IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB270 SEC Adhoc Comment Resolutions Part 2 | | | | |
| Date: 2022-12-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |
| Dan Harkins | HPE |  |  |  |

Background

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

R0 – Initial version.

R1 –

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3469 |  | 12 |  |  | We refer to 802.1X-2010 but there's an 802.1X-2020 | Update references to be to the current standard |

### Discussion:

* There are 40 occurrences of 802.1X-2010 in the draft. After review, all occurrences could be replaced without affecting the context of their usage.
* There are no changes to 802.1X in IEEE Std 802.1X-2020 that would affect IEEE 802.11.

### Proposed Resolution: (3469)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3468 | 2899.00 | 12.7.2 |  |  | It is not clear whether the Packet Body Length field in EAPOL-Key frames can indicate that there are some octets after the packet body | Say "The Packet Body Length field is specified in IEEE Std 802.1X. This field may indicate the presence of octets beyond the end of the Key Data field, and may imply the presence of octets after the EAPOL PDU." |
| 3467 | 2899.00 | 12.7.2 |  |  | It is not clear whether the Packet Body Length field in EAPOL-Key frames can indicate an EAPOL PDU size that extends beyond the end of the Key Data field (but still within the packet body) | At 2899.65 add a para "The Packet Body Length field is specified in IEEE Std 802.1X. This field may indicate the presence of octets beyond the end of the Key Data field, and may imply the presence of octets after the EAPOL PDU." |

### Discussion:

* Two comments with the same proposed resolution:
* The text the comment is referencing is the following:

Text

Description automatically generated with medium confidence

* The comment proposes adding this text after the figure:

“The Packet Body Length field is specified in IEEE Std 802.1X. This field may indicate the presence of octets beyond the end of the Key Data field, and may imply the presence of octets after the EAPOL PDU”

* The Packet Body Length field is clearly defined in IEEE Std 802.1X as “This two octet field encodes an unsigned binary number that defines the length in octets of the Packet Body field.”
* Furthermore in the requirements for receiving an EAPOL PDU, IEEE Std 802.1X states: “The Packet Body Length denotes a Packet Body that is contained within the octets of the received EAPOL MPDU.

Otherwise the received EAPOL PDU shall be discarded.

Any octets following the Packet Body field in the frame conveying the EAPOL PDU shall be ignored.”

* These requirements are clearly specified in IEEE Std 802.1X and do not need to be updated in this draft.
* However the description of the EAPOL-Key frame could be improved by moving the paragraph at 2899.36 to the end of paragraph starting at 2899.38. The editing instructions would be:

Delete the paragraph at 2899.36.

At the end of the paragraph starting at 2899.38, append the following sentences. “The Protocol Version, Packet Type, and Packet Body Length are specified in clause 11.3 of IEEE Std 802.1X. The IEEE 802.11 Key Descriptor maps to the IEEE 802.1X Descriptor as described in this subclause.”

At 2900.4, change “IEEE 802.11 Key Descriptor” to “IEEE 802.11 Key Descriptor Type”

### Proposed Resolution: (3467, 3468)

REVISED. Clarify the mapping of IEEE 802.1X fields in the IEEE 802.11 EAPOL-Key frame, including the Packet Body Length.

Delete the paragraph at 2899.36.

At the end of the paragraph starting at 2899.38, append the following sentences. “The Protocol Version, Packet Type, and Packet Body Length are specified in clause 11.3 of IEEE Std 802.1X. The IEEE 802.11 Key Descriptor maps to the IEEE 802.1X Descriptor as described in this subclause.”

At 2900.4, change “IEEE 802.11 Key Descriptor” to “IEEE 802.11 Key Descriptor Type”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3394 | 2934.00 | 12.7.9.4 |  |  | "StaProcessEAPOL-Key (S, M, A, I, K, RSC, ANonce, RSC" -- it is confusing to have RSC twice and only differing by italicisation. Based on 12.7.4 it actually looks as if the second RSC is bogus | Delete the second ", RSC". Italicise RSC at 2934.60, 2935.7 |

### Discussion:

* The cited text in context is:

A picture containing text

Description automatically generated

* Agree with the commenter that the second RSC is incorrect and it should be italicized in the pseudo code.

