IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA3 Security comment resolutions | | | | |
| Date: 2024-07-17 | | | | |
| 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 the SA Ballot recirculation on D6.0.

R0 – Initial version.

R1 – Review of comments on July 15

R2 – Review of comments on July 16 AM2

R3 – Updates to comments on July 16 and 17 AM2

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8039 | 4963.00 | 34.3.2 |  |  | The reference to TIM element is incorrect - it should be 9.4.2.5 | Replace "(see 9.4.2.314 ...)" with "(see 9.4.2.5 ...)" |

### Discussion:

* Upon consultation with Abhi

### Proposed Resolution: (8039)

REVISED. Make the changes in <this> document under “Proposed Resolution: (8039)”

**34.3.2 EBCS DL procedure at an EBCS AP**

***TGm editor, please modify the contents of this paragraph (including adding a NOTE) as show below:***

An EBCS AP, which is not an S1G AP, shall advertise its EBCS capabilities in the EBCS Support field in the Extended Capabilities element in Beacon frames and Probe Response frames. An EBCS AP that has EBCS DL enabled shall transmit EBCS Info frames periodically. The interval between two consecutive EBCS Info frames is specified by dot11EBCSInfoInterval. An EBCS AP shall advertise the timing of the next EBCS Info frame transmission in the EBCS Info Frame TX Countdown field in the EBCS Parameters element and shall not signal an upcoming EBCS Info frame via the TIM element or the EBCS TIM element ~~(see 9.4.2.314 (EBCS TIM element)) in Beacon frames~~. An EBCS AP shall advertise the certificate group in Beacon frames using the Compressed Certificate Group ID field in the EBCS parameters element if the EBCS AP belongs to an EBCS certificate group. An EBCS AP shall advertise the EBCS AP group by the EBCS Group ID field in the EBCS Parameters element in Beacon frames if the EBCS AP belongs to an EBCS AP group. The EBCS Info frame shall be transmitted among the set of group addressed frames transmitted immediately after the Beacon frame identified by the EBCS Info Frame TX Countdown field set equal to 1 in the EBCS Parameters element. Details of EBCS Info frame generation are described in 34.3.4 (EBCS Info frame generation and usage).

NOTE - An EBCS AP might provide the timing of the next EBCS Info frame transmission for a reported AP by including a TBTT Information field (corresponding to the reported AP) carrying the EBCS Info Frame TX Countdown field within a Reduced Neighbor Report element.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8192 | 2653.00 | 11.11.3 |  |  | "(i.e., height above ground is in meters or, in other words, the altitude is in meters above adjacent terrain) -- why are other words needed? | Delete from "or, in other words, the altitude is in meters above adjacent terrain" |

### Discussion:

* The cited text is shown as follows:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8192)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8197 | 3170.00 | 12.13.4 |  |  | "FILS AKMP 00-0F-AC:14" should be just "AKMP 00-0F-AC:14" | As it says in the comment |

### Discussion:

* The cited text for the comments in context is:

A close-up of a document

Description automatically generated

### Proposed Resolution: (8197)

REVISED. Change “FILS AKMP” to “AKM” at cited location.

Also, at 3070.8, change “AKMP” to “AKM”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8198 | 3002.00 | 12.4.3 |  |  | "In an infrastructure BSS for which an SAE AKM is indicated" -- the term "SAE AKM" is not defined | Either list the specific selectors (risk of spec rot) or say something like "An AKM for which the Authentication type cell in Table 9-190—AKM suite selectors identifies SAE" |

### Discussion:

* The cited text in context (see last sentence)

A close-up of a text

Description automatically generated

### Proposed Resolution: (8198)

REVISED.

