IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for 11be D2.0 Clause 12 Security CIDs |
| Date: 2022-09-20 |
| 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 LB (TGbe Draft 2.0).

* CIDs: 12094, 12095, 12096, 12980, 12981, 13174, 13175, 13176, 13177, 13178, 13180, 13181, 13203, 13498, 13499, 13500, 13501 (17 CIDs)

Revisions:

* Rev 0: Initial version of the document.
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 |
| 12094 | Chaoming Luo | 12.6.1.1.8 | 346 | 29 | "that are received by the non-AP STAs affiliated with the non-AP MLD" looks like the STAs on different link would also decrypt the MPDUs on that link, which is not the intention of the sentence. | Change to "that are received by the non-AP STA that operate on the link and is affiliated with the non-AP MLD" | **REVISED.**Agree with the comment to clarify that the non-AP MLD is operating on the link; similar change is also made to the AP side. TGbe editor to make the changes shown in IEEE 802.11-22/1646r0 under all headings that include CID 12094. |
| 12095 | Chaoming Luo | 12.6.1.1.8 | 346 | 29 | The encrypting may also happen on non-STA STA affiliated with the non-AP MLD since the non-AP MLD could also transmit group addressed Data frames, please update to reflect that. | As commented | **REJECTED.**Non-AP STAs do not transmit group addressed MPDUs.  |
| 12096 | Chaoming Luo | 12.6.1.1.8 | 346 | 44 | Should the GTKSA/IGTKSA/BIGTKSA also consist the AP STA's MAC address since it is a per-AP context? | Please clarify | **REJECTED.**GTKSA/IGTKSA/BIGTKSA only consist of the Authenticator MAC Address; supplicant MAC Address is not required. |
| 12980 | Chunyu Hu | 12.6.1.1.9 | 347 | 3 | "any of its links" ==> "each of its links" for better wording | As in comment | **ACCEPTED.** |
| 12981 | Chunyu Hu | 12.6.1.1.11 | 347 | 29 | The setup links can be multiple. To be consistent with the previious paragraph, change "for its setup link" to "each of its setup links". | As in comment | **ACCEPTED.** |
| 13174 | Mark RISON | 12.6.1.1.8 | 346 | 24 | "Between an APMLD and a non-AP MLD that have completed a successful multi-link (re)setup, for each setup link there isone GTKSA used exclusively for encrypting group addressed MPDUs that are transmitted by the APaffiliated with the AP MLD and for decrypting group addressed transmissions that are received by the non-AP STAs affiliated with the non-AP MLD. " -- I'm not sure this is the case given GTK rekeying, which results in two GTKSAs (with different key IDs) | Change to say "... there are one or two GTKSAs ..." | **REJECTED.**The cited text is consistent with the baseline rule that there is **one** GTKSA per BSS: “In an infrastructure BSS, there is **one** GTKSA, used exclusively for encrypting group addressed MPDUs that are transmitted by the AP and for decrypting group addressed transmissions that are received by the STAs.”  |
| 13175 | Mark RISON | 12.6.1.1.11 | 347 | 23 | "An AP MLD'sSME creates a BIGTKSA for each of its links when dot11BeaconProtectionEnabled is true." is not clear as to whether there is a single BIGTKSA that is used for all the links, or a different BIGTKSA for all the links | Change to "An AP MLD'sSME creates a single BIGTKSA that is used for each of its links when dot11BeaconProtectionEnabled is true." | **REJECTED.**One BIGTKSA is created for each setup link, so the proposed change to specify “a single BIGTKSA” is not correct. The original sentence is correct. |
| 13176 | Mark RISON | 12.6.1.1.6 | 346 | 1 | This should not be a new bullet | Delete the new bullet. At the end of the previous bullet add "For MLO, the Authenticator MAC address is the MLD MAC address of the AP MLD." and at the end of the bullet before add "For MLO, theSupplicant MAC address is the MLD MAC address of the non-AP MLD" | **ACCEPTED.** |
| 13177 | Mark RISON | 12.6.1.1.8 | 346 | 44 | This should not be a new bullet | Delete the new bullet. At the end of the previous bullet add "For MLO, the Authenticator MAC address is the MLD MAC address of the AP MLD." | **REVISED.**Agree with the comment. The same changes is also applied to IGTKSA.TGbe editor to make the changes shown in IEEE 802.11-22/1646r0 under all headings that include CID 13177. |