### Proposed Resolution: (3394)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3812 | 2850.00 | 12.5.4.3.1 |  |  | "NOTE--Retransmitted MPDUs are not modified on retransmission." The MPDU includes the MAC header and the Retry subfield in the Frame Control field in the MAC header is modified during the retransmission. This NOTE is wrong. | Change to "NOTE 1--The frame body of the reetransmitted MPDU is not modified on retransmission." |

### Discussion:

* The cited text in context is:

Text

Description automatically generated with low confidence

* The comment proposes changing the note text to “The frame body of the retransmitted MPDU is not modified on retransmission.”
* Agree with the commenter but there is a typo and NOTE-1 should be NOTE

### Proposed Resolution: (3812)

ACCEPTED

Note to Editor. The changed text with typos corrected is: “NOTE—The frame body of the retransmitted MPDU is not modified on retransmission.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3811 | 2836.00 | 12.5.2.3.1 |  |  | "NOTE 1--Retransmitted MPDUs are not modified on retransmission." The MPDU includes the MAC header and the Retry subfield in the Frame Control field in the MAC header is modified during the retransmission. This NOTE is wrong. | Change to "NOTE 1--The frame body of the reetransmitted MPDU is not modified on retransmission." |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* The comment proposes changing the note text to “The frame body of the retransmitted MPDU is not modified on retransmission.”
* Agree with the commenter but there is a typo.

### Proposed Resolution: (3811)

ACCEPTED

Note to Editor. The changed text with typos corrected is: “NOTE 1 —The frame body of the retransmitted MPDU is not modified on retransmission.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3131 | 250.00 | 3.4 |  |  | PWE is used both with ECC (see 12.4.4.2.2 P2812 L35) and FFC (see12.4.4.3.2 P2817 L56) groups, so it should not be defined with a constraint of "an ECC group". | At P250 L51, replace "password element of an ECC group" with "password element". |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* For generating the PWE with ECC:

Text

Description automatically generated

* For generating the PWE with FCC

Text

Description automatically generated

* Both ECC and FCC are finite cyclic groups so it would be better to change the acronym definition to address both cases.

### Proposed Resolution: (3131)

REVISED. At P250.51, replace “password element of an ECC group” with “password element of a finite cyclic group”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3133 | 2963.00 | 12.12 |  |  | 12.12 was added as a generic location for covering various security constraints. While this was added as a part of P802.11ax, the design and intent of the subclause was such that it could be used as a placeholder for collecting all similar requirements from the full standard into a single location instead of maintaining them in various locations (e.g., see 5.1.2 and the end of 12.2.5). This would make it easier for the reader to find the required constraints preventing use of various obsole and deprecated mechanisms. | Delete P343 L50-59 (at the end of 5.1.2).  At P2963 L62, add the following subclauses:  12.12.3 Security constraints for HT STAs  An HT STA shall not use either of the pairwise cipher suite selectors: "Use group cipher suite" or TKIP to communicate with another HT STA.  12.12.4 Security constraints for VHT STAs  A VHT STA shall not use either of the pairwise cipher suite selectors: "Use group cipher suite" or TKIP to communicate with another HT STA or VHT STA.  12.12.5 Security constraints for HE STAs  An HE STA shall not use either of the pairwise cipher suite selectors: "Use group cipher suite" or TKIP to communicate with another HT STA, VHT STA, or HE STA.  12.12.6 Security constraints for S1G STAs  An S1G STA shall not use the pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or "Use group cipher suite".  12.12.7 Security constraints for mesh STAs  A mesh STA shall not use the pairwise cipher suite selectors WEP-40, WEP-104, or TKIP.  12.12.8 Security constraints for STAs that support nanagement frame protection  A STA that has associated with management frame protection enabled shall not use pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or "Use group cipher suite." |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* Agree with the commenter that it would make sense to include the constraints in one place.

***Delete P343 L50-59 (at the end of 5.1.2).***

~~A STA that has associated with management frame protection enabled shall not use pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or “Use group cipher suite.”~~

~~A mesh STA with dot11MeshSecurityActivated equal to true shall not use the pairwise cipher suite selectors WEP-40, WEP-104, or TKIP.~~

~~An S1G STA shall not use the pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or “Use group cipher suite”.~~

***At P2963 L62, add the following subclauses:***

**12.12.3 Security constraints for HT STAs**

An HT STA shall not use either of the pairwise cipher suite selectors "Use group cipher suite" or TKIP to communicate with another HT STA.

**12.12.4 Security constraints for VHT STAs**

A VHT STA shall not use either of the pairwise cipher suite selectors:

"Use group cipher suite" or TKIP to communicate with another HT STA or

VHT STA.

**12.12.5 Security constraints for HE STAs**

An HE STA shall not use either of the pairwise cipher suite selectors:

"Use group cipher suite" or TKIP to communicate with another HT STA, VHT

STA, or HE STA.

**12.12.6 Security constraints for S1G STAs**

An S1G STA shall not use the pairwise cipher suite selectors WEP-40,

WEP-104, TKIP, or "Use group cipher suite".

**12.12.7 Security constraints for mesh STAs**

A mesh STA shall not use the pairwise cipher suite selectors WEP-40,

WEP-104, or TKIP.

**12.12.8 Security constraints for STAs that support management frame**

**protection**

A STA that has associated with management

frame protection enabled shall not use pairwise cipher suite selectors

WEP-40, WEP-104, TKIP, or "Use group cipher suite."

