IEEE P802.11Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Resolutions to 11az LB253 CID-5453 | | | | |
| Date: 2021-06-30 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Qi Wang | Apple Inc. |  |  | qi\_wang2@apple.com |

Abstract

This submission proposes to revisit 11az LB253 CID-5453 and proposes an alternative resolution.

The page and line numbers for proposed changes refer to those in 11az Draft 3.0 [1].

**Introduction**

The current resolution for CID-5453 is to “reject” (see LB253 comments database 2021/258r4), with the rationale that “The text at p191.18 states “The hash function to be employed in HKDF is SHA-256.” and per RFC 5869 2.2 referenced above p191.22, PRK is derived using the hash function.

This submission proposes to revisit the comment and proposes an alternative resolution.

**Comments:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page/Line | Clause | Comment | Proposed change | Resolution |
| 5453 | 191/22 | 12,2,11 | "A pseudo-random key (PRK) is generated using the hash function accepting IKM and salt as inputs.  See RFC 5869 section 2.2." The hash function to generate PRK is undefined. | Please add that : "The hash function to be employed to generate the PRK is SHA-256." | Accept. |

**Discussion:**

In 11az\_D3.0, for EDMG secure ranging sequences generation, HKDF-Expand is called each time to generate the random bits, as follows:

Random\_bits = HKDF-Expand (PRK, Info field, length).

Although 11az specifies SHA-256 to be used for HKDF-expand function to generate the random bits, the hash function to generate PRK is undefined. The reference RFC 5869/2.2 (as shown below) doesn’t specify it, either.



This submission proposes to specify SHA-256 as such hash function, as proposed by the commenter of CID-5434.

The page and line numbers for proposed changes refer to those in 11az Draft 3.0 [1].

**TGaz Editor: please change the text in 12.2.11 as follows:**

* + 1. **DMG Secure Ranging Sequences**

EDMG Secure Ranging uses Secure TRN subfields, see 28.9.3 (DMG secure ranging PPDU), as part of the TRN fields of EDMG PPDUs. Those TRN subfields are based on bit sequences henceforth denoted as Secure TRN Sequences. These Secure TRN bit Sequences are generated as follows:

The Secret Key is 32 octets (#**3832**) randomly generated by the ISTA and sent in the Secure Ranging Operation Parameters field, see Figure 9-626e (Secure Ranging Operation Parameters field format), of the EDMG Specific Parameters subelement of the Fine Timing Parameters element sent by the ISTA to the RSTA in the initial Protected Fine Timing Measurement request; see 11.21.6.3.6 (Negotiation for Secure EDMG TRN in EDCA based Ranging measurement exchange). (#**3936**) The Secret Key is used as Input Key Material (IKM) to generate pseudo-random Secure TRN Sequences that are used to construct secure ranging waveforms at the I-STA and R-STA respectively. The Secret Key and Salt shall be discarded after the FTM session is terminated. Each FTM session shall have a different Secret Key.

Pseudo-random Secure TRN Sequences are generated using HKDF (Hashed Message Authentication Code (HMAC)-based Key Derivation Function) specified in IETF RFC 5869:

The hash function to be employed in HKDF is SHA-256.

The Secret Key is to be used as the IKM in HKDF. See RFC 5869, section 2.2.

The Salt is the PMKID corresponding to the security association between the ISTA and RSTA. See RFC 5869, section 2.2.

A pseudo-random key (PRK) is generated using the hash function accepting IKM and salt as inputs. See RFC 5869 section 2.2. The hash function to be employed to generate the PRK is SHA-256. (#5453)

The Info field is a fixed string “EDMG Secure RTT”, which is (#**3823**) unique to this protocol in order to guard against accidental key re-use in a different subsystem. Key reuse across different subsystems must be avoided through careful system design, and the Secret Key must not be visible outside of the subsystem. See RFC 5869, section 2.3.

Pseudo-random Secure TRN Sequences are the output of the HKDF-Expand function with the PRK, Info field and the length of Secure TRN Sequences required as inputs. See RFC 5869, section 2.3. One-time calculation of all pseudo-random Secure TRN Sequences for multiple timing measurements should be used for minimizing HKDF set-up costs in case of multiple ranging attempts. The length of the Secure TRN sequences generated shall be long enough for generating Secure TRN subfields for the number of bursts expected in the session.

(#**1454**, #**1455**, #**1456**, #**1450**, #**1089**)

Furthermore, if memory is not constrained in an implementation, caching multiple Secret Keys and Salt pairs and pre-generating all Secure TRN Sequences for multiple timing measurements and multiple FTM sessions is allowed provided that this information is not revealed to third parties.

**References**

[1] IEEE P802.11az™/D3.0