IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for 11be D0.3 Group Key Handshake CIDs |
| Date: 2021-02-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGbe comment collection (TGbe Draft 0.3).

* CIDs: 1028, 2505, 2594 (3 CIDs)

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Removed the mandatory requirement for the inclusion of the MLO GTK KDE for the transmitting link.
* Rev 2: Set Key RSC = 0 in the Group Key handshake message 1 (and also for 4-way handshake message 3) for MLO based on Yongho’s comment. Changes in CYAN.
* Rev 3: Changes based on comments received during call and offline. “available link” -> “enabled link” based on Jay’s comments, MLO\_GTK/IGTK/BIGTK -> MLO GTK/IGTK/BIGTK (removed underscore) based on Yonggang’s feedback. Changes in green.
1. **Introduction**

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbe Draft. The introduction and the explanation of the proposed changes are not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbe Draft (i.e. they are instructions to the 802.11be editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Clause  | Page | Line | Comment | Proposed Change | Resolution |
| 1028 | Abhishek Patil | 12.7.7 | 118 | 34 | Update clause 12.7.7 to handle GTK/IGTK/BIGTK delivery for other links of the AP MLD | As in comment | **Revised.**Agree with the comment that clause 12.7.7. need to be updated to allow update of the GTK/IGTK/BIGTK of other links to be delivered in a single Group Key Handshake. TGbe editor to make the changes shown in IEEE 802.11-21/0300r3 under all headings that include CID 1028. |
| 2505 | Po-Kai Huang | 12.7.7 | 122 | 1 | Group handshake is used to update the group key. Similar to the design we add in 12.7.6. Allow group key handshake to update keys of all setup links in one excahgne. | Follow the design in 12.7.6 for group key handshake by allowing KDE of GTK, IGTK, BIGTK of other links to be included in group key handshake to complete update in one handshake. | **Revised.**Agree with the comment that clause 12.7.7. need to be updated to allow update of the GTK/IGTK/BIGTK of other links to be delivered in a single Group Key Handshake. TGbe editor to make the changes shown in IEEE 802.11-21/0300r3 under all headings that include CID 2505. |
| 2594 | Rojan Chitrakar | 35.3.5.2 | 132 | 1 | Clause 12.7.7 (Group key handshake) should also be expanded to allow delivery of the GTK/IGTK/BIGTK of other setup links using a single group key handshake. | Expand  Clause 12.7.7 (Group key handshake)  to allow delivery of the GTK/IGTK/BIGTK of other setup links using a single group key handshake. | **Revised.**Agree with the comment that clause 12.7.7. need to be updated to allow update of the GTK/IGTK/BIGTK of other links to be delivered in a single Group Key Handshake. Reference for 12.7.7 was also added in 35.3.5.2. TGbe editor to make the changes shown in IEEE 802.11-21/0300r3 under all headings that include CID 2594. |

**Discussion:** In D0.4, the 4-way handshake (12.7.6) already allows the GTK/IGTK/BIGTK of all the setup links to be delivered during a single 4-way handshake by including the MLO GTK/IGTK/BIGTK KDEs in Message 3. Clause 12.7.7 (Group Key Handshake) is also similarly expanded to deliver the GTK/IGTK/BIGTK of one or more setup links using a single Group Key handshake by including the MLO GTK/IGTK/BIGTK KDEs in Message 1. MLO KDEs are used even for delivery of GTK/IGTK/BIGTK of the link on which the EAPOL-Key frame is transmitted in order to uniquely associate the keys with the link. (This is same as the 4-way handshake (see 21/483r3).



**Propose:**

Revised for CIDs 1028, 2505, 2594 as per discussion and editing instructions in IEEE 802.11-21/0300r3.

SP: Do you agree to incorporate the changes proposed in IEEE 802.11-21/0300r3 to the lastest 11be draft for CIDs 1028, 2505, 2594?

12.7.2 EAPOL-Key frames (CIDs 1028, 2505, 2594)

***TGbe editor: Change the seventh paragraph as follows (Track Change On):***

* **Group key handshake message 1** is an EAPOL-Key frame with the Key Type subfield equal to 0. For non-MLO, the Key Data field shall contain a GTK KDE and shall be encrypted. For MLO, the Key Data field may include one MLO GTK KDE, one MLO IGTK KDE and one BIGTK MLO KDE for each of the setup links and shall be encrypted.
* **Group key handshake message 2** is an EAPOL-Key frame with the Key Type subfield equal to 0. The Key Data field can be empty.
* 4-way handshake message 3 (CIDs 1028, 2505, 2594)

***TGbe editor: Modify the subclause as the following (Track Changes ON):***

Key RSC = For PTK generation for non-MLO, starting TSC or PN that the Authenticator’s STA uses in MPDUs protected by GTK. 0 for MLO.

