IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe SA1 EAPoL-Key Notation Clean-up |
| Date: 2024-03-25 |
| 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

### 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)

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

* 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]}) ~~or {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]) ~~[, OCI] or {RSNE, Device ID KDE} or {RSNE, OCI KDE, Device ID KDE} or {RSNE, RSNXE, Device ID KDE} or {RSNE, OCI KDE, RSNXE, Device ID KDE} or {RSNE, MAC Address} or {RSNE, RSNXE, MAC Address} or {RSNE, OCI KDE, RSNXE, MAC Address} or {RSNE, MAC Address, MLO Link~~~~n~~ ~~} or {RSNE, RSNXE, MAC Address, MLO Link~~~~n~~ ~~}or {RSNE, OCI KDE, RSNXE, MAC Address, MLO Link~~~~n~~~~}~~)

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]}) ~~[, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)]} or {RSNE, GTK[N], Device ID KDE} or {RSNE, GTK[N], OCI KDE, Device ID KDE} or {RSNE, GTK[N], RSNXE, Device ID KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, Device ID KDE} or {RSNE, GTK[N], IRM KDE} or {RSNE, GTK[N]. OCI KDE, IRM KDE} or {RSNE, GTK[N], RSNXE, IRM KDE} or {RSNE, GTK[N], OCI KDE, RSNXE, IRM KDE} or {MAC Address, MLO Link~~~~m~~~~, MLO GTK~~~~n~~~~, MLO IGTK~~~~n~~~~, MLO BIGTK~~~~n~~~~} or {OCI KDE, MAC Address, MLO Link~~~~m~~~~, MLO GTK~~~~n~~~~, MLO IGTK~~~~n~~~~, MLO BIGTK~~~~n~~~~}~~)

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

~~Address}).~~.

* Group key handshake
* General

The Authenticator may initiate the exchange at any time when a Supplicant is disassociated or deauthenticated.

Message 1: Authenticator ® Supplicant:

EAPOL-Key(1,1,1,0,G,0, RSC,0, MIC, {[GTK(N)] [, OCI} [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [(11ba), WIGTK(R, WIPN)] [, MLO GTKn] [, MLO IGTKn] [, MLO BIGTKn]})

Message 2: Supplicant ® Authenticator: EAPOL-Key(1,1,0,0,G,0,0,0,MIC,{ [OCI]})

NOTE 1—Elements and KDEs in the key data field can be included in any order.

* FT initial mobility domain association
* Overview

The FT initial mobility domain association is the first (re)association in the mobility domain, where the SME of the STA enables its future use of the FT procedures.

FT initial mobility domain association is typically the first association within the ESS. In addition to Association Request and Response frames, Reassociation Request and Response frames are supported in the initial mobility domain association to enable both FT and non-FT APs to be present in a single ESS.

* FT initial mobility domain association in an RSN

***Update the following text at the beginning of page 450 of TGbe D5.0 as follows:***

Between a non-AP MLD and an AP MLD, the FT 4-way handshake is as follows:

R1KH→S1KH: EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0, {MAC Address})

S1KH→R1KH: EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE(PMKR1Name), MDE, FTE [, RSNXE] [, OCI] , MAC Address, MLO Linkn})

R1KH→S1KH: EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, {~~RSNE(PMKR1Name)~~ MAC Address, MLO Linkm(RSNE(PMKR1Name)), MLO GTKn [, MLO IGTKn] [, MLO BIGTKn, [, OCI] , MDE, FTE, TIE(ReassociationDeadline), TIE(KeyLifetime) [, WIGTK(R, WIPN)] , })

S1KH→R1KH: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {[MAC Address]})

(#6590)NOTE—Elements and KDEs in the key data field can be included in any order.