IEEE P802.11
Wireless LANs

|  |
| --- |
| LB249-Clause-12-2-11-CIDs |
| Date: 2020-01-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm |  |  | akasher@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions to LB249 comments on subclause 12.2.11. The base is TGaz D2.0. The CIDs are 3823, 3832, 3936

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3823 | 177.00 | 12.2.11 | "The Info field is a fixed string unique to this protocol" -- well, err, which fix string is it then? | As it says in the comment |  **Revise: See 11-20-0167** |

***TGaz Editor: Modify the text in P177L33 (12.2.11) as follows:***

The Info field is the fixed string ”EDMG Secure ToF”, which is (#3823) unique to this protocol in order to guard against accidental key reuse in a different subsystem. Key reuse across different subsystems must be avoided through …

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3832 | 177.00 | 12.2.11 | "The Secret Key is 32 bit octets" -- well, which is it? | Change to "The secret key is 32 octets" |  **Acceot: See 11-20-0167** |

***TGaz Editor: Modify the text in P177L14 (12.2.11) as follows:***

The Secret Key is 32 (#3832) octets randomly generated by the ISTA and sent in the Secure Ranging

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3936 | 177.00 | 12.2.11 | "see 11.22.6.3.5 EDMG 17 Secure ToF Measurement Setup" wrong reference | replace by "see 11.22.6.3.5 Negotiation for Secure EDMG TRN in EDCA based Ranging measurement exchange" |  **Accept** |

***TGaz Editor Modify the test in P177L17-18 (12.2.11) as follows:***

to the RSTA in the initial Protected Fine Timing Measurement request. (see 11.22.6.3.5 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

**References:**

**P802.11az D2.0**