IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment resolutions for protected WUR frames – part 1 |
| Date: 2019-04-10 |
| 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 D2.0 with the following CIDs (18 CIDs):

* 2057, 2067, 2118, 2420, 2518, 2557, 2560, 2580, 2581, 2820,
* 2821, 2822, 2329, 2331, 2339, 2321, 2322, 2328

Revisions:

* Rev 0: Initial version of the document.

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** |
| 2057 | Alfred Asterjadhi | 76.49 | Several CIDs that were listed in document 11-18/2145r2 were not resolved. Review and resolve the issues that were identified by the unresolved CIDs that are contained in that document. | As in comment. | Rejected –The comment fails to identify changes in enough detail for the group to make changes that would satisfy the comment. Several CIDs that were rejected during the previous LB are now being addressed by the group and the expectation is that those issues are addressed by the incorporation of changes due to the new comments.  |
| 2067 | Amelia Andersdotter |  | In LB235, it was indicated to the group that the procedures described in clause 31.8 has serious implications for privacy and security. Hostile wake ups can have serious concerns over battery drainage and false functioning of systems in case of association with the attacker. Intruder can eavesdrop privacy information in WUR packets. The response to this from the TGba is "TGba is unable to reach consensus on a resolution" which is really not satisfactory - it could have just as easily been "can't be arsed". | Fix the problem. | Rejected –Protected WUR frames were introduced to address security and randomization of WUR IDs can address privacy. |
| 2118 | Guido Hiertz | 77.17 | This chapter is not for the definition of fields. | Move definition of AAD to Clause 9. | Rejected –Clause 9 is for the definition of fields of frames or fields that are carried in frames. The AAD definition here is provided to provide the AAD structure which is used for its construction. This is equivalent to the definitions of other AADs that are provided in clause 12, which in the WUR case these functionalities are defined here.  |
| 2420 | Michael Montemurro | 76.52 | There are multiple types of WUR frames. Are they all protected using the same mechanism? It doesn't sound like it | Explain the protection (or no protection) associated with each type of WUR frame). | Revised –Agree in principle with comment. Currently only WUR Wake up frames can be protected. Proposed resolution is to explicitly state this in the first subclause. TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2420. |
| 2518 | Po-Kai Huang | 77.10 | Pairwise temporal key is mentioned here, but I think the intention is to say PTK, which is pairwise transient key. | Change pairwise temporal key to pairwise transient key. | Revised –Agree in principle with the comment. The proposed resolution clarifies the terminology, inline with its use in 12.7.6.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2518. |
| 2557 | Po-Kai Huang | 77.17 | It will be better to have a reference here for the embedded BSSID. | As in comment. | Revised –Agree in principle with the comment. Proposed resolution adds a reference to the sublcause that defines the Compressed BSSDI and specifies that the embedded BSSID is the 16 MSBs of it.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2557. |
| 2560 | Po-Kai Huang | 77.39 | IPN is called IGTK packet number in revmd 2.1. Since we use WUR IGTK, IPN is no longer a proper name. Given that in 30.9.3.1, IPN is simply PN for different case. Propose to simply use PN. | As in comment. | Revised –Agree in principle with the comment. Since PN is used also in other clauses the proposed resolution is to append “WUR” to it.TGba Editor: Please replace “IPN” with WUR PN” throughout the draft. |
| 2580 | Rojan Chitrakar | 77.38 | What is the "current Key ID value"? An AP may have may Keys installed, its better to explicitly refer to the KEY ID associated with the WUR keys. | change "current Key ID value" to:the corresponding WUR IGTK or WUR TK Key ID value" | Accepted |
| 2581 | Rojan Chitrakar | 77.43 | MIC field is not defined in "IPN, and insert the truncated output into the MIC field of the WUR frame." | Change to:"IPN, and insert the 16-bit truncated output (MIC) into the FCS field of the WUR frame." | Revised –Agree in principle with the comment. Proposed resolution accounts for the suggested changes, plus certain editorial improvements.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2581. |
| 2820 | Yunsong Yang | 77.05 | "an integrity key" cannot be just any integrity key. It must be one of the two keys mentioned in the following sub-bullet. Also, recommend to break the following sub-bullet into two such that the uses of the WUR IGTK and WUR TK are clearly separated. | Change "an integrity key to compute the MIC of the WUR frame." to "an integrity key to compute the MIC of the WUR frame, as defined below:" And break the sub-bullet following the cited sentence into two bullets such that one is for the broadcast and group addressed WUR frames, and the other is for the individually addressed WUR frames. | Revised –Agree in principle with the comment. Proposed resolution accounts for the suggested changes, plus certain editorial improvements.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2820. |
