IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB270 SEC Adhoc Comment Resolutions Part 1 | | | | |
| Date: 2022-12-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |

Background

This contribution proposes comment resolutions to selected REVme SEC adhoc comments from LB270.

R0 – Initial version.

R1 – Updated based on TG review on Nov 28 teleconference

R2 – Updated based on TG discussion on Dec 6 at TGme adhoc

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3129 | 2785.00 | 12.2.7 |  |  | "Robust Action frame" term is defined to include both Action and Action No Ack frames, so the first paragraph here defining which frames are robust Management frames is fine without Action No Ack frames being called out separately. However, the "Action frames with" in the following paragraph (L8) does not include Action No Ack frame. While the current text is technically correct, it is incomplete by not saying anything about Action No Ack frames not being robust Management frames under the specied conditions in Table 9-79. | At P2785 L8, replace "Action frames specified" with "Action and Action No Ack frames specified". |

### Discussion:

* The location of the cited phrases is here:

Text

Description automatically generated

* The commenter is correct to point out that the statement is silent on “Action No Ack” frames. It would be better if they were explicitly included.
* For instance, HE Compressed Beamforming/CQI is an Action No Ack frame.

### Proposed Resolution: (3129)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3244 | 2909.00 | 12.7.3 |  |  | Table 12-11--Integrity and key wrap algorithms -- doesn't specify units for Size of MIC | At 2909.5 change "Size of MIC" to "Size of MIC (octets)" |

### Discussion:

* The cited text is:

Table

Description automatically generated

* The commenter is correct in pointing out that the size of the MIC is in octets.

### Proposed Resolution: (3244)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3194 | 2925.00 | 12.7.7.4 |  |  | "The Supplicant shall not install a GTK, an IGTK(11ba), a BIGTK or a WIGTK when the key to be set matches either of these two keys (see 6.3.19 (SetKeys)). " -- that's 4 keys | Change to "The Supplicant shall not install a GTK, an IGTK(11ba), a BIGTK or a WIGTK when the key to be set matches any of these keys (see 6.3.19 (SetKeys)). " |

### Discussion:

* The cited text in context is:

Text

Description automatically generated with low confidence

* The commenter is correct to point out that the cited text is not correct. The recommendation is that the Supplicant not install a key if the key received matches the currently installed key.

### Proposed Resolution: (3194)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3130 | 2785.00 | 12.2.8 |  |  | "In an RSNA enabled BSS .. an AP should" feels a bit confusing since there can be only a single AP in the BSS. | At P2785 L32, replace "an AP should" with "the AP should". |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* The cited text is the second sentence of the second paragraph. The commenter points out correctly that the AP is operating the BSS, so it should be “the AP”

### Proposed Resolution: (3130)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3124 | 2781.00 | 12.2.4 |  |  | Step (a) (5) establish one or more temporal keys (which will in practice be at least two to cover both the pairwise and group cases), but step (a) (6) programs only a singular temporal key. That needs to be plural "keys" to cover all cases. Similar comment applies for (b) (5) and (c) (4), but (g) (4) is already using plural "keys". | At P2781 L32, replace "established temporal key" with "established temporal keys". At P2782 L5, replace "established temporal key" with "established temporal keys". At P2782 L44, replace "established temporal key" with "established temporal keys". |

### Discussion:

* The cited text in context is:

Text, letter

Description automatically generated

* And

Text

Description automatically generated

* AndText

  Description automatically generated
* In all three cited case, “temporal key” should be “temporal keys.

### Proposed Resolution: (3124)

REVISED.

At P2781 L32, replace "established temporal key" with "established

temporal key(s)".

At P2782 L5, replace "established temporal key" with "established

temporal key(s)".

At P2782 L44, replace "established temporal key" with "established

temporal key(s)".

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3123 | 2782.00 | 12.2.4 |  |  | PSK and SAE can be used with FT, so the step (b) (4) here needs to include FT similarly to the 802.1X case in step (a) (5). | At P2782 L2, replace "using the protocol defined by 12.7 (Keys and key distribution)" with "using the protocol defined by 12.7 (Keys and key distribution) or 13 (Fast BSS transition)". |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* Note that for a), the 802.1X and FILS case, the parallel item includes FT:



* The commenter is correct and the proposed resolution looks correct.

