IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB273 Security Adhoc Comment Resolutions Part 1 | | | | |
| Date: 2023-06-12 | | | | |
| 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 LB273.

R0 – Initial version.

R1 –

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4175 |  | 12 |  |  | " See 12.3.4.6 (TKIP replay protection procedures) and 12.5.2.4.4 (PN and replay detection)" should also refer to the GCMP subclause | At 979.5/24 change "and 12.5.2.4.4" to ", 12.5.2.4.4 and 12.5.4.4.4". In the middle cell for PC34.1.10 in B.4 add "12.5.4.3.6 (GCM originator processing), 12.5.4.4.2 (GCM recipient processing), 12.5.4.4.4 (PN and replay detection)" |

### Discussion:

* The locations of the proposed resolution appear to be in these places:

A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a document

Description automatically generated with low confidence

* The commenter is asking to update the description of bits 2 and 3, and the PICS PC34.1.10 with GCM clause references, which looks to be correct.

### Proposed Resolution: (4175)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4350 |  | 12 |  |  | "GNoStations--" in Figure 12-53--Authenticator state machines, part 2 at 2938.13 should be "GNoStations--". Ditto "GKeyDoneStation--". Ditto "GKeyDoneStations -" | At 2938.13 change "GNoStations--" to "GNoStations--". At 2938.22 change "GKeyDoneStation--" to "GKeyDoneStations--" (2 fixes). At 2940.34 change "GKeyDoneStations --" to "GKeyDoneStations--". At 2934.14 and 2938.20 change "Keycount" to "keycount" |

### Discussion:

* The locations of the proposed change appear to be:

A picture containing text, screenshot, diagram, font

Description automatically generated

and

A picture containing text, screenshot, diagram, parallel

Description automatically generated

* It looks as though for the first change at 2938.13 and 2940.34 is actually to change “– ” to “--"
* The other changes are “GKeyDoneStation” to “GKeyDoneStations” at 2938.22 and “Keycount” to "keycount" at 2038.20. Key count should be lower case.

### Proposed Resolution: (4350)

ACCEPTED.

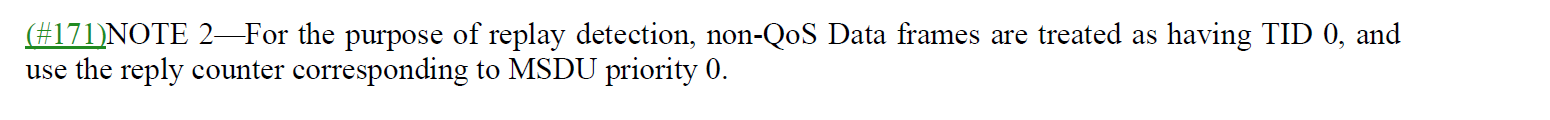
Note to Editor: At 2938.13 and 2940.34 change “– ” to “--"

### Comment

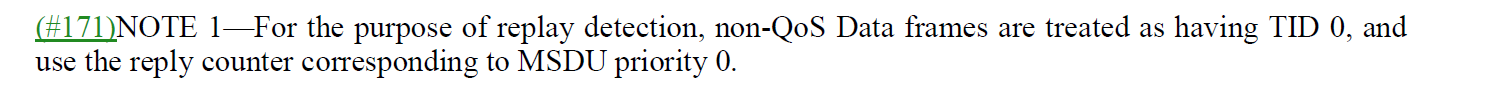
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4300 |  | 12.5 |  |  | "use the reply counter corresponding to MSDU priority 0" -- but replay counters are based on MPDUs not MSDUs. Also typo in "reply" | At 2843.58 and 2853.52 change "the reply counter corresponding to MSDU priority 0" to "the replay counter corresponding to MPDU priority 0" |