Change

“In an infrastructure BSS for which an SAE AKM is indicated, the AP shall”

To

“In an infrastructure BSS advertising an AKM for which the Authentication type cell in Table 9-190 identifies SAE, the AP shall”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8199 | 3147.00 | 12.11.2.2 |  |  | "FILS AKM" is not defined (2x) | Either list the specific selectors (risk of spec rot) or say something like "An AKM for which the Authentication type cell in Table 9-190—AKM suite selectors identifies FILS" |

### Discussion:

* The cited text in the comment is:

A screenshot of a document

Description automatically generated

### Proposed Resolution: (8199)

REVISED. At 3147.42 and 3147.50, change

“indicating support for a FILS AKM in …”

to

“indicating support for an AKM in Table 9-190 for which the Authentication type cell identifies FILS in …”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8190 | 2711.00 | 11.21.6.3.3 |  |  | "NOTE 2—Because the FTM procedure executes at the PHY/MAC layer" -- it's not clear what "the PHY/MAC layer" is, nor what it means for a procedure to execute at this layer, whatever it is | Delete the NOTE |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer error

Description automatically generated

* The note seems to indicate that the ISTA has the option not to share the measurements with the RSTA and use them for some other purposes such as sharing information with higher layers.

### Proposed Resolution: (8190)

REVISED. Change the note as follows:

Change

“NOTE 2—Because the FTM procedure executes at the PHY/MAC layer, an RSTA accepting a ranging request despite…”

to

“NOTE 2—An RSTA that accepts a ranging request despite…”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8228 | 2809.00 | 11.22.2 |  |  | The normative text says "The HESSID value shall be … and all BSSs in the HeSS use the same value." But, as clearly stated in NOTE 1 just below, this is an administrative task outside the control of 802.11 requirements. Similar situations use "needs to" language to express such (external to the Standard) requirements, this should align. | Change to "and all BSSs in the HeSS need to use the same value for proper operation." Change NOTE 2 to, "The HESSID field in the Interworking element needs to be managed by the network administrator, so that it has the same value across all BSSs in an HeSS." |

### Discussion:

* The cited text in the comment is:

A close-up of a text

Description automatically generated

* The changes are:

At 2809.34, change

“in the HeSS and all the BSSs in the HeSS use the same value.”

To

“in the HeSS. All the BSSs in the HeSS use the same value.”

At 2809.41, change (actually NOTE 1)

“…needs to be administered to have the same value across all BSSs in the HeSS.”

To

“…needs to be managed by the network administrator so that it has the same value across all BSSs in the HeSS.”

### Proposed Resolution: (8228)

REVISED.

At 2809.34, change

“in the HeSS and all the BSSs in the HeSS use the same value.”

To

“in the HeSS. All the BSSs in the HeSS use the same value.”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8146 | 1093.00 | 9.4.2.46 |  |  | "The Key Length field is the length of the BIGTK in octets" -- or the length of the Wrapped Key field, actually? Ditto WIGTK | As it says in the comment |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8146)

REVISED. The cited text is consistent with the definition of the GTK and IGTK.

At 1093.41. Delete the second sentence.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8148 | 605.00 | 9.2.2 |  |  | "Without further qualification, reception by the MAC sublayer implies that the frame contents are valid, and that the protocol version is supported (see 9.2.4.1.2 (Protocol Version subfield)), with no implication regarding frame addressing or regarding whether the frame type or other fields in the MAC header are meaningful to the MAC entity, where the frame is addressed to the STA (individually addressed or group addressed).(#6185) " -- "with no implication regarding frame addressing" contradicts the latter part of the sentence and the next para, where the frame addressing is relevant | Delete "frame addressing or" |

### Discussion:

* The cited text in the comment is:

A close-up of a text

Description automatically generated

### Proposed Resolution: (8148)

REVISED. Make the changes provided by the commenter, fixing the repetitive “regarding”

At cited location, change “with no implication regarding frame addressing or regarding …” to “with no implication regarding….”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8234 | 2616.00 | 11.9.3.2 |  |  | We don't generally use the phrase "protected management frame" (there are only two occurences, here, and P3038.58). | At 2616.59, replace "was based on a protected management frame" with "was based on a management frame received with management frame protection enabled". At 3038.59, replace "a protected Management frame" with "a BIP encapsulated Management frame". |

### Discussion:

* The cited text in the comment is:

A close-up of a text

Description automatically generated

* And at 3038.59:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8234)

REJECTED. The proposed resolution causes more confusion than the existing text.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8183 | 2691.00 | 11.21.3.1 |  |  | "All outstanding diagnostic requests, as indicated by received MLME-DIAGREQUEST.indication primitives, are canceled upon a BSS transition, except when the BSS transition occurs as a result of responding to or initiating a diagnostic request. All outstanding diagnostic requests, as indicated by received MLME-DIAGREQUEST.indication primitives, are canceled after the time indicated in the Diagnostic Timeout field, in the Diagnostic Request frame." -- these are normative requirements on the SME, so should be "The SME shall cancel all..." | As it says in the comment |

### Discussion:

* The cited text in the comment is:

A close-up of a text

Description automatically generated

* One way to address this comment would be to change “are canceled” to “shall be canceled by the SME” on lines 42 and 44

### Proposed Resolution: (8183)

REVISED. At 2691.42 and 2691.44, change “are canceled” to “shall be canceled by the SME”

At 2691.47, change “the STA shall” to “the SME shall”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8185 | 825.00 | 9.4.1.31 |  |  | "The maximum value permitted in the GAS Query Fragment ID is 127." -- well, duh, it's a 7-bit field. Also missing the word frame | Delete the cited text |

### Discussion:

* The cited text in the comment is:

A close-up of a text

Description automatically generated

### Proposed Resolution: (8185)

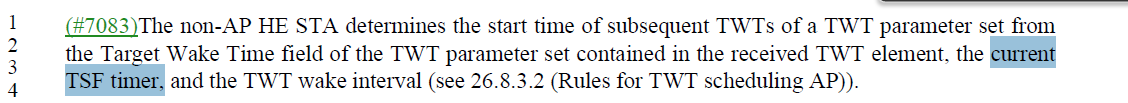
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8162 |  | 26.8.3 |  |  | "current TSF timer" -- there is only one TSF timer (2x) | Change to "TSF timer" |

### Discussion:

* The cited text in the comment is:
* 4141.2



* 4146.8

A close-up of a text

Description automatically generated

### Proposed Resolution: (8162)

REVISED.

At 4141.2, change “current TSF timer” to “TSF timer”

At 4146.8, change “current TSF timer” to “current value of the TSF timer”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8166 | 3080.00 | 12.6.20.4 |  |  | "Only TPK-TK in the TPKSA is required for the supported band/channel. " is not clear. Maybe better as "The TPK-KCK in the TPKSA is not required" but even so the "for the supported band/channel" bit is not clear | As it says in the comment |

### Discussion:

* The cited text in the comment is:

A close-up of a document

Description automatically generated

* Looking at the text in context, the TPKSA is derived from communications in one band and the TPK-TK is used for encapsulation in the other band. A better way to improve would be change the last sentence to be: “The TPK-TK is used for cryptographic encapsulation of MPDUs in the other supported band/channel”

### Proposed Resolution: (8166)

REVISED. At 3080.30, change

“Only TPK-TK in the TPKSA is required for the supported band/channel.”

To

“The TPK-TK in the TPKSA is used for cryptographic encapsulation of MPDUs in the other supported band/channel.”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8172 | 1118.00 | 9.4.2.62 |  |  | "If transmitted in a (Re)Association Request frame, the Switch Timeout field is not present in the Channel Switch Timing element." -- but the figure says it's always present | In Figure 9-471—Channel Switch Timing element format change the rightmost 2 to "0 or 2" |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8172)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8168 | 3028.00 | 12.5.2.3.1 |  |  | "Construct the (#209)CCM nonce as defined in 12.5.2.3.4 (Construct CCM nonce) from the PN, A2, and the priority value of the MPDU" -- the nonce has other stuff, e.g. Managementness and PV1ness, so this is misleading. The perils of duplication! | Delete the "from the PN, A2, and the priority value of the MPDU" (but keep the "where A2 is" bit since this is relevant) and replace with a comma. Ditto at line 54. At 3046.63 delete "from the PN and A2" |

