IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for Secure Ranging |
| Date: 2024-07-08 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Ali Raissinia | Qualcomm Inc. |  |  | alirezar@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document provides comment resolutions to CIDs 8001, 8003, 8004, 8005, 8006, 8007, 8009, 8010, 8018, 8028, 8029, 8030, 8032, 8033 and 8035 (total of 15 CIDs) addressing technical discrepancies between various sections of the REVme D6.0 specification related to Secure Ranging.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Line** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 8001 | 3165.00 |  | 12.13.7 | The L() function was changed in the baseline to ExtractBits() but the changes were not propagated to the text rolled in from 802.11az. There are two clauses where updates are required. | Change "L(" to "ExtractBits(" in the following locations: On p2751 - 3x: on lines 6,7,8 On p3165 - 3x: on lines 39, 44, 51 | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx>  |
| 8003 | 2758.00 | 15 | 11.21.6.3.4 | Change Figure 11-68 and 11-69 so that the equation for "LTF Keyseed Generation" matches the equation in P2715L38 | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8004 | 2757.00 | 18 | 11.21.6.3.4 | Modify Figure 11-68 and 11-69 so that the equation for "LTF Key Generation" matches the equation in P2755L60-61 | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8005 | 2715.00 | 38 | 11.21.6.3.4 | Change "Secure HE-LTF" with "Secure LTF" in equation so that it matches the test Vector results in J.14. | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8006 | 208.00 | 55 | 3.1 | Add a definition of L() used in P2756L6-9 is section 3.1 | Add the definition "L(SEQ, S, L) - It is defined as the octet sub-sequence in SEQ of length L in bits starting at position S in bits of sequence SEQ. Position starts with value of 0." | ReviseREVme TG decided to use ExtractBits() instead<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8007 | 3090.00 | 43 | 12.7.1.6.2 | Change the text "K, Label, and Context are bit strings and are represented using the ordering conventions of 9.2.2 (Conventions) " to | K, Label, and Context are octet strings. | Reject<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8009 |  |  |  | “Secure HE-LTF” and “secure HE-LTF” are used throughout. | Should they all be “Secure HE-LTF”? | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8010 |  |  |  | “secure LTF” and “secure HE-LTF” are used throughout. | Should they all be “Secure HE-LTF”, except for “Secure-LTF-Key-Seed” and “Secure-LTF-Counter”. | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8018 | 2749.00 | 43 |  | s/Secure LTF Counter/Secure HE-LTF Counter | As in comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8028 | 2755.00 | 61 | 11.21.6.4.5.4 | Change "Secure HE-LTF Expansion" with "Secure LTF Expansion" in equation so that it matches the test Vector results in J.14. | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8029 | 6085.00 | 19 | J.14 | Chage "Secure HE-LTF" and "Secure HE-LTF Expansion" in J14 so that test vector results match the equations in P2715L38 and P2755L60-61 | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8030 | 6085.00 |  | J.14 | Change Table in J14 to improve clarity and specify details of output block | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| ####8032 | ####### |  $25.00  |  11.21.6.4.5.2  |  Change the text "The STA shall discard the SAC value used in the frame exchange and shall not use the same SAC value in the current measurement exchange" to  |  The STA shall use a new SAC value and its corresponding ista-ltf-key and rsta-ltf-key in every other ranging measurement exchange even if the current ranging measurement exchange is unsuccessful.  | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8033 | 2728.00 | 58 | 11.21.6.4.2.7 | Change the text "…which the Ack was not received, except for updating the Dialog Token field if it was nonzero, and a new Secure TRN Sequence shall be used. The Sequence Number field in the MAC header is also updated." to | which the Ack was not received, except for updating the Dialog Token field if it was nonzero, and a new Secure TRN Sequence (see 2.2.11 (EDMG Secure Ranging Sequence)), shall be used. The Sequence Number field in the MAC header is also updated. | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |
| 8035 | 2760.00 | 57 | 11.21.6.4.6 | There is a typo. Change "SRP\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED" to "PRS\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED" | As per comment | Revise<https://mentor.ieee.org/802.11/dcn/24/11-24-1070-02-00m-comment-resolutiona-for-secure-ranging.docx> |