12.7.7 Group key handshake (CIDs 1028, 2505, 2594)

12.7.7.1 General

***TGbe editor: Modify the subclause as the following (Track Changes ON):***

The Authenticator uses the Group key handshake to send a new GTK and, if management frame protection is negotiated, a new IGTK, and if beacon protection is enabled, a new BIGTK to the Supplicant. When the Authenticator is an AP MLD and the Supplicant is a non-AP MLD, the Authenticator may also use the Group Key handshake to send new GTK/s for any of the setup links and, if management frame protection is negotiated, new IGTK/s for any of the setup links, and if beacon protection is enabled, new BIGTK/s for any of the setup links to the Supplicant.

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

Message 1: Authenticator → Supplicant:

EAPOL-Key(1,1,1,0,G,0,Key RSC,0, MIC, {GTK[N], IGTK[M], BIGTK[Q]} or {MLO GTKn, MLO IGTKn, MLO BIGTKn})

Message 2: Supplicant → Authenticator: EAPOL-Key(1,1,0,0,G,0,0,0,MIC,{})

The following apply:

— Key RSC denotes the last TSC or PN sent using the GTK.

— GTK[N] denotes the GTK with its key identifier as defined in 12.7.2 using the KEK defined in 12.7.1.3 and associated IV.

— IGTK[M], when present, denotes the IGTK with its key identifier as defined in 12.7.2 using the KEK defined in 12.7.1.3 and associated IV.

— BIGTK[Q], when present, denotes the BIGTK with its key identifier as defined in 12.7.2 using the KEK defined in 12.7.1.3 and associated IV.

— The MIC is computed over the body of the EAPOL-Key frame (with the MIC field zeroed for the

computation) using the KCK defined in 12.7.1.3.

— OCI KDE represents the current operating channel information using which the EAPOL-Key frame

is sent. OCI KDE is included when dot11RSNAOperatingChannelValidationActivated is true on the STA sending the message.

— MLO GTKn, when present, denotes the GTK for the AP affiliated with the AP MLD for the link specified by LinkID n as defined in 12.7.2 (EAPOL-Key frames).

— MLO IGTKn, when present, denotes the IGTK for the AP affiliated with the AP MLD for the link specified by LinkID n as defined in 12.7.2 (EAPOL-Key frames).

— MLO BIGTKn, when present, denotes the BIGTK for the AP affiliated with the AP MLD for the link specified by LinkID n as defined in 12.7.2 (EAPOL-Key frames).

12.7.7.2 Group key handshake message 1

***TGbe editor: Modify the section as the following (Track Changes ON):***

***…***

Key RSC = last TSC or PN for the GTK for non-MLO. 0 for MLO.

Key MIC = Not present when using an AEAD cipher; otherwise, MIC(KCK, EAPOL)

Key Data Length = length of Key Data field in octets

Key Data = encrypted, encapsulated

—For non-MLO, GTK and the GTK’s key identifier (see 12.7.2 (EAPOL-Key frames))

—When present, IGTK, IGTK’s key identifier, and IPN (see 12.7.2 (EAPOL-Key frames))

—When present, BIGTK, BIGTK’s key identifier, and BIPN (see 12.7.2 (EAPOL-Key

frames))

—OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the

Authenticator(M58)

—For MLO, when present, the MLO GTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links

— For MLO, when present, the MLO IGTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links

—For MLO, when present, the MLO BIGTK KDE (see 12.7.2 (EAPOL-Key frames)) for any of the setup links

The Authenticator sends message 1 to the Supplicant.

On reception of message 1, the Supplicant:

a) Verifies that the Key Replay Counter field value has not yet been seen before, i.e., its value is

strictly larger than that in any other EAPOL-Key frame received thus far during this session.

b) If dot11RSNAOperatingChannelValidationActivated is true and Authenticator RSNE indicates

OCVC capability, the Supplicant silently discards message 1 if any of the following are true:

— OCI KDE is missing in the message

— Channel information in the OCI KDE does not match current operating channel parameters

(see 12.2.9)

c) Verifies that the MIC is valid, i.e., it uses the KCK that is part of the PTK to verify that there is no data integrity error, or that the AEAD decryption steps succeed.

d) When the Supplicant is not an MLD, uses the MLME-SETKEYS.request primitive to configure the temporal GTK and, the IGTK when present, and the BIGTK if beacon protection is enabled, into the MAC. When the Supplicant is a non-AP MLD, uses the MLME-SETKEYS.request primitive to configure the temporal GTK/s when present and, the IGTK/s when present, and the BIGTK/s when present for the indicated link/s into the MAC of the affiliated non-AP STA/s operating on the indicated link/s.

e) Responds by creating and sending message 2 of the group key handshake to the Authenticator and incrementing the replay counter.

35.3.5.2 Multi-link security (CIDs 2594)

***TGbe editor: Modify the section as the following (Track Changes ON):***

***…***

Different links use different GTK/IGTK/BIGTK and each link has its own PN space. The GTK/IGTK/BIGTK of each setup links are delivered to the non-AP MLD using a single 4-way handshake as defined in 12.7.6 (4-way handshake). When a GTK/IGTK/BIGTK update is triggered for an AP affiliated with the AP MLD, the updated GTK/IGTK/BIGTK may be delivered to the non-AP MLD using the Group key handshake over any enabled link as defined in 12.7.7 (Group key handshake). (#2594)