| 13178 | Mark RISON | 12.6.1.1.11 | 347 | 40 | This should not be a new bullet | Delete the new bullet. At the end of the previous bullet add "For MLO, the Authenticator MAC address is the MLD MAC address of the AP MLD." | **ACCEPTED.** |
| 13180 | Mark RISON | 12.6.1.1.11 | 347 | 29 | "A non-AP MLD's SME creates a BIGTKSA for its setup link whendot11BeaconProtectionEnabled is true, upon receiving a BIGTK for the link from its Authenticator." is not clear: which is the SME's "setup link"? | "A non-AP MLD's SME creates a BIGTKSA for each of its setup links whendot11BeaconProtectionEnabled is true, upon receiving BIGTKs for the links from its Authenticator." | **REVISED.**Agree with the comment to clarify that the BIGTKSA is created for each of its setup links. The change is already made as part of the resolution for CID 12981 in IEEE 802.11-22/1646r0. No further changes required from the TGbe editor for CID 13180. |
| 13181 | Mark RISON | 12.6.1.1.11 | 347 | 23 | "An AP MLD'sSME creates a BIGTKSA for each of its links when dot11BeaconProtectionEnabled is true." is not clear as to whether there is a single BIGTKSA that is used for all the links, or a different BIGTKSA for all the links | Change to "An AP MLD'sSME creates a different BIGTKSA for each of its links when dot11BeaconProtectionEnabled is true." | **REJECTED.**The emphasis here is that one BIGTKSA is created for each setup link, it is not necessary to specify whether they are same or different across links. |
| 13203 | Jing Guo | 12.6.1.1.6 | 346 | 1 | This bullet should be moved to elsewhere given the fact that it explains the previous points | as in comment | **REVISED.**Agree with the comments, however this issue is already resolved as part of the resolution for CID 13176 in IEEE 802.11-22/1646r0. No further changes required from the TGbe editor for CID 13203.  |
| 13498 | Liwen Chu | 12.6.1.1.6 | 346 | 1 | This bullet should not be an independent bullet since it explains the previous bullets. | move the content of it to the proper location | **REVISED.**Agree with the comments, however this issue is already resolved as part of the resolution for CID 13176 in IEEE 802.11-22/1646r0. No further changes required from the TGbe editor for CID 13498. |
| 13499 | Liwen Chu | 12.6.1.1.8 | 346 | 44 | With the added bullet, an AP MLD can't configure the diffreent GTK for each link. | Update the GTK creation formula or change the text here | **REVISED.**Even though the GTK generation method provided in the baseline is only an example, agree with the comment that it is better to associate the GTKSA for each link with the MAC Address of the AP operating on the link.TGbe editor to make the changes shown in IEEE 802.11-22/1646r0 under all headings that include CID 13499. |
| 13500 | Liwen Chu | 12.6.1.1.9 | 347 | 16 | With the added bullet, an AP MLD can't configure the diffreent IGTK for each link. | Update the IGTK creation formula or change the text here | **REVISED.**Even though the IGTK generation method is not provided in the baseline, agree with the comment that it is better to associate the IGTKSA for each link with the MAC Address of the AP operating on the link.TGbe editor to make the changes shown in IEEE 802.11-22/1646r0 under all headings that include CID 13500. |
| 13501 | Liwen Chu | 12.6.1.1.11 | 347 | 40 | With the added bullet, an AP MLD can't configure the diffreent BIGTK for each link. | Update the BIGTK creation formula or change the text here | **REVISED.**Even though the BIGTK generation method is not provided in the baseline, agree with the comment that it is better to associate the BIGTKSA for each link with the MAC Address of the AP operating on the link.TGbe editor to make the changes shown in IEEE 802.11-22/1646r0 under all headings that include CID 13501. |

The baseline for this document is 11be D2.1.