| 2821 | Yunsong Yang | 77.16 | The AAD construction is one of the exceptions, which the first paragraph of this page starts to decribe, therefore, should be listed as a level-1 bullet, like the other two level-1 bullets above it. | Change the cited paragraph as the third level-1 bullet under the first paragraph of this page. | Accepted |
| 2822 | Yunsong Yang | 77.16 | The AAD construction doesn't include the TD Control field, thus allowing attacks that replays a legimate Protected WUR frame with a forged sequence number. | Revised the cited paragraph and Figure 30-2 such that the AAD has a length of 48 bits, consisting of the Frame Control, the ID field, the Type Dependent Control field, and the Embedded BSSID field, without any reserved bit. | Rejected –The TD Control field contains the LSBs of the PN, which is used to calculate the MIC but is not part of the AAD. A forget SN in this case would cause the MIC to fail.This is similar in nature with descriptions of current encryption techniques (please refer to clause 12 descriptions of AAD construction). |
| 2329 | MARC EMMELMANN | 60.30 | MIC field is not defined in "..., and insert the truncated output into the MIC field of the WUR frame." | Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Revised –Agree in principle with the comment. Proposed resolution is based on the proposed changes suggested by CID 2581, which is essentially a copy of the comment cited by the commenter in this comment.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2329. |
|  |  |  |  |  |  |
| 2331 | MARC EMMELMANN | 60. 24 | What is the "current Key ID value"? An AP may have may Keys installed, its better to explicitely refer to the KEY ID associated with the WUR keys. | Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Revised –Agree in principle with the comment. Proposed resolution is based on the proposed changes suggested by CID 2580, which is essentially a copy of the comment cited by the commenter in this comment.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2331. |
| 2339 | MARC EMMELMANN | 59. 35 | Explicitly call out which WUR frames can be protected and which ones cannot. And also that when protection is used then it is used all the times between that AP and WUR STA. Also clarify what is meant with "current Key ID" in this subclause, from both the transmitters perspective and from the recipients perspective. | Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Revised –Agree in principle with the comment. Currently only WUR Wake Up frames can have the Protected bit set to 1. Proposed resolution calls out the WUR Wake up frame as being protected. TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2339. |
| 2321 | MARC EMMELMANN | 60.59 | What is the "current Key ID value"? A STA may have may Keys installed, its better to explicitely refer to the KEY ID associated with the WUR keys. | Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Revised –Agree in principle with the comment. Proposed resolution is based on the proposed changes suggested by CID 2580, which is essentially a copy of the comment cited by the commenter in this comment.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2321. |
| 2322 | MARC EMMELMANN | 60.58 | The bullets on L58 and L60 shouldn't be at the same level as the previous bullets, because they are executed only when the MIC values match under the previous bullet. | Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Agree in principle with the comment. Proposed resolution is based on the proposed changes suggested by CID 2821, which is essentially similar in content as the comment cited by the commenter in this comment.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2322. |
|  |  |  |  |  |  |
| 2328 | MARC EMMELMANN | 60.42 | What is the "current Key ID value"? A STA may have may Keys installed, its better to explicitely refer to the KEY ID associated with the WUR keys. | Picking up on comments made in the previous letter ballot on D1.0, the TG did not properbly address the issue raised in the comment, nor does the TG provide an indication that the text commented on has been deleted and hence the comment does not apply. (Note, page and line and sublause number refer to D1.0). In fact, as stated in the TGba minutes (11-19/226r0), the intend of the task group was to "Move to resolve CIDs that have no approved resolution as rejected with a reason read "TGba is unable to reach consensus on a resolution" in the interest of releasing draft 2.0". Also, the statement ""TGba is unable to reach consensus on a resolution" was added to the motion text there was one person speaking against the motion." was only added to the motion after objection to the original motion trying to reject comments in bulk with the reason of releasing a new LB.The TG is asked to give the original comment due consideration and debade the proposed comment resolution as included in 11-18/1794r10. The referenced document includes an actionable comment resolution. | Revised –Agree in principle with the comment. Proposed resolution is based on the proposed changes suggested by CID 2580, which is essentially a copy of the comment cited by the commenter in this comment.TGba editor to make the changes shown in 11-19/0585r0 under all headings that include CID 2328. |