### Proposed Resolution: (3123)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3122 | 2781.00 | 12.2.4 |  |  | RSNA with 802.1X can use the FT protocol over-the-air and as such, FT authentication, in addition to the Open System and FILS authentication listed here. FT is covered in step (a) (5), so it should be covered here in (a) (2) as well. | At P2781 L20, replace "invoke Open System or FILS authentication" with "invoke Open System, FT, or FILS authentication". |

### Discussion:

* The cited text in context is:

Text, letter

Description automatically generated

* Agree with the commenter that FT is missing from a) 2)
* ACTION. Mark R to post to the reflector and schedule for Tuesday AM1 on Dec 6 to revisit this CID.

### Proposed Resolution: (3122)

REVISED. Make the changes proposed by the commentor and

at 2781.25, change

“… or uses FILS authentication to authenticate as described in 12.11 (Authentication for FILS).”

to

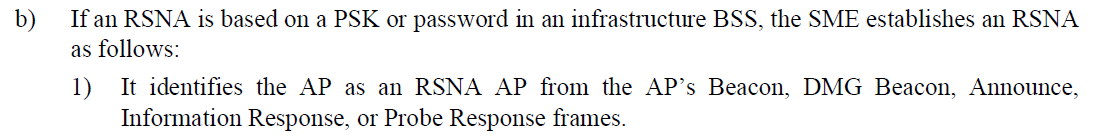
“… FT protocol to authenticate as described in 13.5 (FT protocol) or uses FILS authentication to authenticate as described in 12.11 (Authentication for FILS).”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3121 | 2781.00 | 12.2.4 |  |  | An AP might be identified as an RSNA AP based on its FILS Discovery frame as well, so the list here is not complete. | At P2781 L18, replace "Beacon, DMG Beacon, Announce, Information Response, or Probe Response frames." with "Beacon, DMG Beacon, Announce, Information Response, FILS Discovery, or Probe Response frames." |

### Discussion:

* The cited text in context is:



* Agree with the commenter that an AP can be identified as an RSNA AP based on a FILS Discovery frame. It makes sense to add FILS Discovery to the list of frames.

### Proposed Resolution: (3121)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3120 | 2784.00 | 12.2.5 |  |  | "In the case of PSK" does not feel correct in item (b) which discusses the case of IEEE 802.1X authentication and the repeated "the selected AP" for each of the listed cases looks odd as well. Since this item (b) includes IBSS, I'd guess this particular sentence was supposed to cover the IBSS (instead of PSK) case where the AS is connected with each STA (instead of AP). | At P2784 L14, replace "The STA shares authentication credentials with the AS utilized by the selected AP or, in the case of PSK, the selected AP" with "The STA shares authentication credentials with the AS utilized by the selected AP or, in the case of IBSS, the selected STA". |

### Discussion:

* The cited text in the “RSNA assumptions and constraints” clause, in context is:

Text, letter

Description automatically generated

* For the cited text, in an ESS, the STA shares credentials with the AS used by the selected AP, but in the case of PSK, the text is correct in that the STA shares credentials with the selected AP.
* Agree with the commenter that the IBSS case is missing. Therefore it would be better to modify the cited sentence to refer to an ESS and add a separate sentence to refer to an IBSS.

### Proposed Resolution: (3120)

REVISED. At 2784.14, replace

“The STA shares authentication credentials with the AS utilized by the selected

AP or, in the case of PSK, the selected AP.”

with  
“In an ESS, the STA shares authentication credentials with the AS utilized by the selected

AP or, in the case of PSK, the selected AP.”

At 2784.19, Insert the following paragraph “In an IBSS, the STA shares authentication credentials with the selected STA.”

At 2784.13, Remove “or IBSS”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3119 | 2784.00 | 12.2.5 |  |  | "PSK authentication" does not seem to be in the scope of the item (b) which discussed the case of IEEE 802.1X authentication. | At P2784 L17, replace "the successful completion of the IEEE 802.1X EAP or PSK authentication" with "the successful completion of the IEEE 802.1X EAP authentication" |

### Discussion:

* The cited text in context is:

Text, letter

Description automatically generated

* The first paragraph of the item refers to EAP authentication and IEEE 802.1X. The second paragraph seems to deal with mutual authentication for both ESS and IBSS. It seems as if there should be a new paragraph starting with the sentence beginning with “The SSID provides an …”