### Proposed Resolution: (3133)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3199 | 2880.00 | 12.6.20 |  |  | "the protected variant is used when management frame protection has been negotiated" -- needs to be "a non-protected variant shall be discarded when management frame protection has been negotiated" | As it says in the comment |

### Discussion:

* The cited text in context is:

Text

Description automatically generated with medium confidence

* The third sentence of the paragraph begins with “When an action frame is transmitted for which ….” and describes behavior in terms of the transmitter and relates to the “Protected” parameter in the MLME. As such the cited sentence “Where there is no such parameter, the protected variant ….” is correct.

### Proposed Resolution: (3199)

REJECTED. The cited paragraph describes requirements for behaviour associated with the transmission of Protected Dual of Public action frames. The cited text is correct and consistent with the other text in the paragraph.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3228 | 2871.00 | 12.6.10.1 |  |  | "SAE authentication is initiated when a STA's MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member that advertises support for SAE in its RSNE." -- not necessarily (maybe the AP also supports PSK) and the STA is not necessarily in an ESS (initial assoc). And maybe you don't want to connect to that AP at all? Ditto other auths | Change to "SAE authentication can be initiated when a STA's MLME-SCAN.confirm primitive identifies an AP that advertises support for SAE in its RSNE." Similarly change the next 3 lines to FILS authentication can be initiated when a STA's MLME-SCAN.confirm primitive identifies an AP that advertises support for FILS authentication in its RSNE. (#1084)OWE can be initiated when a STA's MLME-SCAN.confirm primitive identifies another AP within the ESS of which the STA is a member that advertises support for OWE in its RSNE. IEEE 802.1X authentication can be initiated by any one of the following mechanisms: |

### Discussion:

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

Text

Description automatically generated

* The proposed change affects the 2nd, 3rd, 4th and the beginning of the 5th paragraph.
* The changes in general replace “is” with “can”, rewords the sentence, and removes the reference to the ESS.

### Proposed Resolution: (3228)

REVISED

At 2871.40, change

“SAE authentication is initiated when a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member that advertises support for SAE in its RSNE.”

To

“SAE authentication can be initiated when a STA's MLME-SCAN.confirm primitive identifies an AP that advertises support for SAE in its RSNE.”

At 2871.44, change

“FILS authentication is initiated when a STA’s MLME-SCAN.confirm primitive finds an AP that advertises support for FILS authentication in its RSNE.”

To

“FILS authentication can be initiated when a STA's MLME-SCAN.confirm primitive identifies an AP that advertises support for FILS in its RSNE.”

At 2871.48 change

“OWE is initiated when a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member that advertises support for OWE in its RSNE.”

To

“OWE authentication can be initiated when a STA's MLME-SCAN.confirm primitive identifies an AP that advertises support for OWE in its RSNE.”

At 2871.51, change

“IEEE 802.1X authentication is initiated by any one of the following mechanisms:”

To

“IEEE 802.1X authentication can be initiated by any one of the following mechanisms:”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3230 | 2780.00 | 12.2.1 |  |  | "12.2.1 Classes of security algorithm This standard defines two classes of security algorithms for IEEE 802.11 networks: -- Algorithms for creating and using an RSNA, called RSNA algorithms -- Pre-RSNA algorithms" -- also TSN algorithms, since non-RSNA includes pre-RSNA an TSN | Change the last bullet to "Pre-RSNA and TSN algorithms" |

### Discussion:

* The cited text in context is:

A picture containing text

Description automatically generated

* Note that TSN is defined as “**transition security network (TSN):** transition security network (TSN): A security network that allows the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs. A TSN is identified by the indication in the robust security network element (RSNE) of Beacon frames that the group cipher suite in use is wired equivalent privacy (WEP).
* TSN was added to address security for pre-RSNA STAs and APs. TSN includes the WEP algorithm which is already included in the bulleted list. Therefore since TSN is a security mechanism and not an algorithm, it does not need to be included.

### Proposed Resolution: (3230)

REJECTED. TSN is defined as a security method and makes use of the WEP algorithm. As such, it does not need to be included in the list at the cited location.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3257 |  | 12 |  |  | It is not clear what the difference between "PeerKey" (e.g. in MLME-SETKEYS.req) and "TPK" (in 12.7.8.2 TPK handshake) is. It might be that "TPK" is TDLS PeerKey as opposed to AP PeerKey, but if so, it's not clear what an unlabelled "PeerKey" means (12x in Clause 6, 3x in 9.4.2.24.4, 1x in 12.7.8.4.2, 1x in Figure 12-51, 1x in 12.10.2) | Change "PeerKey" to "AP PeerKey" at 2946.62. Change "PeerKeyInit" to "EAPOL-Key PDU" at 2932.53 |

### Discussion:

* Relative to the proposed, change the context at 2946.62:

Text

Description automatically generated

* Agree with the commenter that PeerKey should be AP PeerKey at that location.
* Relative to the proposed change, the context at 2932.53 is:

A picture containing timeline

Description automatically generated

* The proposal is to change “PeerKeyInit” to “EAPOL-Key PDU”. The text above the figure says that the Supplicant enters the STAKEYSTART state on receiving the EAPOL-Key PDU, so it would be better to say “EAPOL-Key PDU received”.

