IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for clause 30.9.2 and 30.9.3 Protected WUR frames – part 2 |
| Date: 2019-05-06 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
| Lei Huang |  |  |  |
| Yoshio Urabe |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGba comment collection (TGba Draft 2.0).

* CIDs:
	+ 2314, 2315, 2316,
	+ 2319, 2320, 2323,
	+ 2324, 2325, 2326, 2327
	+ 2559, 2582, 2583, 2587, 2588, 2589 (16 CIDs)

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Text changes based on offline discussions. Changes in blue.
	+ Changed resolution for CID 2588 to revised. Update of BPN only applies when the Common IPN subfield is 0.
	+ Removed Key ID update related texts. Key ID update is performed when the integrity key is set in the MAC.
	+ WUR Action frames are used for BPN update instead of header compression procedure.
	+ Revised the IPN initialization related text.
* Rev 2:
	+ CID 2317 is deferred.
	+ Resolutions for some CIDs changed from Rejected to Revised.
* Rev 3: Revised text for BPN updatate based on feedback from Alfred. Changes in grey.
	+ Created a subclause for the BPN update procedure and moved all related text to the new subclause.
	+ Added text to mandate that Protected Management Frame shall be activated by a WUR STA that negotiates WUR Protection.
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 TGba 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 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 | Page.Line  | Clause | Comment | Proposed Change | Resolution |
| 2559 | Po-Kai Huang | 78.65 | 30.9.3.1 | Is the temporal key here mean WUR IGTK and WUR PTK? Similar question to page 79 line 7. | Propose to directly say WUR IGTK or WUR PTK. | **Revised.**Agree with the commenter. Since the integrity keys for protected WUR frames are negotiated separately, it is better to directly say WUR IGTK or WUR TK. TGba editor to make the changes shown in 11-19/0729r2 under all headings that include CID 2559. |
| 2582 | Rojan Chitrakar | 77.56 | 30.9.2 | What is the "current Key ID value"? A STA 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.** |
| 2583 | Rojan Chitrakar | 77.60 | 30.9.2 | How is the RC is initialized before the first protect WUR frame is received needs to be defined. Is it equal to the IPN when the link is established or is it provided during the 4 way/group key handshake? | Clarify how the RC is initialized before the first protect WUR frame is received | **Revised.**Agree with the commenter that it should be clarified how the replay counters (RC) are initialized. In addition, it is also clarified that separate RCs are maintained for WUR IGTK and WUR TK. TGba editor to make the changes shown in 11-19/0729r2 under all headings that include CID 2583. |
| 2587 | Rojan Chitrakar | 78.6 | 30.9.2 | What is the "current Key ID value"? A STA 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.** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 2316 | MARC EMMELMANN | 62.42 | 31.8.3.2 | should locally store BPN bit range be [17:56], because on L18 it says BPN is from bit 17 to 56? | 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. | **Rejected.**In D2.0 BPN has been changed to IPN so the bit range [9:56] is correct.   |
|  |  |  |  |  |  |  |
| 2319 | MARC EMMELMANN | 61.2 | 31.8.2 Protected WUR frame reception | "implementation specific value" needs to be defined. | 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. | **Rejected.**Implementation specific value means that the value is chosen based on whatever consideration of the implementers. |
| 2320 | MARC EMMELMANN | 60.61 | 31.8.2 | TSF update process should not be part of protected WUR frame reception. The protected reception should detect/filter corrupted frames, and then normal frame processing (including WUR Beacon processing, etc.) should happen, so that all these details can be kept in only one place in the Standard | 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. | **Rejected.**If the protected WUR frames carry TSF, it is required for a WUR STA to update its local TSF timer based on the received TSF in order to correctly validate the MIC.  |
| 2323 | MARC EMMELMANN | 60.55 | 31.8.1 | If the MIC value does not match, the STA should not proceed to the next step (Update the RC). | 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.**The issue is already resolved in D2.1. If the MIC value does not match, the BIP procession is terminated for this reception. No further change is required. |
| 2324 | MARC EMMELMANN | 60.53 | 31.8.2 | The following text (4th bullet point) should have an exit statement. Namely, if MIC error occurs, the rest of the procedure shall not be performed.If the result does not match the received MIC value, then the receiver shall discard the frame and increment its internal MIC error counter by 1. | 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.**The issue is already resolved in D2.1. If the MIC error occurs, the BIP procession is terminated for this reception. No further change is required. |
| 2325 | MARC EMMELMANN | 60.49 | 31.8.2 | dot11RSNAStatsCMACWURReplays is not defined. | 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.**The issue is already resolved in D2.1. dot11RSNAStatsCMACWURReplays is defined in D2.0. No further change is required. |
| 2326 | MARC EMMELMANN | 60.49 | 31.8.2 | If the replay protection failed (i.e. if the IPN is less than or equal to the RC), the STA should not proceed to the next step (construct AAD). | 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.**The issue is already resolved in D2.1. If the replay protection fails, the BIP procession is terminated for this reception. No further change is required. |
| 2327 | MARC EMMELMANN | 60.46 | 31.8.1 | How is the RC is initialized before the first protect WUR frame is received needs to be defined. Is it equal to the IPN when the link is established or is it provided during the 4 way/group key handshake? | 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 with the commenter that it should be clarified how the replay counters (RC) are initialized. In addition it is also clarified that separate RCs are maintained for WUR IGTK and WUR TK. TGba editor to make the changes shown in 11-19/0729r2 under all headings that include CID 2327. |

