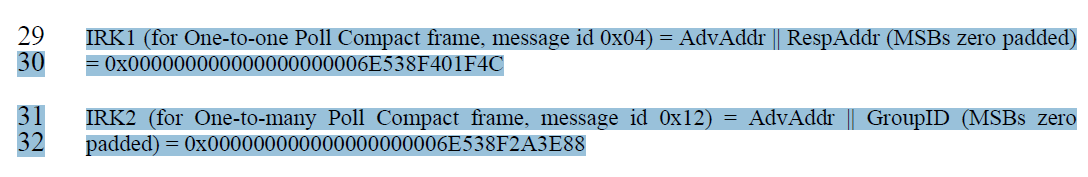
The resolution proposal aligns with the resolution for CID#512 in 15-24-0223-01-04ab-draftc-comment-resolution-compact-frames-rpa-cids-497-507-508-509.docx. To generate an RPA\_hash using public addresses, the IRK should be represented as a sequence of bits, not an integer as the commenter mentioned. According to the resolution proposal for CID#512, this input value is generated not for AES-128-ECB, but for AES-128, which is a block cipher. The previous integer representation methods, such as MSB and LSB, and the concatenation functions are removed. To make the bit order clear, the format of the IRK has been revised.

**Resolution: Revised**

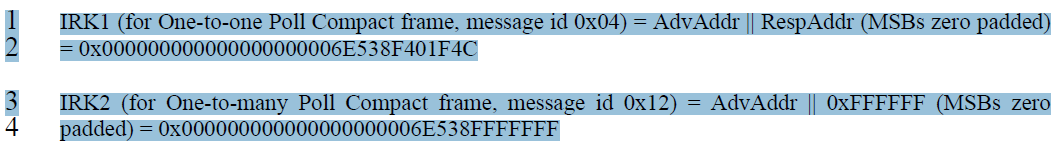
**- Original Text**



……….



……….



**- Proposed change**

***Revise the sub-clause 10.38.7.2 RPA\_hash generation and resolution after initialization using public addresses in IEEE P802.15.4ab/Draft (pre-ballot) C as follows:***

**10.38.3.2.4.2 RPA\_hash generation and resolution after initialization using public addresses**

……….

***pp 55, L11-L15***

For the ranging session after the initialization setup handshake using the Public Compact frames which are Public Advertising Poll Compact frame, Public Advertising Response Compact frame, Public Advertising Confirmation Compact frame and Public Start of Ranging Compact frame, the IdentityResolvingKey (IRK) shall be generated using the public addresses which are known to both the initiator and the responder(s) for the RPA\_hash specified in 10.38.10.2.1 to use in poll, response and report frames. The IRK for Public Compact frames shall be formatted as shown in Figure 33.

|  |  |  |
| --- | --- | --- |
| **Bits: 0-79** | **80-103** | **104-127** |
| Padding | Address 1 | Address 2 |

Figure 33 – IdentityResolvingKey format for Pubic Compact frames

The Padding field shall be set to 0 which size is 80 bits

The Address 1 field is shall be set to InitiatorAddr from the initialization setup handshake using Public Compact frames.

The Address 2 field is shall be set to RespAddr or Group ID from the initialization setup handshake using Public Compact frames.

……….

***pp55, L29-30***

InitiatorAddr = 0x6E538F, RespAddr = 0x401F4C, GroupId = 0x2A3E88

IRK1 (for One-to-one Poll Compact frame, message id 0x04) = 00 00 00 00 00 00 00 00 00 00 6E 53 8F 40 1F 4C

***pp55, L31-32***

IRK2 (for One-to-many Poll Compact frame, message id 0x12) = 00 00 00 00 00 00 00 00 00 00 6E 53 8F 2A 3E 88

……….

***pp56, L1-L2***

InitiatorAddr = 0x6E538F, RespAddr = 0x401F4C

IRK1 (for One-to-one Poll Compact frame, message id 0x04) = 00 00 00 00 00 00 00 00 00 00 6E 53 8F 40 1F 4C

***pp56, L3-L4***

IRK2 (for One-to-many Poll Compact frame, message id 0x12) = 00 00 00 00 00 00 00 00 00 00 6E 53 8F FF FF FF

***Comment index #166 in 15-24-0010-14-04ab-tg4ab-consolidated-comments-draft-c.xlsx***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Index #** | **Pg** | **Sub-clause** | **Ln** | **Comment** | **Proposed change** | **Disposition** |
| Benjamin Rolfe | 166 | 91 | 10.38.10.16 | 1 | Multiple missing things: length of fields SMC TLVs and Adv Data (3); missing definitions for CAP duration field, Initialization Slot Duration field, Group ID field, actual format of TLVs (how many bits for length, type and value), | Complete specification or remove clause | Revised |

**Discussion:**

Regarding missing length of the field for Adv Data, it is resolved by the resolution of CIDs 546, 650, 704 and 812 in 15-24-0108-02-04ab-proposed-resolution-for-MMS-MAC-public\_part1.docx

Regarding missing definition for Group ID, it is resolved by the resolution of CIDs 545, 811 and 908 in 15-24-0144-02-04ab-proposed-change-for-MMS-MAC-public\_part2.docx

Regarding missing length of the field for SMC TLVs and actual format of TLVs, those are resolved by the resolution of CID 63 in 15-24-0177-00-04ab-consensus-cids-extracted-from-dcn-103r6.docx

Regarding missing definitions for the CAP duration field and the Initialization Slot Duration field, those are resolved by the resolution of CIDs 518, 637, 741, 905, 519, 742, 906, 809, 810 and 381 in 15-24-0024-00-04ab-proposed-comments-resolution-on-compact-frame

**Resolution: Revised**