### Proposed Resolution: (3257)

REVISED. Make changes in the direction proposed by the commenter.

At 2946.62, change “PeerKey” to “AP PeerKey”.

At 2932.53, change “PeerKeyInit” to “EAPOL-Key PDU received”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3269 | 2857.00 | 12.6.1.1.6 |  |  | "There shall be only one PTKSA per key ID per band (see 12.6.19 (Protection of robust Management frames)) with the same Supplicant and Authenticator MAC addresses." -- xref seems bogus | Identify the correct xref |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* The cited text refers to multi-band RSNA. The appropriate clause would be 12.6.22 (Multi-band RSNA)

### Proposed Resolution: (3269)

REVISED. The cited text refers to multiband operation, change cross reference from 12.6.19 to 12.6.22 at cited location.

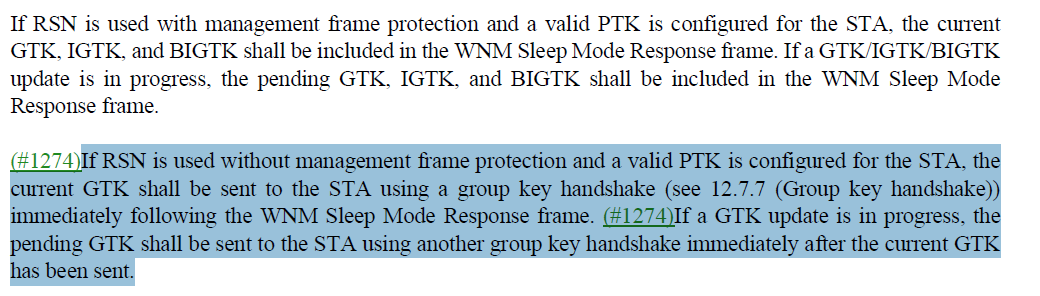
Note to Editor. Clause titles would be updated with the update in cross-reference.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3281 | 2402.00 | 12.7.7.1 |  |  | "If RSN is used without management frame protection and a valid PTK is configured for the STA, the current GTK shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame." -- can BIGTK be used without PMF? If so then BIGTK needs to be covered here | As it says in the comment |

### Discussion:

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



* The commenter is correct to point out that IGTK and BIGTK should be included.
* The updated text is shown below in the proposed resolution.

### Proposed Resolution: (3281)

REVISED. Incorporate the changes under “Proposed Resolution: (3281)” in <this> document

***Update the cited paragraph as follows:***

“If RSN is used without management frame protection and a valid PTK is configured for the STA, the current GTK, IGTK, and BIGTK shall be sent to the STA using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame. (#1274)If a GTK/IGTK/BIGTK update is in progress, the pending GTK, IGTK, and BIGTK shall be sent to the STA using another group key handshake immediately after the current GTK, IGTK, and BIGTK has been sent.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3292 | 492.00 | 6.5.14.1.4 |  |  | "identify a new key to be set" (2x) is not clear. It would be safest to say that a new key is a new Key parameter value (the odds of a PTK and a GTK or whatever having the same temporal key are vanishingly small) | At 492.20 add a "NOTE---A new key is identified by virtue of having a different Key parameter than used so far during the membership of the current BSS." |

### Discussion:

* The cited text in context is:

Text

Description automatically generated

* The commenter suggests adding a note to clarify what constitutes a “new key”
* However, not sure what's so confusing and "…so far during the membership of the current BSS" implies that the MAC is going to keep track of key parameters for a period of time. The new key is the key included in the MLME-SETKeys primitive that differs from the current key.

### Proposed Resolution: (3292)

REJECTED. The new key is the key included in the MLME-SETKeys primitive that differs from the current key.

Or

REVISED. At 492.20 add a "NOTE---A new key is identified by virtue of having a different Key parameter than used by the MAC."

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3302 |  | 12.7.6 |  |  | The Secure bit might be 1 in M1 and M2 if rekeying | At 2913.23 change "Secure = 0" to "Secure = 0 or 1 (see 12.7.2)". At 2914.15 change "Secure = 0 -- same as message 1" to "Secure = 0 or 1 (see 12.7.2)" |

### Discussion:

* The cited text (at the first location) in context is:

Graphical user interface, text, application, email

Description automatically generated

* The second location is 4-way handshake message 2.
* Agree with the commenter that in the re-keying case, the Secure bit can be set to 1.