**Discussion: *None.***

* Protected WUR frames

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 2420, 2339):***

A WUR AP may transmit a protected WUR Wake up frame addressed to a WUR non-AP STA if the Protected WUR Frame Support field in the WUR Capabilities element transmitted by the WUR AP and the WUR non-AP STA is set to 1; otherwise the AP shall not transmit a protected WUR Wake up frame to the WUR non-AP STA.*(#2420, 2339)*

A WUR AP may transmit a protected WUR Wake up frame addressed to more than one WUR non-AP STAs if the Protected WUR Frame Support field in the WUR Capabilities element transmitted by the WUR AP and all the WUR non-AP STAs is set to 1.*(#2420, 2339)*

The WUR AP shall set the Protected subfield of the Frame Control field of transmitted WUR Wake up frames to 1 if the WUR frame is protected; otherwise the WUR AP shall set the Protected subfield of the Frame Control field of the WUR frame to 0.*(#2420, 2339)*

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 2518, 2820, 2557, 2821, 2322, 2339):***

The WUR AP shall protect the WUR Wake up frame using the BIP protocol as defined in 12.5.4 (Broadcast/multicast integrity protocol (BIP)) except that:

* The WUR AP shall use BIP-CMAC-128 to provide data integrity and replay protection and shall use an integrity key to compute the MIC of the WUR Wake up frame, which is defined below:
* Broadcast and group addressed WUR Wake up frames shall be protected using a separate WUR integrity group temporal key (IGTK) that is negotiated as defined in 12.7.7 (Group key handshake)
* Individually addressed WUR Wake up frames shall be protected using a separate WUR temporal key (TK) that is negotiated as defined in 12.7.6 (4-way handshake).*(#2518, 2820)*
* The CMAC output for BIP-CMAC-128 shall be truncated to 16 bits: MIC = Truncate-16 (CMAC Output). The MIC shall be included in the FCS field of the protected WUR Wake up frame.*(#2420, 2339)*
* The AAD shall have a length of 40 bits consisting of the Frame Control and the ID field, which are obtained from the WUR Wake up frame, the Embedded BSSID field, which is equal to the 16 MSBs of the compressed BSSID (see 30.4.1a (Compressed BSSID), and 4 reserved bits as shown in Figure 30-2 (AAD construction for WUR frames).*(#2420, 2557, 2822, 2821, 2322, 2339)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0          B7 | B8             B19 | B20             B23 | B24             B39 |
|  | Frame Control | ID | Reserved | Embedded BSSID |
| Bits: | 8 | 12 | 4 | 16 |
| * AAD construction for WUR frames
 |

* Protected WUR frame transmission

**TGba Editor: *Change the paragraphs below of this subclause as follows (#CID 2580, 2581, 2331, 2321, 2328, 2560, 2329):***

A WUR AP that sends a protected WUR frame shall follow the rules in 12.5.4.5 (BIP transmission) except that the WUR AP shall:

* Select the appropriate integrity key associated to protected WUR frames (see 30.9 (Protected WUR frames)), Key ID that is equal to the corresponding WUR IGTK or WUR TK Key ID value, a WUR PN that is generated and partially included in the WUR frame as defined in 30.9.3.1 (Generation of the IPN by a WUR AP).*(#2580, 2331, 2321, 2328, 2560)*
* Construct the AAD as defined in Figure 30-2 (AAD construction for WUR frames).
* Compute an integrity value over the concatenation of AAD, the Frame Body field (if present), and the WUR PN, and insert the 16-bit truncated output, which is the MIC, into the FCS field of the WUR frame. The integrity value is computed using AES-128-CMAC.*(#2581, 2560, 2329)*
* Transmit the protected WUR frame.