**Discussion:** None

**Propose:**

Revised for CIDs 2327, 2559, 2583, 2589 as per discussion and editing instructions in 11-19/0729r2.

* Protected WUR frames
* Protected WUR frame reception (CIDs 2327, 2583)

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

A WUR non-AP STA with WUR frame protection negotiated that receives a protected WUR Wake-up frame shall follow the rules in 12.5.4.6 (BIP reception) except that the WUR non-AP STA shall:

* Use the appropriate integrity key associated to protected WUR Wake-up frames (see 30.9 (Protected WUR frames)), and associated state based on Key ID equal to the current Key ID value.
* Perform replay protection on the received WUR Wake-up frame as defined in 12.5.4.4 (BIP replay protection) except that the WUR non-AP STA shall construct the IPN locally as defined in 30.9.3.2 (Construction of the IPN by a WUR non-AP STA) and the WUR non-AP STA shall maintain a separate replay counters (*RC*) for each WUR IGTK and WUR TK when the most recently received WUR Operation element has the Common IPN subfield equal to 0. The WUR non-AP STA shall initialize the replay counter to the initial value of the corresponding IPN prior to any update due to WUR Wake-up frames. The WUR non-AP STA shall also initialize the replay counter to the initial value of the corresponding IPN when it resets the WUR IGTK or WUR TK. If IPN is less than or equal to the corresponding *RC* then the WUR non-AP STA shall discard the WUR Wake-up frame, increment its internal dot11RSNAStatsCMACWURReplays counter by 1, and terminate BIP processing for this reception. (#2327, #2583)
* Construct the AAD as defined in Figure 30-2 (AAD construction for WUR frames).
* Extract and save the received MIC value from the FCS field of the WUR Wake-up frame and compute a verifier over the concatenation of AAD, Frame Body field (if present), and the locally constructed IPN. If the result does not match the received MIC value, then the receiver shall discard the frame, increment its internal MIC error counter by 1, and terminate BIP processing for this reception.(#2586)
* Update the *RC* for the integrity key associated to protected WUR Wake-up frames identified by Key ID equal to the current Key ID value with the corresponding IPN. (#2327, #2583)
* If the Common IPN subfield is equal to 1, update the local TSF timer as follows:

**…**

NOTE1—Before the adjusted value of the received partial TSF timestamp is set as the value of bit position 9 to 16 of the temporary timestamp, the temporary timestamp may be further compensated for a clock drift offset between the WUR AP and the WUR non-AP STA, which is determined by multiplying the estimated clock drift by the time between receiving the latest TSF from the WUR AP and the time at which the WUR frame is received from the WUR AP, where the estimated clock draft is determined based on two or more received TSF values from the WUR AP and comparing these to the internal TSF at the WUR non-AP STA.