### Proposed Resolution: (3302)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3328 | 2831.00 | 12.4.8.6.3 |  |  | "Otherwise, the frame shall be processed by first checking whether a password identifier is present. If so and there is no password associated with that identifier, BadID shall be set and the protocol instance shall construct and transmit an Authentication frame with Status Code set to UNKNOWN\_PASSWORD\_IDENTIFIER" -- should be an SAE Authentication frame, specifically? Or even an SAE Commit message? Ditto below | Change "Authentication frame" to "SAE Authentication frame" at 2831.46/51 |

### Discussion:

* This is the cited text in context:

A screenshot of a computer

Description automatically generated with medium confidence

* Agree with the comment that calling it an “SAE Authentication frame” would be better in this context.

### Proposed Resolution: (3328)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3353 | 2876.00 | 12.6.18 |  |  | CID 1851 -- also need change "In the case of an IBSS, the SME shall delete the PTKSA and the receive GTKSA and any IGTKSA." to allow for multiple PTKSAs etc. | Change to "... any PTKSA(s) ... any IGTKSA(s)" |

### Discussion:

* This is the cited text is actually on page 2878:

Text

Description automatically generated

* The comment is asking for the IBSS requirement to be modified to acknowledge multiple PTKSAs, GTKSAs, and IGTKSAs. The change would be as shown in the proposed resolution (with the correct reference).

### Proposed Resolution: (3353)

REVISED. Make the following changes at the correct location in line with the proposed changes. At 2878.27, change

“In the case of an IBSS, the SME shall delete the PTKSA and the receive GTKSA and any IGTKSA.”

to

“In the case of an IBSS, the SME shall delete the PTKSA(s) and the receive GTKSA(s) and any IGTKSA(s)."

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3685 |  | 12.6.1.1 |  |  | 12.6.1.1.8: "The GTKSA results from a successful 4-way handshake, FT 4-way handshake, FT protocol, FT resource request protocol, (11ai)group key handshake, or FILS authentication(11ai)" but 12.6.1.1.1: "GTKSA: A result of a successful group key handshake, 4-way handshake, FT 4-way handshake, (11ai)FT authentication sequence, or FILS authentication(11ai)." -- the two sets differ (" FT protocol, FT resource request protocol" v. "FT authentication sequence" | Make the two sets identical, or even better avoid the duplication in the first place by only keeping one and xreffing to it from the other |

### Discussion:

* The cited text from 12.6.1.1.8:

Text

Description automatically generated

* The cited text from 12.6.1.1.1:

Text

Description automatically generated

* The GTKSA statement in 12.6.1.1.1 is consistent with the other security associations described in the bulleted list. The list summarizes the types of security associations in 802.11.
* The description of FT protocols is different in the two lists. Note that the FT protocol and FT resource request protocol are FT authentication sequences. The description in 12.6.1.1.8 is more accurate so it would be better to align 12.6.1.1.1 with the description in 12.6.1.1.8. Update the list in 12.6.1.1.1 in Proposed Resolution

### Proposed Resolution: (3685)

REVISED. Align the two cited sentences. At 2855.34, change:

“GTKSA: A result of a successful group key handshake, 4-way handshake, FT 4-way handshake, FT authentication sequence, or FILS authentication.”

to

“GTKSA: A result of a successful group key handshake, 4-way handshake, FT 4-way handshake, FT protocol, FT resource request protocol, or FILS authentication.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3407 | 491.00 |  |  |  | If MLME-SETKEYS.req is passed the same Key, Key Type as an existing key, but a different Key ID, this is suspect (some kind of new KRACKy thing) and should probably be rejected | After the first sentence of the subclause insert the sentence "Otherwise, irrespective of the Key Type, when the Key is the same as a key installed as a result of EAPOL-Key PDUs or exiting WNM sleep mode, receipt of this primitive shall have no effect." |

### Discussion:

* This is the cited text in context:

Text, letter

Description automatically generated

* The commenter is requesting that the following sentence is inserted after the first sentence, making the first two sentences read:

“When the Key Type is Group, IGTK, BIGTK, or WIGTK(11ba), and the key matches the GTK, IGTK, BIGTK, or WIGTK(11ba), if any, installed as a result of (#1836)EAPOL-Key PDUs (see 12.7.7.4 (Group key handshake implementation considerations)) or exiting WNM sleep mode (see 11.2.3.16.1 (WNM sleep mode capability)) receipt of this primitive shall have no effect except updating the RSC(s) when they are greater than those currently stored.(#1679). Otherwise, irrespective of the Key Type, when the Key is the same as a key installed as a result of EAPOL-Key PDUs or exiting WNM sleep mode, receipt of this primitive shall have no effect. Otherwise, receipt of this primitive causes the MAC to apply the keys as follows, subject to the MLME-SETPROTECTION.request primitive:”

* The “Otherwise,” in the Proposed Change is not required.
* The current sentence seems to cover the case where the same key is received with a different Key ID.
* You could add “irrespective of the Key ID,” before “receipt of this…”

### Proposed Resolution: (3407)

REJECTED. The first sentence of the cited paragraph covers the case where the key matches the existing installed key, irrespective of the Key ID.