### Discussion:

* The text referred to in the Proposed Change is



and



* The Proposed Change replaces MSDU with MPDU in the notes

### Proposed Resolution: (4300)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4117 | 2948.00 | 12.11.2.2 |  |  | Shouldn't 12.11 have mentioned somewhere the use of MIB attribute dot11AuthenticationAlgorithm set to filesSharedKey\* or files PrivateKey? | Add to 12.11.2.2 first paragraph, "An AP \_with dot11AuthenticationAlgorithmsTable including an entry with dot11AuthenticationAlgorithm equal to filsSharedKeyWithoutPFS, filsSharedKeyWithPFS, or filsPublicKey\_ indicates support ...". Add to 12.11.2.3.1 second paragraph, "A STA \_with dot11AuthenticationAlgorithmsTable including an entry with dot11AuthenticationAlgorithm equal to filsSharedKeyWithoutPFS, filsSharedKeyWithPFS, or filsPublicKe\_ may initiate ...". |

### Discussion:

* The cited text where the proposed text changes are:

A close-up of a sign

Description automatically generated with low confidence

and

A close-up of a document

Description automatically generated with low confidence

* The first change appears to be:

At 2948.42, change

“An AP indicates that it is capable of performing FILS authentication by indicating support”

to

“An AP with dot11AuthenticationAlgorithmsTable including an entry with dot11AuthenticationAlgorithm equal to filsSharedKeyWithoutPFS, filsSharedKeyWithPFS, or filsPublicKey indicates support”

* The second change appears to be:

At 2949.15, change

“A STA may initiate FILS Shared Key authentication”

to

“, "A STA with dot11AuthenticationAlgorithmsTable including an entry with dot11AuthenticationAlgorithm equal to filsSharedKeyWithoutPFS, filsSharedKeyWithPFS, or filsPublicKey may initiate FILS Shared Key authentication”

### Proposed Resolution: (4117)

REVISED.

At 2948.42, change

“An AP indicates that it is capable of performing FILS authentication by indicating support”

to

“An AP with dot11AuthenticationAlgorithmsTable including an entry with dot11AuthenticationAlgorithm equal to filsSharedKeyWithoutPFS, filsSharedKeyWithPFS, or filsPublicKey indicates support”

At 2949.15, change

“A STA may initiate FILS Shared Key authentication”

to

“, "A STA with dot11AuthenticationAlgorithmsTable including an entry with dot11AuthenticationAlgorithm equal to filsSharedKeyWithoutPFS, filsSharedKeyWithPFS, or filsPublicKey may initiate FILS Shared Key authentication”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4293 | 2831.00 | 12.4.8.6.4 |  |  | "BadID shall be set" -- not clear by whom. If by protocol instance, then move to the "the protocol instance shall" list | Change "BadID shall be set, the protocol instance shall send a Del event to the parent process and transition back to Nothing state" to "the protocol instance shall set BadID, send a Del event to the parent process, and transition back to Nothing state". At 2830.49 change "the protocol instance shall set BadID and construct and transmit an (#3328)SAE Authentication frame with (#3326)status code UNKNOWN\_PASSWORD\_IDENTIFIER(#3327), and a Del event shall be sent to the parent process." to "the protocol instance shall set BadID and construct and transmit an (#3328)SAE Authentication frame with (#3326)status code UNKNOWN\_PASSWORD\_IDENTIFIER(#3327), and send a Del event to the parent process." |

### Discussion:

* The cited text where the proposed changes are:

A picture containing text, screenshot, font, number

Description automatically generated

and

A picture containing text, screenshot, font, line

Description automatically generated

* The first change (in order of page) is:

At 2830.49, change

“BadID shall be set, the protocol instance shall send a Del event to the parent process and transition back to Nothing state"

to

“the protocol instance shall set BadID, send a Del event to the parent process, and transition back to Nothing state".

At 2830.49 change

"the protocol instance shall set BadID and construct and transmit an SAE Authentication frame with status code UNKNOWN\_PASSWORD\_IDENTIFIER, and a Del

event shall be sent to the parent process."

to

"the protocol instance shall set BadID and construct and transmit an SAE Authentication

frame with status code UNKNOWN\_PASSWORD\_IDENTIFIER, and send a Del

event to the parent process."