NOTE2— When the most recently received WUR Operation element has the Common IPN subfield equal to 1, only a single common replay counter is maintained for both WUR IGTK and WUR TK. (#2327, #2583)

* Generation and construction of IPN for WUR frames

***TGba editor: Add the following sentences:***

The IPN for WUR IGTK is defined as WIPN and the IPN for WUR TK is defined as WTPN. When the Common IPN subfield in the WUR Operation element sent by the WUR AP is equal to 1 then WIPN and WTPN are derived in the same way and are equal. (#2327, #2583)

* Generation of the IPN by a WUR AP (CID 2559)

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

A WUR AP that intends to transmit protected WUR frames shall set the Common IPN subfield in the WUR Operation element it transmits to 0 if it intends to maintain separate IPN counters for WUR IGTK and WUR TK and shall set the Common IPN subfield to 1 if it intends to maintain a common IPN for all protected WUR frames generated within its BSS. (#2559)

The WUR AP that intends to transmit a protected WUR frame shall construct the IPN as follows:

—If the Common IPN subfield is equal to 1:

* IPN = PN0||PN1||PN2||PN3||PN4||PN5 = TSF timer [9: 56], where the TSF timer is obtained as defined in 30.5.1 (General).
* The IPN shall never repeat for protected WUR frames generated using the same WUR IGTK or WUR TK (#2559)
* The WUR AP shall include PN0, i.e., the PPN, which is equal to its TSF timer [9: 16], in the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame
* If the Common IPN subfield is equal to 0:
* IPN = PN0||PN1||PN2||PN3||PN4||PN5, where IPN shall be incremented by one for each transmitted WUR frame using the same WUR IGTK or WUR TK. (#2559)
* The IPN shall never repeat for protected WUR frames generated using the same WUR IGTK or WUR TK (#2559)
* The WUR AP shall include PN0||PN1[0:3] (i.e., the PPN) in the Type Dependent Control field of the WUR Wake-up frame, if the WUR Wake-up frame is not broadcasted

If the most recently transmitted WUR Operation element has the Common IPN subfield equal to 0, the local WTPN at the WUR AP is initialized to 0 and the local WIPN at the WUR AP is initialized to the WIPN provided in the WIGTK KDE (Figure 12-xxx WIGTK KDE format) when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)).. (#2327, #2583)

If the most recently transmitted WUR Operation element has the Common IPN subfield equal to 1,the local WTPN and WIPN at the WUR AP, which are the same in this case, are initialized to the value of the local TSF timer [9: 56] when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)). (#2327, #2583)

* Construction of the IPN by a WUR non-AP STA (CID 2559)

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

**…**

* If the Common IPN subfield is equal to 0, the IPN is obtained as follows:
* The IPN is obtained as PPN||BPN, where PPN is equal to the value of the Type Dependent Control field of the received WUR frame, and BPN is retrieved from the locally stored BPN at the receiver for the corresponding WUR IGTK or WUR TK (#2559)
* PN0||PN1[0:3] = PPN, and PN1[4:7]||PN2||PN3||PN4||PN5 = BPN

If the most recently received WUR Operation element has the Common IPN subfield equal to 0, the locally stored WTPN at the WUR non-AP STA is initialized to 0 and the local WIPN at the WUR non-AP STA is initialized to the WIPN provided in the WIGTK KDE (Figure 12-xxx WIGTK KDE format) when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)). (#2327, #2583)

If the most recently received WUR Operation element has the Common IPN subfield equal to 1, the locally stored WTPN and WIPN, which are the same in this case, at the WUR non-AP STA is initialized to the value of the local TSF timer [9: 56] when the corresponding integrity key (WTK or WIGTK) is set in the MAC (see 12.7.6 (4-way handshake) and 12.7.7 (Group key handshake)). (#2327, #2583)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Page.Line  | Clause | Comment | Proposed Change | Resolution |
| 2588 | Rojan Chitrakar | 80.1 | 30.9.3.2 | Explicit update of BPN would only be needed when the Common IPN subfield is 0. | Clarify that Explicit update of BPN only applies when the Common IPN subfield is 0. | **Revised.**Agree with the commenter that the update of BPN is only needed when the Common IPN subfield is 0. When the Common IPN subfield is 1, i.e. TSF is used as the PN, STA may use alternative methods to update the TSF. TGba editor to make the changes shown in 11-19/0729r3 under all headings that include CID 2588. |
| 2315 | MARC EMMELMANN | 62.47 | 31.8.3.2 | Explicit update of BPN would only be needed when the Common IPN subfield is 0. | 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 with the commenter that the update of BPN is only needed when the Common IPN subfield is 0. When the Common IPN subfield is 1, i.e. TSF is used as the PN, STA may use alternative methods to update the TSF. TGba editor to make the changes shown in 11-19/0729r3 under all headings that include CID 2315. |
| 2589 | Rojan Chitrakar | 80.1 | 30.9.3.2 | It is better to define a new element for this purpose (update of BPN) for WUR. Since 36 bits are required for BPN, the CCMP update field is not suitable anyway. Header compression has no meaning for WUR, it is better to use WUR Mode setup frames to carry the update element. And why does Key ID need to be updated. If key is changes, the entire key negotiation needs to be redone, and not simply update of Key ID. | Define a new element for this purpose (update of BPN) for WUR. Use WUR Mode setup frames to perform the exchange. | **Revised.**Agree with the commenter. A new element is defined for the purpose of updating of BPN. The element can be included in WUR Mode setup frames. A WUR STA will always use the latest installed Key, so Key ID update is not required. TGba editor to make the changes shown in 11-19/0729r3 under all headings that include CID 2589. |
| 2314 | MARC EMMELMANN | 62.47 | 31.8.3.2 | It is better to define a new element for this purpose (update of BPN) for WUR. Since 36 bits are required for BPN, the CCMP update field is not suitable anyway. Header compression has no meaning for WUR, it is better to use WUR Mode setup frames to carry the update element. And why does Key ID need to be updated. If key is changes, the entire key negotiation needs to be redone, and not simply update of Key ID. | 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 with the commenter. A new element is defined for the purpose of updating of BPN. The element can be included in WUR Mode setup frames. A WUR STA will always use the latest installed Key, so Key ID update is not required. TGba editor to make the changes shown in 11-19/0729r3 under all headings that include CID 2314. |