**or**

REVISED. At 491.59, change “receipt of this primitive” to “irrespective of the value of the Key ID parameter, receipt of this primitive”.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3465 | 2899.00 | 12.7.2 |  |  | 802.1X-20q0 says that for EAPOL-Key frames "The first two fields in the Descriptor Body [i.e. after the Descriptor Type field] comprise a Subtype and a Version", but our EAPOL-Key frames have no subtype field | At 2899.65 add a "NOTE---IEEE Std 802.1X-2020 says that for EAPOL-Key frames "The first two fields in the Descriptor Body [i.e. after the Descriptor Type field] comprise a Subtype and a Version, but the 802.11 EAPOL-Key frames have a key type instead of the subtype." |

### Discussion:

* From IEEE 802.1X-2020:

Table

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* From D2.0:

Table

Description automatically generated Graphical user interface, text, application

Description automatically generated

* First of all, it looks like in IEEE 802.1X-2020 in the context, “The first two fields in the Descriptor Body” should be “The first two fields in the Packet Body” given the statement that the Descriptor body is not constrained by the IEEE 802.1X standard.
* However, more can be done to align the two descriptions. See changes in the Proposed Resolution.

### Proposed Resolution: (3465)

REVISED. The note is not required since the Descriptor Body field is definition is not constrained by the IEEE 802.1X standard. However the mapping between the two standards can be improved as follows:

At 2899.36, replace

“The IEEE 802.11 Key Descriptor maps to the IEEE 802.1X Key Descriptor as described in this subclause.”

with

“The IEEE 802.1X Key Descriptor Type and Descriptor Body for the EAPOL-Key frame are described in this sub clause.”

At 2900.3, replace

“**Descriptor Type.** This field has a value defined by IEEE Std 802.1X-2010, identifying an

IEEE 802.11 Key Descriptor.”

with

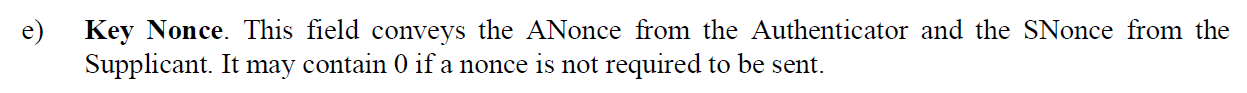
“**Descriptor Type.** This field is set to the value of IEEE 802.11 Key Descriptor Type as defined in IEEE Std 802.1X-2020.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3466 | 2902.00 | 12.7.2 |  |  | "It may contain 0 if a nonce is not required to be sent." is confusing | Change to "It shall contain 0 if a nonce is not required to be sent." |

### Discussion:

* This is the cited text in context:



* "It may be zero" is a notice to a recipient that you might get something that has a zero value. Mandating it being sent as zero is very different.

### Proposed Resolution: (3466)

REJECT: the text informs a recipient of a frame of its possible contents, it does not mandate content.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3486 | 2904.00 | 12.7.2 |  |  | It's not clear whether KDEs are extensible (e.g. can the PMKID KDE have more than 16 octets in the Data field?) | At the end of the referenced para add "Unless stated otherwise, KDEs are not extensible." |

### Discussion:

* This is the cited text in context:

Table

Description automatically generated

* Comment proposes adding an extensibility statement after sentence that introduces the table.

### Proposed Resolution: (3486)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3492 | 2905.00 | 12.7.2 |  |  | "If the value of the Tx field is 1, then the IEEE 802.1X component shall configure the temporal key derived from this KDE into (#408)the IEEE 802.11 MAC for both transmission and reception. If the value of the Tx field is 0, then the IEEE 802.1X component shall configure the temporal key derived from this KDE into (#408)the IEEE 802.11 MAC for reception only." -- 1 is not used anywhere (0 is used in 12.11.2.6.3 (Re)Association Response for FILS key confirmation) | Delete the cited text and in Figure 12-36--GTK KDE format change Tx to Reserved and in 12.11.2.6.3 delete " with Tx subfield equal to 0" (2960.51) |

### Discussion:

* This is the cited text in 12.7.2 context:

Graphical user interface, table, timeline

Description automatically generated

* The cited text in 12.11.2.6.3 is

Text

Description automatically generated with medium confidence

* The commenter is correct in pointing out that the Tx field is always set to 0 so we could remove the field and make it reserved.