### Proposed Resolution: (4293)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4166 | 2844.00 | 12.5.2.4.4 |  |  | "If the receiver set the MFPC bit on a given link to 1, it shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter"  -- even if the peer didn't set the MFPC bit on the link? Ditto in equivalent GCMP subclause | Change to refer to whether MFP was negotiated, as in other locations. Ditto at line 1 and ditto (2x) in 12.5.4.4.4 [confirm direction] |

### Discussion:

* The cited text in the comment is:

A picture containing text, screenshot, font, number

Description automatically generated

* Agree with the commenter that the requirement is dependent on MFP being negotiated.
* There are two locations that use “if the receiver …”: 2844.18 and 2854.6
* There are two locations that use “if the recipient …”: 2844.1 and 2853.54
* All four location could be updated with the format:

“If MFP is negotiated for a given link, the receiver shall”

### Proposed Resolution: (4166)

Revised. Update the text at 4 locations indicating that the condition is “If MFP is negotiated …”

At 2844.18 and 2854.6, change

“If the receiver set the MFPC bit on a given link to 1, it shall”

to

“If MFP is negotiated for a given link, the receiver shall”

At 2844.1 and 2853.54, change

“If the recipient set the MFPC bit on a given link to 1, it shall”

to

“If MFP is negotiated for a given link, the receiver shall”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4319 | 2846.00 | 12.5.3.4 |  |  | "robust GQMFs within an AC that are transmitted to the same RA." -- can a group-addressed Management frame be anything other than broadcast? | Delete "that are transmitted to the same RA" at lines 31 and 32 |

### Discussion:

* The cited text is the following:

A close-up of a text

Description automatically generated with low confidence

* In this case, it’s a group-addressed robust management frame so in this case its OK to leave out “that are transmitted to the same RA”
* An UL group-addressed management frame can be sent as a GQMF.
* P802.11bc introduces UL multicast management frames so it might be good to leave this text.

### Proposed Resolution: (4319)

ACCEPTED

Or

REJECTED. A group-addressed frame can be transmitted to a broadcast RA or a multicast RA. Also a group-addressed frame is transmitted as an individually addressed frame from a non-AP STA to an AP.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4322 |  | 12.5.3.5 |  |  | The stuff in 12.5.3.5 about "should" not use the old key when IGTK rekeying should be promoted to a "shall", as for GTK and BIGTK | Change "Once a STA transmits a protected group addressed robust Management frame using a new IGTK, the STA should not transmit protected group addressed robust Management frames using the previously used IGTK" to "Once a STA transmits a protected group addressed robust Management frame using a new IGTK, the STA shall not transmit protected group addressed robust Management frames using the previously used IGTK" |

### Discussion:

* The cited text in context is:

A picture containing text, screenshot, font, line

Description automatically generated

* The proposed change is as follows:

Change

“Once a STA transmits a protected group addressed robust Management frame using a new IGTK, the STA should not transmit protected group addressed robust Management frames using the previously used IGTK"

to

"Once a STA transmits a protected group addressed robust Management frame using a new IGTK, the STA shall not transmit protected group addressed robust Management frames using the previously used IGTK"

* The IGTK behaviour should follow the same behaviour as the BIGTK.