 Resolution for CID 8005, 8009, 8010, 8028, and 8029

**Discussion**:

11az specification included generation of Secure LTF Key Seed and SAC (Sequence Authentication Code) & LTF keys for use in the normative behavior described in section **11.21.6.4.5 Secure HE-LTF in the TB and non-TB ranging measurement exchange protocol**. It was identified that the normative text is inconsistent with the test vectors specified in section **J.14 LTF Sequence Generation Test Vectors**. The primary reason was that a general comment was added during a letter ballot review (LB) to modify the text “Secure LTF” to “Secure HE-LTF” and unfortunately the phrase “HE-“ was not used to calculate the text vectors in J.14 hence caused the discrepency. This issue was identified during the IOT testing and venders have decided to remove the phrase “HE-“ so that the test vectors is still correct. This document suggests the necessary changes to be included to the REVmeD6.0.

*Instruction to TGme Editor. Please modify the text in P2715L38 as below*

Secure-LTF-Key-Seed = HMAC-Hash(KDK, “Secure ~~HE-~~LTF key seed”)

*Instruction to TGme Editor. Please modify the text in P2755 L60-61 as below*

SAC-and-LTF-Keys = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure ~~HE-~~LTF Expansion”, Secure-LTF-Counter)

*Instruction to TGme Editor. Please modify the text in P6085 L13-45 as below*

**J.14 LTF Sequence Generation Test Vectors(11az)**

As defined in 11.21.6.3.4 (Negotiation for secure HE-LTF in the TB and non-TB ranging measurement

exchange), Secure-LTF-Key-Seed is derived from KDK as follows:

Secure-LTF-Key-Seed = HMAC-Hash(KDK, “Secure ~~HE-~~LTF key seed”)

Hash: SHA-256

KDK: 6c 7f b9 7c eb 55 b0 1a cf f0 0f 07 09 42 bd f5

29 1f eb 4b ee 38 e0 36 5b 25 a2 50 bb 2a c9 ff

Secure-LTF-Key-Seed: 07 60 6f 7b 0d 98 ca 03 ec 2d 61 e1 7c 6b df d3

0e 2f 20 30 e3 47 02 22 55 1a 05 ec 55 d1 35 b9

SAC || ista-ltf-key || rsta-ltf-key = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure HE-LTF

Expansion”, Secure-LTF-Counter)

Hash: SHA-256

Length: 272 (bits)

Secure-LTF-Key-Seed: 07 60 6f 7b 0d 98 ca 03 ec 2d 61 e1 7c 6b df d3

0e 2f 20 30 e3 47 02 22 55 1a 05 ec 55 d1 35 b9

Secure-LTF-Counter: 0x000000000100

SAC: 23 cf

ista-ltf-key: d2 a8 a2 b7 6c 3c 29 2d 81 e1 82 a4 69 fd e8 3c

rsta-ltf-key: 65 02 7a 83 8d 58 59 3c 57 b9 41 6f 17 24 e6 c4

Transmitter MAC address: 00 10 18 32 76 54

Resolution for CID 8007 is “Reject” with following explanation-

**Discussion:** The commenter provided the comment below as part of the WFA security review

**Subclause 12.7.1.6.2, Page 3083, Line 16:** Context is defined as a bit string. The HMAC algorithm expects the input to be an octet string. Since this is specified as a library function, it needs to require that the provided bit string is a multiple of eight bits.

HMAC can generate output that converts bit-strings to octet-strings using baseline conventions stated in section 9.2.2.

Resolution for CID 8003, 8004, 8018 and 8030

**Discussion**: There are several discrepancies in text (i.e., ‘key seed’, ‘Secure-LTF-key-seed’ and ‘Secure-LTF-Counter’) with respect to the normative equations in P2715L38 and P2755L60-61 that needs to be fixed in Figure 11-68 and 11-69 in addition to adding the octet numbers for ltf-keys as well as ltf-iv. Finally the table in J.14 needs to improve to remove ambiguities so that there would be no interoperability issues with respect to implementation, specifically details of the “output block” so that the psueorandome phase rotation octets and QAM 64 symbol octet values are identified.