### Proposed Resolution: (3492)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3497 | 2929.00 | 12.7.8.4.2 |  |  | "The FTE shall be set as follows: SNonce shall be set to a value chosen randomly by the TDLS initiator STA, see 12.7.5 (Nonce generation) for a recommended procedure. All other fields shall be set to 0." -- it is not clear what the last sentence means in terms of the optional subelements | Change to "The FTE shall be set as follows:  SNonce shall be set to a value chosen randomly by the TDLS initiator STA, see 12.7.5 (Nonce  generation) for a recommended procedure.  All other fields shall be set to 0. The Optional  Parameter(s) field shall not be present.", on the basis none of the subelements make sense for TDLS |

### Discussion:

* This is the cited text in context:

Text

Description automatically generated

* The change is proposing to append “The Optional  
  Parameter(s) field shall not be present” at the end of the last highlighted sentence.
* From 2992.39 in the FT protocol description “When this message of the authentication sequence appears in a Reassociation Response frame, the Optional Parameter(s) field in the FTE may include the GTK, IGTK, BIGTK, and WIGTK(11ba) subelements. If a GTK, an IGTK, a BIGTK, or WIGTK(11ba) are included, …”

### Proposed Resolution: (3497)

ACCEPTED

Note to Editor, at the cited location, the change is:

At 2929.31, change

“All other fields shall be set to 0.”

to

“All other fields shall be set to 0. The Optional

Parameter(s) field shall not be present."

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3551 |  | 12.6.21 |  |  | Consider the following scenario: - AP has set up the GTK with Key ID 3 - Evil STA leaves the BSS - AP is the suspicious type and (rightly) does a GTK rekey, and sets up the GTK with Key ID 2 - The remaining STAs duly install the new GTK under Key ID 2 - Sadly, the old key is still there under Key ID 3 - So Evil STA can forge group frames with the old GTK, and get the remaining STAs to accept them The old GTK needs to be disabled when the new one is set, even with a different Key ID | At the end of the referenced subclause add a para: "After performing GTK rekeying, to avoid attacks from STAs that have left the BSS, a Supplicant shall delete the old GTK when it receives a frame encrypted with the new key." |

### Discussion:

* This is the related text in context:

Text

Description automatically generated

* First of all, the role of the Supplicant is to perform the group key handshake and install the updated key material in the MAC.
* When the group key handshake completes, the Supplicant installs the new group key which replaces the old group key….however could not find text to describe this.

### Proposed Resolution: (3551)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3575 |  | 12.5.3.4.4 |  |  | "If the recipient set the MFPC bit on a given link to 1, it(#199) shall maintain a single replay counter for received individually addressed robust Management frames that are received with the To DS subfield equal to 0," -- it is not clear why an AP should have to do so. Nor why this is only for PV0 | Delete "that are received with the To DS subfield equal to 0" |

### Discussion:

* This is the cited text in clause 12.5.2.4.4 PN and replay detection (assumed):

Text

Description automatically generated

* Note from clause 9.3.3.1 on IQMF and GQMF:

Graphical user interface, text, application

Description automatically generated

* To DS and From DS are set to 0 for non-QMF management frames. The “To DS subfield” indicates that the frame is not QMF.
* A PV1 Frame does not have a To DS field.

### Proposed Resolution: (3575)

REJECTED. In the cited text, the qualification for the To DS subfield equal to 0 indicates that the management frame is not a QMF frame. This applies to PV0 frames only because PV1 frames do not include a To DS subfield.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3620 |  | 12 |  |  | The scope of 12.1 Conventions should be explicitly limited to Clause 12 | Change the first sentence to "In the context of Clause 12, reserved fields and subfields are set to 0 upon transmission and are ignored upon reception." |

### Discussion:

* This CID is a direct copy of previous CID 1898:
  + Comment: The scope of 12.1 Conventions should be explicitly limited to Clause 12
  + Proposed Change: Change the first sentence to "In the context of Clause 12, reserved fields and subfields are set to 0 upon transmission and are ignored upon reception."
* The TG considered this comment in the last round and rejected the comment. Since no further justification has been provided, the comment should be rejected.

