IEEE P802.11
Wireless LANs

|  |
| --- |
| PeerKey Deletion Cleanup |
| Date: February 2, 2018 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Menzo Wentink | Qualcomm | Utrecht, The Netherlands | +31-65-183-6231 | mwentink@qualcomm.com |
|  |  |  |  |  |

Abstract

This document contains some remaining items related to the deletion of the PeerKey protocol. Changes shown are relative to REVmd draft 1.0.

383.45 delete clause 6.3.23 (MLME-PEERKEY-START) (ends 384.24)

2231.64 edit as shown:

An AP with dot11ProtectedTXOPNegotiationActivated true that does not have an active security association with a peer AP that indicates support for protected HCCA TXOP negotiation shall use the AP PeerKey protocol (as defined in 12.11.2 (AP PeerKey protocol)) and authenticated mesh peering exchange (AMPE) (as defined in 14.5 Authenticated mesh peering exchange (AMPE)) to negotiate security parameters and create a new PMKSA and PTKSA to secure the Protected HCCA TXOP Advertisement frames. The use of AMPE proves possession of the PMK (generated using the procedures described in 12.11.2 (AP PeerKey protocol)) and implicitly the private key that corresponds to the peer’s public key.

2371.44 delete "- SMKSA: A result of a successful initial SMK handshake."

2390.48 delete "SMKSA, "

2416.13 delete "/SMK"

2427.14 delete "/SMK"

2427.16 delete "SMK Message = 0"

2428.12 delete "/SMK"

2435.31 move 12.7.8.5 (Supplicant state machine procedures) to behind 12.7.9.3 (Supplicant state machine variables)

2437.57 delete 12.7.8.6 (Supplicant PeerKey state machine states) (ends 2439.29)

2439.30 delete 12.7.8.7 (Supplicant PeerKey state machine variables) (ends 2440.3)

3911.48 delete

dot11RSNAConfigSTKKeysImplemented,dot11RSNAConfigSTKCipher,dot11RSNAConfigSTKRekeyTime,dot11RSNAConfigSMKUpdateCount,dot11RSNAConfigSTKCipherSize,dot11RSNAConfigNumberOfSTKSAReplayCounters,dot11RSNAPairwiseSTKSelected,

3912.8 delete

dot11RSNSMKcachingGroup OBJECT-GROUP OBJECTS { dot11RSNAConfigSMKLifetime, dot11RSNAConfigSMKReauthThreshold } STATUS deprecated DESCRIPTION "Deprecated because mechanisms for use of cached SMKSAs are not defined. The dot11RSNSMKcachingGroup object class provides the necessary support for managing SMKSA caching functionality in the STA." ::= { dot11Groups 29 }