IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Alignment of secure LTF normative text with test vectors | | | | |
| Date: 2024-01-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Ali Raissinia | Qualcomm Inc. |  |  | alirezar@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document resolves the discrapency between the normative text associated with generation of Secure-LTF-Key-Seed, SAC-and-LTF-keys and the test vectors specified in section **J.14 LTF Sequence Generation Test Vectors**

**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.13 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.13 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 REVmeD4.2.

Instruction to TGme Editor. Please modify the text in P2671 L38 as below

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

Instruction to TGme Editor. Please modify the text in P2710 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 P2671 L38 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

**References:P802.11REVme-D4.2**