### Proposed Resolution: (3620)

REJECTED. This comment was considered by the task group in previous letter ballot round (CID 1898 of LB 258). The commenter did not provide any further justification for making the change in this comment. With respect to CID 1858, the TG reviewed the Comment and Proposed Change and concluded that the Proposed Change could not be accepted, as the issue raised is of broader scope than the resolution.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3638 |  | 12.7.2 |  |  | "4-way handshake message 1 is an EAPOL-Key frame with the Key Type subfield equal to 1. Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a cached PMKSA is not being used, inclusion of the PMKID (if derived) is optional.(#589)(#190)" is both duplication (whether the PMKID is optional or not is specified in the subclause about M1) and incomplete (it's much more than just an EAPOL-Key frame with Key Type 1) | Delete " is an EAPOL-Key frame with the Key Type subfield equal to 1. Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a cached PMKSA is not being used, inclusion of the PMKID (if derived) is optional.(#589)(#190)" |
| 3639 |  | 12.7.2 |  |  | "4-way handshake message 1 is an EAPOL-Key frame with the Key Type subfield equal to 1. Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a cached PMKSA is not being used, inclusion of the PMKID (if derived) is optional.(#589)(#190)" is both duplication (whether the PMKID is optional or not is specified in the subclause about M1) and incomplete (it's much more than just an EAPOL-Key frame with Key Type 1) | Delete " is an EAPOL-Key frame with the Key Type subfield equal to 1. Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a cached PMKSA is not being used, inclusion of the PMKID (if derived) is optional.(#589)(#190)" and similarly for the other messages; put anything specified here that's not specified in 12.7.6/7 into those subclauses |

### Discussion:

* This is the cited text in context:

Text

Description automatically generated

* Looking at Clause 12.7.6.2 and 12.6.10.3.
* It would be good to point to clause 12.7.6.2 in the description.
* The last sentence could be left out. See the revised text in the Proposed Resolution.

### Proposed Resolution: (3638, 3639)

REVISED. The description of message 1 is modified to point to the clause that describes the fields and parameters included in the message.

At 2906.15, change

“Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management). When a cached PMKSA is not being used, inclusion of the PMKID (if derived) is optional.”

to

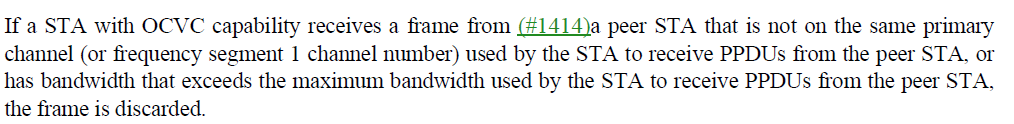
“The fields and their values in the EAPOL-Key PDU are described in 12.7.2. Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.10.3 (Cached PMKSAs and RSNA key management).”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3334 | 2786.00 | 12.2.9 |  |  | If a STA with OCVC capability receives a frame from a peer STA which is not on the same primary channel (or frequency segment 1 channel number) used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded.  -> that "or" parenthetical is not clear. How can you have the same primary channel but not same FS1CN? What if the frame is a 40M or 80M frame (when the BSS bandwidth is 80 or more)? | Change to "If a STA with OCVC capability receives a frame from a peer STA which is not on the same channel used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded." |

### Discussion:

* The cited text in context is here:



* The proposed change is:

"If a STA with OCVC capability receives a frame from a peer STA which is not on the same channel used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded."

* The updated text looks clearer.

### Proposed Resolution: (3334)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3711 |  | 6 |  |  | It is not clear whether the SME picks the Key ID for transmission of encrypted frames (using the Key ID parameter of the MLME-SETKEYS.request) or whether the MAC does so | Specify that frames of a given classification (e.g. unicast, groupcast) are transmitted with the key ID most recently specified for that classification using MLME-SETKEYS.request |

### Discussion:

* The commenter does not cite text, but the relevant text in given in clause 6.5.14.1.4 (Effect of receipt) for MLME-SETKeys

Text

Description automatically generated

* The above behavior describes how the MAC uses the key information.

### Proposed Resolution: (3711)

REJECTED. The text specifying behavior that the commenter is requesting is already present in clause 6.5.14.1.4. See D2.0 at the top of page 492.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 3397 | 2870 | 12.6.9 |  |  | "This means that Data frames other than those containing EAPOL PDUs are discarded when received  before the initial 4-way handshake (see 12.7.6 (4-way handshake)) completes, and the unprotected Data frames (other  than those containing retransmissions of the third message of the initial 4-way handshake (see 12.7.6.6 (4-way  handshake implementation considerations)) are discarded when received after the initial 4-way handshake completes." -- does this need to be extended to cover FILS/FT, where there isn't the usual assoc+4WH sequence? | As it says in the comment |

### Discussion:

* The cited text in context is:

A picture containing timeline

Description automatically generated

* In comment asks whether this needs to be extended to FILS/FT. FILS/FT protocols take place prior to the completion of association, so the state of the STAs in the link is State 1 or State 2. However the 4-way handshake takes place after association completes where the state of the STAs in the link are State 3 (permitting Data frame transmissions). Therefore this text does not need to be extended.

### Proposed Resolution: (3397)

REJECTED. The cited text does not need to be extended to FILS/FT because FILS/FT protocols are executed prior to the completion of association when the STAs are in state 1 or 2. Data frames can only be exchanged in state 3. s