IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment Resolutions for 11be D2.0 ML Security CIDs | | | | |
| Date: 2022-10-19 | | | | |
| 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: 10233, 13360 (2 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 |
| 10233 | John Wullert | 35.3.5.2 | 423 | 25 | The conditional phrases describing when IGTKSA and BIGTKSA are required make it hard to parse this sentence accurately. | Rephrase as "After a successful multi-link (re)setup between a non-AP MLD and an AP MLD, a PMKSA and a PTKSA are established between the non-AP MLD and the AP MLD. At the same time, a GTKSA is established between the non-AP MLD and the AP MLD for each setup link, as are an IGTKSA if management frame protection is enabled and a BIGTKSA if beacon protection is enabled, (see Clause 12 (Security)). | **REVISED.**  Agree with the comment that the cited sentence can be rewritten for better readability.    TGbe editor to make the changes shown in IEEE 802.11-22/1647r0 under all headings that include CID 10233. |
| 13360 | Liwen Chu | 35.3.5.2 | 423 | 31 | change to "the GTKSA of a link is used for cryptographic encapsulation and decapsulation of group addressed Data MPDUs" | As in comment | **REJECTED.**  The proposed change is to limit the usage of GTKSA to Data MPDUs, however in baseline (see 12.6.1.1.8 GTKSA), GTKSA is not limited to group address data MPDUs. |

The baseline for this document is 11be D2.2.

SP: Do you agree to incorporate the changes provided in IEEE 802.11-22/1647r0 for the below listed CIDs to the next revision of 802.11be draft?

10233, 13360

Discussion for CID 13360:

Graphical user interface, text, application, email

Description automatically generated

In baseline, GTKSA is not limited to group address data MPDUs.

35.3.5.2 Multi-link security (CIDs 10233)

***TGbe editor: Modify the subclause 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 a PTKSA are established between the non-AP MLD and the AP MLD (#10233). Concurrently, 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 across 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).

…