IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment resolutions for BIP amendments for protected WUR |
| Date: 2019-08-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Alfred Asterjadhi | Qualcomm Inc. | 5775 Morehouse Dr, San Diego, CA 92109 | +1-858-658-5302 | aasterja@qti.qualcomm.com |

Abstract

This submission proposes resolutions for multiple comments related to TGba D3.0 with the following CIDs (2 CIDs):

* 3402, 3403

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revised version including feedback received from Rojan. Changes in green.

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 TGba Draft. This introduction is not part of the adopted material.

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

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 3402 | Yunsong Yang | 89.39 | The third paragraph under 12.5.1 in the baseline standard reads: "BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust Management frames. BIP is used only to protect Management frames within the BSS.", thus needs to be updated to reflect the use of BIP for protected WUR frames. | Change the cite paragraph to read: "BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust Management frames, broadcast and group addressed WUR Wake-up frames, and individually addressed WUR Wake-up frames. BIP is used only to protect Management frames and WUR Wake-up frames within the BSS." | Revised –Agree in principle with the comment. Proposed resolution accounts for the suggested changes (did not explicitly call out individually, group addressed, etc. since it is easier to cover all cases by simpy stating WUR Wake-up frames). Also amended the first paragraph of the subclause.TGba editor to make the changes shown in 11-19/1431r1 under all headings that include CID 3402. |
| 3403 | Yunsong Yang | 90.02 | For all the other group keys, the baseline standard has defined where the key identifier is encoded. But this draft didn't specify where the key identifier for the WIGTK is encoded. If such key identifier is not explicitly included in the frame being protected, need to define which frame carries this key identifier. | As commented. | Revised –Agree in principle with the comment. Proposed resolution is to clarify that the key is encoded in the Key ID field carried in two elements, for which the subclause reference is provided.TGba editor to make the changes shown in 11-19/1431r1 under all headings that include CID 3403. |

**Discussion: *None.***

* RSNA confidentiality and integrity protocols

**12.5.1 Overview**

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 3402):***

This standard defines the following RSNA data confidentiality and integrity protocols: TKIP, CCMP, and GCMP. This standard defines one integrity protocol for Management frames and for WUR Wake-up frames: BIP.*(#3402)*

Implementation of TKIP is optional for an RSNA and used only for the protection of Data frames. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradable by the supplier to support TKIP.

BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust Management frames, and for WUR Wake-up frames (see 29.10 (Protected WUR frames)). BIP is used only to protect Management frames and WUR Wake-up frames within the BSS.*(#3402)*

* Broadcast/multicast integrity protocol (BIP)
* BIP overview

***Change the 1st paragraphs as follows:***

BIP provides data integrity and replay protection for group addressed robust Management frames after establishment of an IGTKSA (see 12.6.1.1.9 (IGTKSA)) and for Beacon frames after establishment of a BIGTKSA (see 12.6.1.1.11 (BIGTKSA)). BIP also provides integrity and replay protection for individually addressed and group addressed WUR frames (see 29.10 (Protected WUR frames)).(#2814)

**TGba Editor: *Change the paragraph below of this subclause as follows (#CID 3403):***

BIP uses the IGTK or BIGTK to compute the MMPDU MIC, uses the WTK to compute the MIC for protecting individually addressed WUR Wake-up frames, and uses the WITGK to compute the MIC for protecting broadcast or group addressed WUR Wake-up frames. The authenticator shall distribute one new IGTK and IGTK PN (IPN) whenever it distributes a new GTK. The IGTK is identified by the MAC address of the transmitting STA plus an IGTK identifier that is encoded in the MME Key ID field. If beacon protection is enabled, the authenticator may distribute one new BIGTK and BIPN when it distributes a new GTK. The BIGTK is identified by the MAC address of the transmitting STA plus a BIGTK identifier that is encoded in the MME Key ID field. If WUR frame protection is negotiated, the authenticator may distribute one new WIGTK and WIPN when it distributes a new GTK. The WIGTK is identified by the MAC address of the transmitting STA plus the WIGTK identifier that is encoded in the Key ID field (see Figure 12-47a (WIGK KDE), 9.4.2.301 (WUR PN Update element) and 9.4.2.47 (Fast BSS Transition element)).*(#3403)* (#2337, #2579)