IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for 11be D1.0Group Key Handshake CIDs |
| Date: 2021-11-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
| Po-Kai Huang | Intel |  |  |  |
| Mike Montemurro | Huawei |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGbe comment collection 36 (TGbe Draft 1.0).

* CIDs: 6205, 6632, 6723, 6724, 7883 (5 CIDs)

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Corrected the resolution and text for CID **6205** regarding GTKSA/IGTKSA/BIGTKSA which are established between AP MLD and non-AP MLD as per D1.4 and not between affiliated APs and affiliated non-APs as proposed in 1277r0. Changes in CYAN.
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 |
| 6205 | Michael Montemurro | 35.3.5.2 | 256 | 10 | The second paragraph of this subclause is redundant with the details described in Clause 12 and should be modified to describe the secuirty association. | Change "Different links use different GTK/IGTK/BIGTK and each link has its own PN space. TheGTK/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)."to"After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, GTKSA, BIGTK SA, and IGTK SAs are established between each affiliated STA and affilated AP managed through the AP MLD and non-AP MLD SME. Key update procedures for group keys are performed between the AP MLD and the non-AP MLD as defined in 12.7.7 (Group key handshake."Note: This proposed resolution assumes that the text changes in https://mentor.ieee.org/802.11/dcn/21/11-21-0300-03-00be-crs-for-d0-3-group-key-handshake-cids.docx are incorporated into the draft. | **Revised.**Agree with the comment that group key security association should be described, however as of D1.3 they are missing in clause 12 and related text is added in 35.3.5.2 (Multi-link security) as part of this resolution to clarify that after a successful multi-link (re)setup between an AP MLD and a non-AP MLD GTKSA, IGTKSA and BIGTKSA are established between an AP MLD and a non-AP MLD for each setup link. Regarding group key update, the relevant text is already added in D1.4. TGbe editor to make the changes shown in IEEE 802.11-21/1277r1 under all headings that include CID 6205. |
| 6632 | Po-Kai Huang | 12.7.7 | 209 | 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 for MLO it should be possible to carry the GTK/IGTK/BIGTK KDEs of multiple links in a single group key handshake. The relevant text is already added in D1.3. No further action required from the TGbe editor for CID 6632. |
| 6723 | Rojan Chitrakar | 12.7.7 |   |   | 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 for MLO it should be possible to carry the GTK/IGTK/BIGTK KDEs of multiple links in a single group key handshake. The relevant text is already added in D1.3. No further action required from the TGbe editor for CID 6723. |
| 6724 | Rojan Chitrakar | 12.7.7 |   |   | The same MLO KDE (e.g. MLO GTK) may occur multiple times for the same link in a Group Key handshake Message 1, e.g. for different Key IDs. | Allow the same MLO KDE (e.g. MLO GTK) to occur multiple times for the same link (and not just for different links) in a Group Key handshake Message 1, e.g. for different Key IDs. | **Rejected.**Similar comment as CID 6722. CID 6724 is rejected with the same resolution: there is only one MLO GTK per link passed from the Authenticator to the Supplicant in the 4-way handshake or the group key handshake. |
| 7883 | Yongho Seok | 35.3.5.2 | 256 | 10 | "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)."Group key handshake (12.7.7) can be also used to deliver the GTK/IGTK/BIGTK of each setup links. | Include the group key handshake. | **Revised.**Agree with the comment that for MLO it should be possible to carry the GTK/IGTK/BIGTK KDEs of multiple links in a single group key handshake. The relevant text is already added in D1.3. No further action required from the TGbe editor for CID 7883. |

Baseline is 11be\_D1.4 and REVme\_D1.0

Discussion for r1:

As of 11be D1.4, it appears that it is already agreed that GTKSAs are manged by the affiliated APs (i.e., an AP MLD would establish mutliple GTKSAs with a non-AP MLD, one per setup link). Selected texts:

***12.6.3.2 RSNA policy selection for MLO***

*… (#6596)The AP MLD manages the PTKSA* ***while the affiliated APs manage the GTKSA****.*

***12.5.3.3.7 CCM originator processing***

*The PN values sequentially number each MPDU. Each transmitter* ***(#6044)****STA that is not affiliated with an MLD shall maintain a single PN (48-bit counter) for each PTKSA and GTKSA. Each MLD shall maintain a single PN (48-bit counter) for each PTKSA****. Each AP affiliated with an AP MLD shall maintain a single PN (48-bit counter) for each GTKSA.*** *Each transmitter STA that is affiliated with an MLD shall use the PN that is maintained by the MLD.*

The GTKSAs are a result of the authentication (e.g., 4-way handshake) between the non-AP MLD and the AP MLD. The AP MLD Authenticator, not the affiliated AP Authenticator distributes the key to a non-AP MLD for each setup link. It's also the AP MLD that updates the GTK, IGTK, and BIGTK for the non-AP MLD, so the SA is still established at the AP MLD.

Based on the above, the resolution for CID 6205 is modified to align with the text in D1.4. While D1.4 doesn’t explicitly state that IGTKSA and BIGTKSA are also managed by the affiliated APs, by extension of GTKSA, the same is also proposed for IGTKSA and BIGTKSA.

