IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reconciling 11-17/1807r12 against resolution to CID 1365 | | | | |
| Date: 2018-07-27 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom Ltd. | 250 Innovation Drive, San Jose CA 95134 | +1 408 922 5924 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |
| Thomas Derham | Broadcom Ltd. | 16340 W Bernardo Dr, San Diego CA 92127 |  | [thomas.derham@broadcom.com](mailto:thomas.derham@broadcom.com) |
| Mathy Vanhoef | KU Leuven |  |  | [mathy.vanhoef@cs.kuleuven.be](mailto:mathy.vanhoef@cs.kuleuven.be) |
| Ido Ouzieli | Intel Ltd. | 94 Em Hamoshavot Way, Petach-Tikva Israel 4970602 | +972 3 920 5700 | ido.ouzieli@intel.com |

Abstract

Document 11-17/1807/r12 proposed changes to support operating channel validation. The changes were based on Draft P802.11REVmd\_D0.3.pdf and was adopted by TGmd for incorporation into TGmd draft during the July 2018 IEEE 802 plenary meeting. Resolution for CID 1365 changed some of the text that was also changed by 1807/r12. This document proposes an small editorial update to resolve the merge conflict between the two changes. There is no change to the semantics or the mechanism used for operating channel validation. The changes proposed are relative to TGmd Draft 1.3-0221 that is currently under preparation.

R2: Includes changes as discussed on 2018-07-27 TGmd teleconference

**Notation**

**pnnnn.mm** – indicates page **nnnn** line **mm**

**Discussion - General**

Document 1807/r12 instructs the editor to modify 4-way handshake subsection ‘12.7.6.1 General’ as follows p2460.4

Message 2: Supplicant **** Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD\_M2)

where DataKD\_M2 = RSNE for creating PTK generation or peer RSNE, Lifetime

KDE, SMKID KDE (for sending SMKID) for STK generation, and OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Supplicant

Message 3: Authenticator ****  Supplicant:

EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD\_M3)

where DataKD\_M3 = RSNE,GTK[N] for creating PTK generation or initiator RSNE,

Lifetime KDE for STK generation, and OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator

Above text has been changed due to the resolution of CID 1365 as shown below.

Message 1:   Authenticator  Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID}) (#1365)

Message 2:   Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE}) n(#1365)

Message 3:  Authenticator ® Supplicant: EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]})(#1365)

Message 4:   Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{})(#1365).

**Instructions to the editor**

***Instruct the editor to modify* ‘12.7.6.1 General*’ p2609.54 as follows***

Message 1:   Authenticator  Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,{} or {PMKID}) (#1365)

Message 2:   Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,{RSNE} or {RSNE, OCI KDE}) (#1365)

Message 3:   Authenticator  Supplicant: EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,{RSNE,GTK[N]} or {RSNE, GTK[N], OCI KDE})(#1365)

Message 4:   Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{})(#1365).

 …

Here, the following assumptions apply:

…

— OCI KDE contains the current operating channel information for the operating channel in which the EAPOL frame is sent.(M58). OCI KDE is present when dot11RSNAOperatingChannelValidationActivated is true on the Supplicant in Message 2 and Authenticator in Message 3. Otherwise it is absent.

**References:**

[1] IEEE P802.11-REVmdTM/D1.3-0221, July 2018

[2] IEEE P802.11-REVmdTM/D0.3, September 2017

[3] Document 11-17/1807r12 – Operating Channel Validation – July 2018

[4] CID 1365 resolution – XXXX?