### Proposed Resolution: (4322)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4299 | 2847.00 | 12.5.3.6 |  |  | "If no such IGTK exists, silently discard(#187) the frame and terminate BIP processing for this recep- tion." should be "If the frame is a robust Management frame and no such IGTK exists, silently discard(#187) the frame and terminate BIP processing for this recep- tion." since the next sentence is about protected beacons | As it says in the comment |

### Discussion:

* The cited text in context is:

A close-up of a document

Description automatically generated with medium confidence

* The proposed change is:

At 2847.26, change

“If no such IGTK exists, silently discard(#187) the frame and terminate BIP processing for this reception.”

to

“If the frame is a robust Management frame and no such IGTK exists, silently discard(#187) the frame and terminate BIP processing for this reception”

### Proposed Resolution: (4299)

ACCEPTED.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4108 | 2857.00 | 12.6.1.1.6 |  |  | "AKM suite" was changed to "AKMP" for CID 3266 (throughout, many locations), but CID 3266 says it was rejected. So, is this change correct and agreed? | Confirm this change, or revert it. |

### Discussion:

* Text at cited location:

A close-up of a document

Description automatically generated with low confidence

* Resolution to CID 3266:

REVISED (EDITOR: 2023-04-04 23:04:24Z) - Make the changes shown under “Proposed changes” for CID 3266 in https://mentor.ieee.org/802.11/dcn/22/11-22-2069-09-000m-resolutions-for-some-comments-on-11me-d2-0-lb270.docx, which make “AKM 00-0F-AC:<n>” an acceptable shorthand for the AKMP identified by that AKM suite selector value. In the cited text, PN and RSC describe the same counter.

### Proposed Resolution: (4108)

REJECTED. The resolution approved by the TG was REVISED and adopted the changes in doc 11-22/2069r9.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4109 | 2857.00 | 12.6.1.1.6 |  |  | Here, it says "Supplicant MAC address or STA's MAC address ..." But, at P2884.32, it says, "In an infrastructure BSS, the IEEE 802.1X Authenticator MAC address (AA) and the AP's MAC address are the same, and the Supplicant's MAC address (SPA) and the STA's MAC address are equal." So, is there some subtle distinction being made in 12.6.1.1.6 for non-infrastructure cases, and if so that should be explained or it won't be understood. Or, is the distinction in 12.6.1.1.6 unnecessary, and it should just say "Supplicant MAC" or "Authenticator MAC" (or "STA's MAC" or "BSSID")? | Clarify this subtlety if it is real, remove it if it is not real. |

### Discussion:

* The cited text in context is

A screenshot of a computer error

Description automatically generated with low confidence

* Other cited text in the comment:

A picture containing text, font, screenshot

Description automatically generated

* Text describing addresses in SAE (12.4.1 p2809.5)

A close-up of a document

Description automatically generated with low confidence

* In SAE, the “or STA’s MAC address” refers to the PTKSA for SAE. Similarly “or BSSID” refers to the AP MAC address when SAE is used in an infrastructure network.

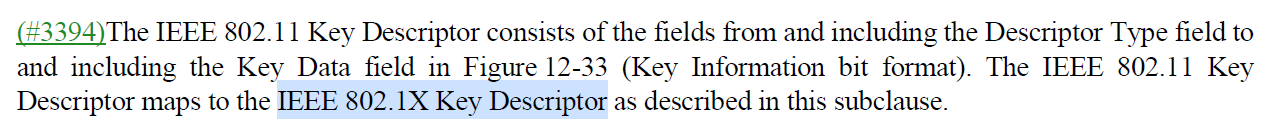
### Proposed Resolution: (4109)

REJECTED. The PTKSA is different depending on the negotiated AKMP. For SAE, the PTKSA is includes the STA MAC Address, and for IEEE 802.1X, the PTKSA includes the Authenticator and Supplicant MAC addresses.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4230 | 2898.00 | 12.7.2 |  |  | "The IEEE 802.11 Key Descriptor maps to the IEEE 802.1X Key Descriptor as described in this subclause." is not saying anything clear or useful | Delete the cited sentence |

### Discussion:

* The cited text in context is:
* This is the only usage in the subclause for “IEEE 802.1X Key Descriptor. Therefore the sentence could be deleted.