--------

SP: Do you agree to incorporate the changes proposed in IEEE 802.11-21/1277r1 to the latest 11be draft for the following CIDs?

CID: 6205

**12.6 RSNA security association management**

**12.6.1 Security associations**

**12.6.1.1 Security association definitions**

12.6.1.1.8 GTKSA (CIDs 6205)

***TGbe editor: Change the subclause as follows (Track Change 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. (#6205) 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 AP affiliated with the AP MLD and for decrypting group addressed transmissions that are received by the non-AP STAs affiliated with the non-AP MLD. In an IBSS or in a PBSS, each STA defines its own GTKSA, which is used to encrypt its group addressed transmissions, and stores a separate GTKSA for each peer STA so that encrypted group addressed traffic received from other STAs may be decrypted. A GTKSA is created by the Supplicant’s SME when message 3 of the 4-way handshake is received, when message 1 of the group key handshake is received, when the Reassociation Response frame of the FT handshake is received, or when the FILS authentication with a status code indicating success is received. The GTKSA is created by the Authenticator’s SME when the SME changes the GTK and has sent the GTK to all STAs with which it has a PTKSA. It has the same lifetime as the BSS, unless superseded. A GTKSA consists of the following:

* Direction vector (whether the GTK is used for transmit or receive).
* Group cipher suite selector.
* ~~(#6205) For non-MLO,~~ GTK. ~~For MLO, one GTK for each setup link.~~
* Authenticator MAC address.
* (#6205) For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD.
* Key ID.
* All authorization parameters specified by local configuration. This might include parameters such as the STA’s authorized SSID.

When the GTK is used to encrypt individually addressed traffic (the selectable cipher suite is “Use group cipher suite”), the GTKSA is bidirectional.

* IGTKSA (CIDs 6205)) (CIDs 6

When management frame protection is enabled, a non-AP STA’s SME creates an IGTKSA when it receives a valid message 3 of the 4-way handshake or FT 4-way handshake, the Reassociation Response frame of the fast BSS transition protocol with a status code indicating success, a Mesh Peering Open Message of the Authenticated Mesh Peering Exchange (AMPE) protocol, a valid message 1 of the group key handshake, or the (Re)Association Response frame of FILS authentication with a status code indicating success. (#6205) When management frame protection is enabled, a non-AP MLD’s SME creates an IGTKSA for each of the setup links when it receives a valid message 3 of the 4-way handshake or FT 4-way handshake, or the Reassociation Response frame of the fast BSS transition protocol with a status code indicating success, a valid message 1 of the group key handshake. 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(#240). (#6205) An AP MLD’s SME creates an IGTKSA for any 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
* ~~(#6205) For non-MLO,~~ IGTK~~. For MLO, one IGTK for each setup link.~~
* Authenticator MAC address
* (#6205) For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD.
* BIGTKSA (CIDs 6205)

An Authenticator’s SME creates a BIGTKSA when dot11BeaconProtectionEnabled is true. (#6205) An AP MLD’s SME creates a BIGTKSA for each of its links when dot11BeaconProtectionEnabled is true. A BIGTKSA has the same lifetime as the BSS, unless superseded.

A Supplicant’s SME creates a BIGTKSA when dot11BeaconProtectionEnabled is true, upon receiving a BIGTK from its Authenticator. (#6205) A non-AP MLD’s SME creates a BIGTKSA for its setup link when dot11BeaconProtectionEnabled is true, upon receiving a BIGTK for the link from its Authenticator.

* Direction vector (whether the BIGTK is used for transmit or receive)
* Key ID
* ~~(#6205) For non-MLO,~~ BIGTK~~. For MLO, one BIGTK for each setup link.~~
* Authenticator MAC address
* (#6205) For MLO, the Authenticator’s MAC address is the MLD MAC address of the AP MLD.

35.3.5.2 Multi-link security (CIDs 6205)

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

After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMKSA and PTKSA are established between the non-AP MLD and the AP MLD (#6205), while a GTKSA, an IGTKSA, if management frame protection is enabled, and a BIGTKSA, if beacon protection is enabled, are established between the non-AP MLD and the AP MLD for each setup link (see Clause 12 (Security)). The PTKSA is used for cryptographic encapsulation and decapsulation of individually addressed MPDUs across all setup links and the GTKSA of a link is used for cryptographic encapsulation and decapsulation of group addressed MPDUs on the link as described in 12.5.3.3 (CCMP cryptographic encapsulation), 12.5.5.3 (GCMP cryptographic encapsulation), 12.5.3.4 (CCMP decapsulation) and 12.5.5.4 (GCMP decapsulation). When management frame protection is enabled, the IGTKSA of a link is used to provide integrity protection for group addressed robust management frames on the link as described in 12.6.19 (Protection of robust Management frames). When beacon protection is enabled, the BIGTKSA of a link is used to provide integrity protection for Beacon frames on the link as described in 12.6.23 (Protection of Beacon frames).

Different (#6205) APs affiliated with an AP MLD use different GTK/IGTK/BIGTK. Each AP and the corresponding non-AP STA affiliated with an associated non-AP MLD maintains a single PN/IPN/BIPN for each GTK/IGTK/BIGTK. 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).