**Discussion:** None.

SP: Do you agree to incorporate the changes provided in IEEE 802.11-22/1646r0 for the below listed CIDs to the next revision of 802.11be draft?

12094, 12095, 12096, 12980, 12981, 13174, 13175, 13176, 13177, 13178, 13180, 13181, 13203, 13498, 13499, 13500, 13501

12.6.1.1.8 GTKSA (#12094, #13177, #13499)

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

The GTKSA results from a successful 4-way handshake, FT 4-way handshake, FT protocol, FT resource request protocol, group key handshake, or FILS authentication, and is unidirectional. In an infrastructure BSS, there is one GTKSA, used exclusively for encrypting group addressed MPDUs that are transmitted by the AP and for decrypting group addressed transmissions that are received by the STAs. Between an AP MLD and a non-AP MLD that have completed a successful multi-link (re)setup, for each setup link there is one GTKSA used exclusively for encrypting group addressed MPDUs that are transmitted by the (#12094) affiliated AP operating on the link and for decrypting group addressed transmissions that are received by the affiliated non-AP STA operating on the link.

...

A GTKSA consists of the following:

* Direction vector (whether the GTK is used for transmit or receive).
* Group cipher suite selector.
* GTK.
* (#13499) For non-MLO, Authenticator MAC address. (#13177) (#13499) operating on the link corresponding to the GTKSA

...

12.6.1.1.9 IGTKSA (#12980, #13177, #13500)

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

...

The Authenticator’s SME creates an IGTKSA when it establishes or changes the IGTK with all STAs to which it has a valid PTKSA or mesh PTKSA. An AP MLD’s SME creates an IGTKSA for (#12980) each of its links when it establishes or changes the IGTK with all non-AP STAs that operate on the link and are affiliated with the non-AP MLDs to which it has a valid PTKSA. An IGTKSA has the same lifetime as the BSS, unless superseded.

An IGTKSA consists of the following:

* Direction vector (whether the IGTK is used for transmit or receive)
* Key ID
* IGTK
* (#13499) For non-MLO, Authenticator MAC address(#13177). (#13500) operating on the link corresponding to the IGTKSA

12.6.1.1.11 BIGTKSA (#12981, #13178, #13501)

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

...

A Supplicant’s SME creates a BIGTKSA when dot11BeaconProtectionEnabled is true, upon receiving a BIGTK from its Authenticator. A non-AP MLD’s SME creates a BIGTKSA for (#12981) each of its setup link when dot11BeaconProtectionEnabled is true, upon receiving a BIGTK for the link from its Authenticator.

A BIGTKSA consists of the following:

* Direction vector (whether the BIGTK is used for transmit or receive)
* Key ID
* BIGTK
* (#13499) For non-MLO, Authenticator MAC address(#13178). (#13501) operating on the link corresponding to the BIGTKSA

12.6.1.1.6 PTKSA (#13176)

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

...

The PTKSA consists of the following:

* PTK, where the PTK includes the KDK when WUR frame protection is negotiated
* Pairwise cipher suite selector, and when WUR frame protection is negotiated, the cipher suite selector 00-0F-AC:6 (BIP-CMAC-128) for individually addressed WUR Wake-up frames
* Supplicant MAC address or STA’s MAC address(#13176). For MLO, the Supplicant’s MAC address is the MLD MAC address of the non-AP MLD.
* Authenticator MAC address or BSSID(#13176). For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD.
* (#13176)

12.7.1.4 Group key hierarchy (#13499)

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

The group temporal key (GTK) shall be a random number. The following is an example method for deriving a random GTK. Any other pseudorandom function, such as that specified in 12.7.1.2 (PRF), could also be used.

...

In this example, the following apply:

a) Group nonce (GNonce) is a random or pseudorandom value contributed by the IEEE 802.1X

Authenticator.

b) The GTK is derived from the GMK by GTK PRF-Length(GMK, “Group key expansion”, AA || GNonce)

(#13499) NOTE - for MLO, AA is replaced with the MAC address of the AP operating on the link.

...

