IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe SA1 EAPoL-Key Notation Clean-up |
| Date: 2024-05-29 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | montemurro.michael@gmail.com  |

Background

This contribution deals with updating EAPoL-Key notation. This addresses CIDs 22102

R0: Initial version

R1: Updated based on offline comments

R2: Fixed typo

R3: text updates with 11bh changes for Device ID and IRM

R4: Fixes to P802.11be D6.0

### Discussion:

The EAPOL-key notation was updated in REVme D5.0 and this contribution addresses CID 22102 to update the text added by P802.11be.

Notation:

* The Key Data field value is denoted by {…}
* Optional key data elements are denoted by […, ]

### Proposed Resolution:

REVISED. Update the EAPoL-key notation for Key Data to make it less cumbersome and more extensible in <this>

NOTE to editor. This updated text pulls in specification text from REVme D5.0

***Update the following text in this clause as follows:***

* EAPOL-Key PDU notation(#1836)

***Updates to P802.11be D6.0:***

* 4-way handshake
* General

***Update the following text at the beginning of the clause:***

RSNA defines a protocol using (#1836)EAPOL-Key PDUs called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator ® Supplicant: EAPOL-Key(0 or 1,0,1,0,P,0,0,ANonce,0, {[PMKID][, MAC Address]})

Message 2: Supplicant ® Authenticator: EAPOL-Key(0 or 1,1,0,0,P,0,0,SNonce, MIC, {RSNE [, RSNXE] [, OCI] [, MAC Address, MLO Linkn] [, Device ID KDE]})

Message 3: Authenticator®Supplicant:
EAPOL-Key(1,1,1,1,P,0, RSC,ANonce, MIC,{RSNE [, RSNXE] [, OCI] [, GTK(N)] [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, MAC Address, MLO Linkm, MLO GTKm] [, MLO IGTKn] [, MLO BIGTKn] [, Device ID KDE] [, IRM KDE]})

Message 4: Supplicant ® Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{[MAC Address] [, IRM KDE]})