*TGm editor: Change Figure 11-68 as shown below:*



*TGme editor: Change Figure 11-69 as shown below:*



*TGme editor, replace the table in J.14 with table below:*

*Note to Editor: This resolution overwrites the changes were made by CID7093 that was included in the REVme D6.0.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octet** | **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| **LTF\_KEY** | d2 | a8 | a2 | b7 | 6c | 3c | 29 | 2d | 81 | e1 | 82 | a4 | 69 | fd | e8 | 3c |
| **LTF\_IV** | 00 | 10 | 18 | 32 | 76 | 54 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 |
| **AES counter [0]** | 00 | 10 | 18 | 32 | 76 | 54 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 |
| **Output block [0]** | M0,15 | M0,14 | M0.13 | M0.12 | M0,11 | M0,10 | M0,9 | M0,8 | M0,7 | M0,6 | M0,5 | M0,4 | M0,3 | M0,2 | M0,1 | M0,0 |
| aa | f6 | 2c | 30 | 6b | cd | 8a | 5d | 89 | 80 | 8b | 03 | 8e | da | 43 | f1 |
| (I,Q)=(2,5) | (I,Q)=(3,3) | (I,Q)=(1,5) | (I,Q)=(0,3) | (I,Q)=(6,5) | (I,Q)=(5,4) | (I,Q)=(2,4) | (I,Q)=(5,6) | (I,Q)=(4,4) | K=1 | K=1 | K=0 | K=1 | K=3 | K=2 | K=7 |
| **AES counter [1]** | 00 | 10 | 18 | 32 | 76 | 54 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 01 |
| **Output block [1]** | M1,15 | M1,14 | M1.13 | M1.12 | M1,11 | M1,10 | M1,9 | M1,8 | M1,7 | M1,6 | M1,5 | M1,4 | M1,3 | M1,2 | M1,1 | M1,0 |
| 54 | 15 | f0 | 5c | 7f | c7 | ee | f5 | 9b | c4 | 58 | d2 | f4 | 6b | 5b | 5a |
| (I,Q)=(1,2) | (I,Q)=(5,2) | (I,Q)=(0,3) | (I,Q)=(1,6) | (I,Q)=(7,7) | (I,Q)=(7,0) | (I,Q)=(3,5) | (I,Q)=(5,3) | (I,Q)=(6,6) | (I,Q)=(1,0) | (I,Q)=(0,6) | (I,Q)=(2,2) | (I,Q)=(1,3) | (I,Q)=(6,5) | (I,Q)=(6,6) | (I,Q)=(2,6) |
| **…****(I, Q) = input index for 64-QAM octet, I = input bits (B0 B1 B2), Q = input bits (B3 B4 B5) defined in Table 17-18.****The integer k is defined in Equation (27-131) that is used to construct the pseudorandom phase rotation. + P** |

Resolution for CID 8001 and 8006

**Discussion**: It appears that function L() is not defined in the baseline spec and it is used Figure 12-32 and in so it makes sense to add it to section 12.1 Conventions.

*TGme editor, make changes in the text P2756L6-9 as below:*

SAC is equal to ~~L~~ExtractBits(SAC-and-LTF-Keys, 0, 16)

ista-ltf-key is equal to ~~L~~ExtractBits(SAC-and-LTF-Keys, 16, 128)

rsta-ltf-key is equal to ~~L~~ExtractBits(SAC-and-LTF-Keys, 144, 128)

Resolution for CID 8032

**Discussion**: The spec text needs to be clear as to when ‘SAC value’ is discarded.

*TGme editor, delete the text in P2750L25-26 and add the text below:*

~~The STA shall discard the SAC value used in the frame exchange and shall not use the same SAC value in the current measurement exchange.~~

The STA shall use a new SAC value and its corresponding ista-ltf-key and rsta-ltf-key in every other ranging measurement exchange even if the current ranging measurement exchange is unsuccessful.

Resolution for CID 8033

**Discussion**: Improve spec language by adding a reference section as to how a ‘new Secure TRN sequence” is generated.

*TGme editor, Modify the text in P2728L58-59 as below:*

which the Ack was not received, except for updating the Dialog Token field if it was nonzero, and a new Secure TRN Sequence (see 12.2.12 (EDMG Secure Ranging Sequence)), shall be used.

Resolution for CID 8035

*TGme editor, change the "SRP\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED" to "PRS\_AND\_NON-SRG\_OBSS-PD\_PROHIBITED" in P2760L57 and P2761L42 as there was a typo.*

**References: P802.11REVme D6.0**