### Proposed Resolution: (3119)

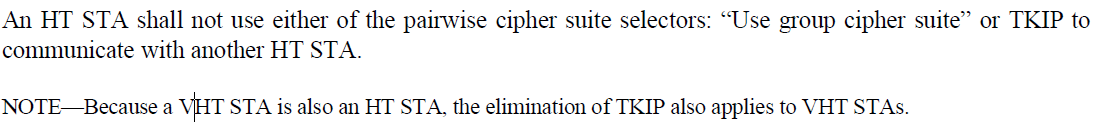
REVISED. Add a paragraph break at 2784.15 before the sentence starting with “The SSID provides an...”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3118 | 2784.00 | 12.2.5 |  |  | Elimination of TKIP is defined here for HT STAs and a note here explains why that applies to VHT STAs as well. However, HE STAs are not mentioned here at all. Since an HE STA is also a VHT STA when operating in 5 GHz or an HT STA when operating in 2.4 GHz (see 4.3.16), the same TKIP elimination applies for those bands. 12.12.2 constraints cover the 6 GHz case separately, so it would seem to be appropriate to add a note here to cover the general TKIP elimination case for HE STAs. | At P2784 L53, add the following note after the existing note covering VHT STAs: "NOTE--Because an HE STA is also an HT STA when operating in the 2.4 GHz band and a VHT STA when operating in the 5 GHz band, and because the security constraints in the 6 GHz band (see 12.12.2) disallow use of TKIP, the elimination of TKIP also applies to HE STAs." |

### Discussion:

* The cited text in context is:



* Agree with the commenter that it would be good to add a note here to clarify the general TKIP elimination case for HE STAs.

### Proposed Resolution: (3118)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3193 | 2925.00 | 12.7.7.5 |  |  | "uses the MLME-SETKEYS.request primitive to configure the GTK, PN, IGTK, RSC, IPN, BIGTK and BIPN in its STA." seems garbled. The GTK is associated with an RSC not a PN; the IPN is associated with the IGTK | Change to "uses the MLME-SETKEYS.request primitive to configure the GTK, GTK RSC, IGTK, IGTK RSC, BIGTK and BIGTK RSC in its STA." |

### Discussion:

* The cited text in context is:

Text, timeline

Description automatically generated with medium confidence

* In the cited text, PN and RSC describe the same counter.

### Proposed Resolution: (3193)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3446 |  | 12 |  |  | "using an AEAD cipher" needs to be clarified -- exactly which ciphers are AEAD ciphers? | At 2900.63 add a para "NOTE---AES-SIV is an AEAD cipher." |

### Discussion:

* The cited text in context in the Key Information description of the EAPOL-key frame is:

Text

Description automatically generated

* AEAD in this context is describing a mechanism defined as part of FILS and is described in 12.11.2.7.

### Proposed Resolution: (3446)

REVISED. Add the following at 2900.63:

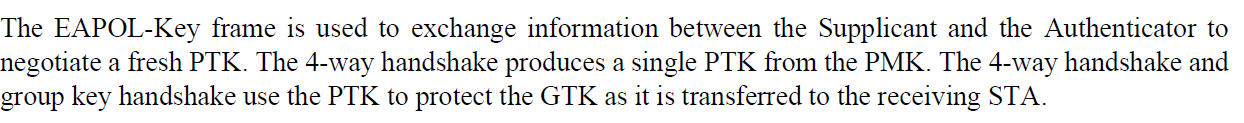
“NOTE—AEAD cipher mode is described in 12.11.2.7.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3490 | 2875.00 | 12.6.11 |  |  | "The EAPOL-Key frame is used to exchange information between the Supplicant and the Authenticator" should be "EAPOL-Key PDUs are used to exchange information between the Supplicant and the Authenticator" | As it says in the comment |

### Discussion:

* The cited text in context in the Key Information description of the EAPOL-key frame is:



* Agree with the comment that “frame” should be “PDU”

### Proposed Resolution: (3490)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3443 | 313.00 | 4.5.4.4 |  |  | "ARC4 license terms that RSA offers to anyone wishing to use ARC4 for the purpose of implementing the IEEE 802.11 TKIP option" -- isn't it out of patent? | Delete the footnote |

### Discussion:

* This is the cited text that is tied to the footnote:

A picture containing text

Description automatically generated

* Agree with the comment that the note is no longer needed.

### Proposed Resolution: (3443)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3442 | 313.00 | 4.5.4.4 |  |  | "IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including TKIP, CCMP, and GCMP." -- what about BIP/GMAC/CMAC? | After the cited text add "IEEE Std 802.11 provides several cryptographic algorithms to protect management traffic, including BIP-CMAC and BIP-GMAC." |

### Discussion:

* This is the cited text in context:

A picture containing text

Description automatically generated

* Agree with the comment that it would be useful to add BIP.