**Discussion:** We propose to use WUR Mode setup frames instead of the header compression frame for the BPN update.

**Propose:**

Revised for CIDs 2314, 2315, 2588, 2589 as per discussion and editing instructions in 11-19/0729r3.

30.9 Protected WUR frames (CID 2315, 2588, 2589, 2314)

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

**…**

A WUR AP that installs the WTK for a WUR non-AP STA (see 12.7.6 (4-way handshake)) shall use the WTK to protect all subsequent individually addressed WUR wake-up frames transmitted to the WUR non-AP STA. A WUR AP that installs the WIGTK (see 12.7.6 (4-way handshake) or 12.7.7 (Group key handshake)) shall use the WIGTK to protect all subsequent protected broadcast or group addressed WUR wake-up frames.

A WUR non-AP STA that installs the WTK (see 12.7.6 (4-way handshake)) shall use the WTK to process all subsequently received protected individually addressed WUR wake-up frames. A WUR non-AP STA that installs the WIGTK (see 12.7.6 (4-way handshake) or 12.7.7 (Group key handshake)) shall use the WIGTK to process all subsequently received protected broadcast or group addressed WUR wake-up frames. (#2314, #2315, #2588, #2589)

The WUR AP shall set the Protected subfield of the Frame Control field of transmitted WUR 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.

A WUR STA with dot11RSNAWURFrameProtectionActivated equal to true shall set dot11RSNAProtectedManagementFramesActivated to true and dot11RSNAUnprotectedManagementFramesAllowed to false. (#2314, #2315, #2588, #2589)

**…**

* Construction of the IPN by a WUR non-AP STA (CID 2315, 2588, 2589, 2314)

***TGba editor: Modify the last paragraph as the following (Track Changes ON):***

When the most recently received WUR Operation element has the Common IPN subfield equal to 0, the BPN may be updated explicitly through a secure WUR Mode Setup request/response exchange as described in 30.9.3.3 (WUR BPN Update procedure). (#2314, #2315, #2588, #2589) (#338, #903, #904, #1250)

* Frame formats (CID 2589, 2314)

*TGba editor: Insert the following new clause after 9.4.2.293 (WUR Discovery element):*

9.4.2.294 WUR Protection element

The WUR Protection element is used to update the BPN maintained by a WUR non-AP STA. The format of the WUR Protection element is shown in Figure 9-xxx (WUR Protection element format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | Key Info  | BPN |
| Octets: | 1 | 1 | 1 | 1 | 0 or 5 |
| Figure 9-xxx - WUR Protection element format |

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Key Info field is 1 octets and is illustrated in Figure 9-xxx (Key ID field).

|  |  |  |  |
| --- | --- | --- | --- |
|  | B0 B3 | B4 | B5 B7 |
|  | Key ID | BPN Present | Reserved |
| Bits: | 4 | 1 | 3 |
|  | Figure 9-xxx Key Info field format |

The Key ID subfield contains the Key ID corresponding to the WUR TK or WUR IGTK.