### Proposed Resolution: (4230)

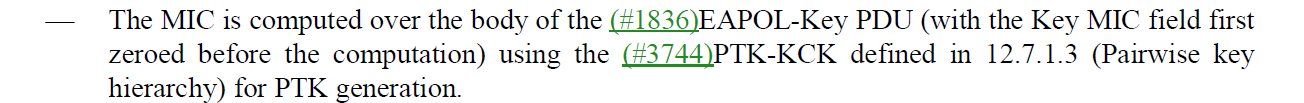
ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4144 | 2911.00 | 12.7.6.1 |  |  | "The MIC is computed over the body of the (#1836)EAPOL-Key PDU (with the Key MIC field first zeroed before the computation) using the KCK defined in 12.7.1.3 (Pairwise key hierarchy) for PTK generation." -- it is not clear what the last 3 words mean. They don't appear for the GKH | Delete " for PTK generation" in the cited text |

### Discussion:

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



* Agree with the comment that “for PTK generation” can be deleted in this sentence.

### Proposed Resolution: (4144)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4165 | 2926.00 | 12.7.8.2 |  |  | "PairwiseCipherSuite field of the RSNE " -- no such field | Change the para at the referenced location to "Pairwise Cipher Suite List field of the RSNE identifies the cipher suite(s) that can be or are used to protect the Data frames sent over the (#2152)TDLS direct link". At line 41 change "TimeoutIntervalType" to "Timeout Interval Type". At line 47 change "AKM suite list" to "AKM Suite List" |

### Discussion:

* This is the cited text in context:

A picture containing text, screenshot, font, document

Description automatically generated

* The changes proposed by the commenter are:

At cited location, change “PairwiseCipherSuite field of the RSNE identifies the cipher suite used to protect the Data frames sent over the TDLS direct link”

to

“Pairwise Cipher Suite List field of the RSNE identifies the cipher suite(s) that can be or are used to protect the Data frames sent over the TDLS direct link”

At line 41, Change "TimeoutIntervalType" to "Timeout Interval Type"

At line 47 change "AKM suite list" to "AKM Suite List"

* The changes look to be mostly aligning field names and capitalization.

### Proposed Resolution: (4165)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4225 | 2928.00 | 12.7.8.4.2 |  |  | "indicate (#3266)AKM 00-0F-AC:7(TPK handshake)" -- what if it includes >1 AKM? Ditto "indicate a negotiated AKM" for FT (but maybe that's OK because it's in the assoc req where you can only have a single AKM -- but is that specified anywhere and what about 2975.42, 2977.54, 2980.9?) | Change the former to "indicate the single (#3266)AKM 00-0F-AC:7(TPK handshake)". |

### Discussion:

* This is the cited text in context:

A screenshot of a computer

Description automatically generated with low confidence

* The commenter is asking to specify that there is a single AKM, changing “indicate TPK handshake (00-0F-AC:7)” to “indicate the single AKM 00-0F-AC:7 (TPK handshake)

### Proposed Resolution: (4225)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4229 | 2929.00 | 12.7.8.4.3 |  |  | "All other RSNE fields shall be same as those received in message 1." -- not the RSN Capabilities field | Change to "All other RSNE fields, apart from the RSN Capabilities field if present, shall be same as those received in message 1." (but what about existing devices?) [needs discussion] |

### Discussion:

* This is the cited text in context:

A picture containing text, screenshot, font, number

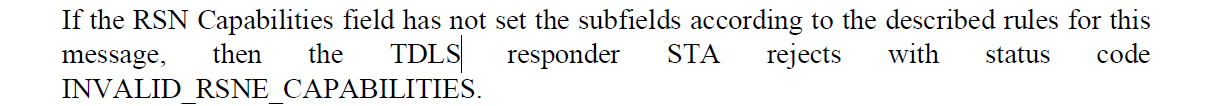
Description automatically generated

* The comment proposed changing the highlighted text above to “to "All other RSNE fields, apart from the RSN Capabilities field if present, shall be same as those received in message 1."
* The RSN Capabilities is defined as follows:

A picture containing text, screenshot, font, number

Description automatically generated

* In the requirements for TPK handshake message 1 on p2929.5, the TDLS responder STA is required to evaluate the value of the RSN Capabilities field:



### Proposed Resolution: (4229)

REJECTED. The purpose of the RSNE used in the TPK handshake is to negotiate a secure TDLS link. The TDLS Responder STA is required to evaluate the RSN Capabilities received in TPK handshake message one and include the same value in message 2.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4143 | 2934.00 | 12.7.9.4 |  |  | PreANonce is not defined | Change PreANonce to PrevANonce (2x) and add "PrevANonce<-0" at 2933.46, where <- is the left arrow glyph |

### Discussion:

* This is the cited text at 2934.4:

A picture containing text, screenshot, font, white

Description automatically generated

* This is the cited text at 2933.46 where the initialization of PrevANonce should be added:

A screenshot of a computer program

Description automatically generated with low confidence

* The previous ANonce may or may not be zero, so initialization to 0 is not correct.

### Proposed Resolution: (4143)

REVISED. Change “PreANonce” to “PrevANonce” at cited locations. The PrevANonce value is 0 or set to the previous ANonce value used in the previous 4-way handshake. Therefore, it is not necessarily initialized to 0.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4396 | 2970.00 | 13.4.2 |  |  | This sentence says that FT initial mobility association is initiated using Open System authentication in non-DMG case. However that is not true when an SAE over FT AKM is used (without PMK caching). | Insert "or SAE algorithm" after "Open System authentication algorithm" on lines 61, 63 and 64. In Figure 13-2, insert "or SAE" after "Open" in the annotations for the top two arrows. In Figure 13-2, insert "or SAE" after "bypassed if PSK" in the annotation for the 5th arrow. |

### Discussion:

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

A picture containing text, font, screenshot, line

Description automatically generated

* Note that the next paragraph on p2971.32 is the following:

A picture containing text, screenshot, font, line

Description automatically generated

* Given that FT with SAE is covered in the next paragraph, it might be more reasonable to rename Fig 13-2 to “FT initial mobility domain association in an RSN using Open System Authentication”

### Proposed Resolution: (4396)

REVISED. The use of FT with SAE is covered in the next paragraph. See p2971.32.

Change the caption of Figure 13.2 to the following:

“FT initial mobility domain association in an RSN using Open System Authentication”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 4397 | 978.00 | 9.4.2.23.3 |  |  | There are various missing references to the new SAE AKMs. e.g. the referenced sentence should also refer to AKM 24 (and the SAE-FT AKMs too?) NOTE 5 (line 20) also seems outdated/incomplete. Also 12.12.2 p2963 line 14 refers to AKMs 8/9 for SAE but not the other SAE AKMs | Per comment, either update the references or remove them and just refer to "SAE" pointing to the AKM suite selector table for details |

### Discussion:

* This is the cited text in context:

A screenshot of a computer

Description automatically generated with medium confidence

* The other referenced clause (12.12.2 – Security Constraints in the 6 GHz band)

A picture containing text, screenshot, font

Description automatically generated

* It would be good to update the text at 978.18 to include AKM 24.
* Similarly, in 12.12.2, It would be good to update the last bullet to include AKMs 24 and 25.

### Proposed Resolution: (4397)

REVISED. Update the cited text to include AKM 24 an 25 where appropriate.

At 978.14, change:

“AKM 00-0F-AC:8 (i.e., SAE authentication with SHA-256) is used when either a password or PSK is used with RSNA key management.”

To

“SAE authentication (AKM 00-0F-AC:8 or 00-0F-AC:24) is used when either a password or PSK is used with RSNA key management.”

At 2963.14, change:

“The STA should use SAE (AKM 00-0F-AC:8 and/or 00-0F-AC:9) if authenticating using a password …”

To

“The STA should use SAE (AKM 00-0F-AC:8, 00-0F-AC:9, 00-0F-AC:24 and/or 00-0F-AC:25) if authenticating using a password …”