### Proposed Resolution: (3442)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3434 | 2913.00 | 12.7.6.2 |  |  | "after (re)association completes for a STA that has authenticated with SAE or PSK authentication is negotiated" is confusing | Change to "after (re)association completes for a STA that has authenticated with SAE or for which PSK authentication is negotiated" |

### Discussion:

* This is the cited text in context:

Text

Description automatically generated

* Agree with the comment that just changes “SAE or PSK” to “SAE or for which PSK”

### Proposed Resolution: (3434)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3341 | 2877.00 | 12.6.15 |  |  | "A STA joining an IBSS is required to" -- should be a shall | At 2877.30 change "A STA joining an IBSS is required to adopt the security configuration of the IBSS" to "A STA joining an IBSS shall adopt the security configuration of the IBSS" |

### Discussion:

* This is the cited text in context:

Text

Description automatically generated with low confidence

* The normative (“shall”) requirements for STA security configuration when joining an IBSS are described in 12.6.5, which is given as a cross-reference in the cited sentence. Therefore there is no need to change “is required to” to “shall”

### Proposed Resolution: (3341)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3759 | 2974.00 | 13.5.2 |  |  | It should be authentication request rather than FT request for the following paragraphs "If the FTE in the FT Request frame contains an invalid R0KH-ID, the AP shall reject the FT Request frame with status code STATUS\_INVALID\_FTE." | Over-the-air FT protocol in an RSN does not use FT request. Over-the-air FT protocol in an RSN uses authentication request. Change the sentence correspondingly. |

### Discussion:

* This is the cited text in context:

Text, letter

Description automatically generated

* Given this is the FT OTA clause, agree with the comment that FT Request should be Authentication-Request

### Proposed Resolution: (3759)

REVISED. In the cited sentence beginning on 2974.57, change “FT Request” to “Authentication-Request” (2 locations).

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3253 | 2891.00 | 12.7.1.4 |  |  | What is the empty box at the bottom right of Figure 12-31--Group key hierarchy about? | Delete bottom right box and expand bottom left box to cover where it used to be |

### Discussion:

* This is the cited text that is tied to the footnote:

Graphical user interface, text, application

Description automatically generatedText

Description automatically generated with medium confidenceDiagram

Description automatically generated

* This is the cited text and note that the figure has not changed since it was published in the IEEE 802.11i amendment.
* The figure is consistent with the Pairwise Key Hierarchy in 12.7.1,3
* As the formula shows that the TK is a truncated value of the GTK.
* The figure reflects the relationship between the GMK-GTK-TK. The TK is a selection of bits from the GTK.
* ACTION: Mark R to post to reflector. Revisit the comment during AM1 on Dec 6 (during adhoc)

### Proposed Resolution: (3253)

REVISED.

Modify Figure 12-31 as follows:

Delete the two lower boxes

Change the Group Temporal Key box, changing “Length bits” to “TK\_bits bits”

Change “PRF-Length…” to “PRF-TK\_bits…”

On p2891.36 in item b) below the figure, change “PRF-Length…” to “PRF-TK\_bits…”

In item c) delete “Length = TK\_bits.”

Delete item d)

In item e) change “temporal key” to “GTK”

Note to Editor: Mark Rison to provide updated figure 12-31.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3231 | 2843.00 | 12.5.2.4.1 |  |  | "When the received frame is a CCMP protected individually addressed robust Management frame or PV1 Management frame, contents of the MMPDU body after protection is removed shall be delivered to the SME via the MLME primitive designated for that MMPDU or PV1 Management frame rather than through the MA-UNITDATA.indication primitive." -- PV1 Management frames are Management frames. Also missing article | Change to "When the received frame is a CCMP protected individually addressed robust Management frame, the contents of the MMPDU body after protection is removed shall be delivered to the SME via the MLME primitive designated for that MMPDU rather than through the MA-UNITDATA.indication primitive." |

### Discussion:

* This is the cited text in context:

A picture containing text

Description automatically generated

* Agree with the comment.
* Proposed updated text:

"When the received frame is a CCMP protected individually addressed robust Management frame, the contents of the MMPDU body after protection is removed shall be delivered to the SME via the MLME primitive designated for that MMPDU rather than through the MA-UNITDATA.indication primitive."

### Proposed Resolution: (3231)

ACCEPTED