The BPN Present subfield is set to 1 if the BPN field is present in the WUR Protection element and is set to 0 otherwise.

The BPN field in the WUR Protection element is present if the BPN Present subfield is set to 1. Otherwise, it is not present.

The BPN field is 5 octets and is illustrated in Figure 9-xxx (BPN field).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | B0 B7 | B8 B15 | B16 B23 | B24 B31 | B32 B39 |
|  | PN1 | PN2 | PN3 | PN4 | PN5 |
| Bits: | 8 | 8 | 8 | 8 | 8 |
|  | Figure 9-xxx BPN field format |

The BPN field contain the portion of the IPN corresponding to the BPN i.e. PN1||PN2||PN3||PN4||PN5 for the integrity key indicated by the Key ID subfield in the Key Info field.

* WUR Mode Setup frame format

***TGba editor: Modify Table 9-524b as the following (Track Changes ON):***

|  |
| --- |
| * WUR Mode Setup frame Action field format
 |
| Order | Information |
| 1 | Category |
| 2 | WUR Action |
| 3 | Dialog Token |
| 4 | WUR Mode element (see 9.4.2.292 (WUR Mode element)) |
| 5 | WUR Operation element (optional) (see 9.4.2.291 (WUR Operation element)) |
| 6 | WUR Protection (optional) (see 9.4.2.294 (WUR Protection element)) |

***TGba editor: Insert the following sentence at the end of the subclause:***

The WUR Protection field contains one or more WUR Protection elements as defined in 9.4.2.294 (WUR Protection element). (#2589, #2314)

***TGba editor: Insert the following new subclause after 30.9.3.2 (Construction of the IPN by a WUR non-AP STA):***

30.9.3.3 WUR BPN Update procedure (CID 2315, 2588, 2589, 2314)

The WUR BPN Update procedure enables a WUR AP and a WUR non-AP with WUR frame protection negotiated with the WUR AP to update the locally stored BPN at the WUR non-AP STA.

When the most recently transmitted WUR Operation element has the Common IPN subfield equal to 0, a WUR AP may indicate the portion of the IPN corresponding to the BPN (i.e. PN1||PN2||PN3||PN4||PN5) maintained by the WUR AP to the WUR non-AP by including one or more WUR Protection elements in the WUR Mode Setup frame with the Action Type in WUR Mode element set to “Enter WUR Mode Response”.

When the most recently received WUR Operation element has the Common IPN subfield equal to 0, the WUR non-AP STA that receives a WUR Mode Setup frame that include a WUR Protection element shall update the locally stored BPN value corresponding to the Key ID indicated in the Key Info field to the received BPN value.

The WUR non-AP STA may request a BPN update by sending a WUR Mode Setup frame with Action Type field of the carrying WUR Mode element set to “Enter WUR Mode Request” and includes a WUR Protection element that indicates a Key ID corresponding to a integrity key currently used by the WUR non-AP STA and optionally includes the corresponding locally stored BPN.

When the most recently transmitted WUR Operation element has the Common IPN subfield equal to 0, a WUR AP that receives a WUR Mode Setup frame with Action Type field of the carrying WUR Mode element set to “Enter WUR Mode Request” and that includes a WUR Protection element shall respond with a WUR Mode Setup frame with Action Type field of the carrying WUR Mode element set to “Enter WUR Mode Response” and includes a WUR Protection element indicating the portion of the IPN corresponding to the BPN (i.e. PN1||PN2||PN3||PN4||PN5) maintained by the WUR AP corresponding to the requested Key ID. All optional sub-fields of the WUR Parameters field in the WUR Mode element may be omitted.

* (CID 2589, 2314)

Protocol Implementation Conformance Statement (PICS) -proforma

* Wake-up Radio (WUR) features

*TGba editor: Change Table B.4.36.1 as follows (Track Change ON):*

|  |
| --- |
| * WUR MAC features
 |
| Item | Protocol capability | References | Status | Support |
|  | Are the following MAC protocol features supported? |  |  |  |
| **…** |  |  |  |  |
| WURM10 | Protected WUR frames | 30.9 (Protected WUR frames) | CFWUR:O | Yes  No  N/A  |
| WURM10.1 | WUR BPN Update procedure | 30.9.3.3 (WUR BPN Update procedure),9.4.2.294 (WUR Protection element) | (CFWUR AND WURM10):O | Yes  No  N/A  |