IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolutions for D4.0 Protected WUR Frames CIDs |
| Date: 2019-10-29 |
| 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 3.0).

* CIDs: 4067, 4095 (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 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 | Clause  | Page | Line | Comment | Proposed Change | Resolution |
| 4067 | Michael Montemurro | 29.1 | 122 | 61 | The normative statement at the cited location does not provide a valid requirement. | Change "WUR frame protection shall be considered as successfully negotiated" to "WUR frame protection negotiiation shall be successfully completed" | **Revised.**Agree with the commenter that the cited sentence can be rewritten without normative requirements. The cited sentence is re-worded similar to management frame protection (REVmd\_D3.0\_P2629L49). TGba editor to make the changes shown in 11-19/1799r0 under all headings that include CID 4067. |
| 4095 | Rojan Chitrakar | 29.10.1 | 124 | 28 | If TSF based protection is used (i.e. common PN subfield is equal to 1) to protect different WUR wake-up frames (either FL or VL group addressed) in different subchannels of a WUR FDMA PPDU, it is likely that the same TSF value will be used as IPN to protect all the WUR wake-up frames. Since the reuse of a PN with the same temporal key voids the security guarantees, such cases should be disallowed. | Add text to disallow the transmissions of multiple protected FL or VL group addressed WUR wake-up frames within the same WUR FDMA PPDU when the common PN subfield is equal to 1. | **Revised.**Agree with the commenter that the same IPN should not be used with the same Key (WIGTK) more than once. As such different FL or VL group addressed WUR Wake-up frames in different sub-channels of a WUR FDMA PPDU are not allowed to use the same TSF value as WIPN. TGba editor to make the changes shown in 11-19/1799r0 under all headings that include CID 4095. |

**Discussion:** None

**Propose:**

Revised for CIDs 4067, 4095 as per discussion and editing instructions in 11-19/1799r0.

* Protected WUR frames (CIDs 4067)

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

***…***

WUR frame protection is considered as successfully negotiated between the WUR AP and the WUR non-AP STA if management frame protection is negotiated, both parties set the Protected WUR Frame Support subfield to 1 in their respective RSNXEs in the (re)association procedure, and it is successfully verified that the WUR Frame Protection Support subfield is equal to 1 in the Extended RSN Capabilities field in the RSNXE received during the 4-way handshake, FT 4-way handshake, FT fast BSS transition protocol, or (re)association procedure of FILS authentication. Otherwise, WUR frame protection is not considered as successfully negotiated.

* Protected WUR frame transmission (CIDs 4095)

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

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 29.10 (Protected WUR frames)), Key ID that is equal to the corresponding WIGTK or WTK Key ID value, a WUR PN that is generated and partially included in the WUR frame as defined in 29.10.3.1 (Generation of the PN by a WUR AP). If the Miscellaneous subfield is present in the protected WUR Wake-up frame, the Key ID subfield is set to the value representing the corresponding WIGTK (see 9.10.3.2 (WUR Wake-up frame format)).(#3262, #3187)
* Construct the AAD as defined in Figure 29-2 (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.
* Transmit the protected WUR frame.

A WUR AP that sends a protected group addressed VL WUR Wake-up frame should include WUR ID(s) of the WUR non-AP STA(s) that have already been provided with the WIGTK used to protect the group addressed VL WUR Wake-up frame and should not include WUR ID(s) of the WUR non-AP STA(s) that have not been provided with the WIGTK used to protect the group addressed VL WUR Wake-up frame.

If the most recently transmitted WUR Operation element has the Common PN subfield equal to 1, in order not to reuse the same WIPN for protection of group-addressed or broadcast-addressed WUR frames with the same WIGTK, a WUR AP shall not transmit more than one protected group addressed or broadcast WUR frames that have different contents in a WUR FDMA PPDU.

NOTE - Since the reuse of a PN with the same temporal key voids the security guarantees, such cases need to be avoided. However, repeating the same protected group-addressed or broadcast-addressed WUR frames in a WUR FDMA PPDU does not void the security guarantees, and therefore, is allowed.