### Discussion:

* The cited text in the comment is:

A close up of a text

Description automatically generated

* Cited text at 3046.63

A close-up of a computer error

Description automatically generated

### Proposed Resolution: (8168)

REVISED

At cited location, change

“Construct the (#209)CCM nonce as defined in 12.5.2.3.4 (Construct CCM nonce) from the PN,

A2, and the priority value of the MPDU where A2 is MPDU Address 2”

To

“Construct the (#209)CCM nonce as defined in 12.5.2.3.4 (Construct CCM nonce)

where MPDU Address 2 is used as A2.”

At 3046.63, change

“Construct the (#209)GCM nonce as defined in (#357)12.5.4.3.4 (Construct GCM nonce) from the PN and A2, where A2 is MPDU Address 2.”

To

“Construct the (#209)GCM nonce as defined in (#357)12.5.4.3.4 (Construct GCM nonce).”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8236 | 3174.00 | 12.13.8 |  |  | Extraneous "3" | Delete the "3" |

### Discussion:

* The cited text in the comment is:

A white paper with black text

Description automatically generated

### Proposed Resolution: (8236)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8238 | 3109.00 | 12.7.6.1 |  |  | The restrutcture of 12.7.6.1 notation has some concerns: - 12.7.4 (which is the normative reference for the syntax) uses "OCI KDE", not just "OCI" - Readability is low, due to the inconsistent use of white space (in my opinion). | Consider: - changing "OCI" to "OCI KDE" to match the notation defined in 12.7.4. Alternatively, remove the "KDE" in the first occurence on line P3108.42, both occurences at P3109.53/54. Similar change (which ever one) on Page 3120, et seq. - adding spaces after the commas, so we don't get weird line-breaks and spacing on Message 1, and it is consistent inside/outside the brackets, and just overall easier to read. |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer

Description automatically generated

* Given 2 other projects are modifying the cited text, the better option at this point is to change OCI KDE to OCI in the notation

### Proposed Resolution: (8238)

REVISED. Update the EAPOL-KEY notation to use OCI only.

At 3108.42 (left most occurrence), 3120.56, change “OCI KDE” to “OCI”.

At 3120.57, change “OCI KDE” to “The OCI KDE”

Add a space after each comma that is not already followed by a space in 12.7.6.1 P3109 L13-L24 and at P3120 L27-30."Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8240 | 713.00 | 9.3.1.22.10 |  |  | Normative verb in clause 9. | Replace "may be" with "is" |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8240)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8241 | 775.00 | 9.3.3.11 |  |  | Normative verb in clause 9. | At 775.49, 775.53, 775.55, 776.13, 776.19, 776.21, 776.28 replace "may be" with "is optionally" |

### Discussion:

* The cited text in the comment is:

A close-up of a web page

Description automatically generated

A white sheet with black text

Description automatically generated

### Proposed Resolution: (8241)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8201 | 3165.00 | 12.13.3.1 |  |  | In Figure 12-59—PASN authentication "PMKID[0..1]" should be "[PMKID]" because the response contains the PMKID that matched, if any | As it says in the comment |

### Discussion:

* The cited text in the comment is:

A diagram of a system

Description automatically generated

### Proposed Resolution: (8201)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8145 | 1091.00 | 9.4.2.46 |  |  | "The Key Length field is the length of the Key field in octets" -- no such field | Change "Key field" to "Wrapped Key field" |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8145)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8203 | 1253.00 | 9.4.2.138 |  |  | Should be clearer that "No-Fragmentation" is for DMG STAs per 10.2.7 but 9.4.2.138 suggests it's for any non-HE STAs | Change "The No-Fragmentation subfield is reserved when transmitted by an HE STA to another HE STA.(11ax) " to "The No-Fragmentation subfield is reserved when not transmitted by a DMG STA " |

### Discussion:

* The cited text in the comment is:

A close-up of a document

Description automatically generated

* From 10.2.7:

A close-up of a text

Description automatically generated

### Proposed Resolution: (8203)

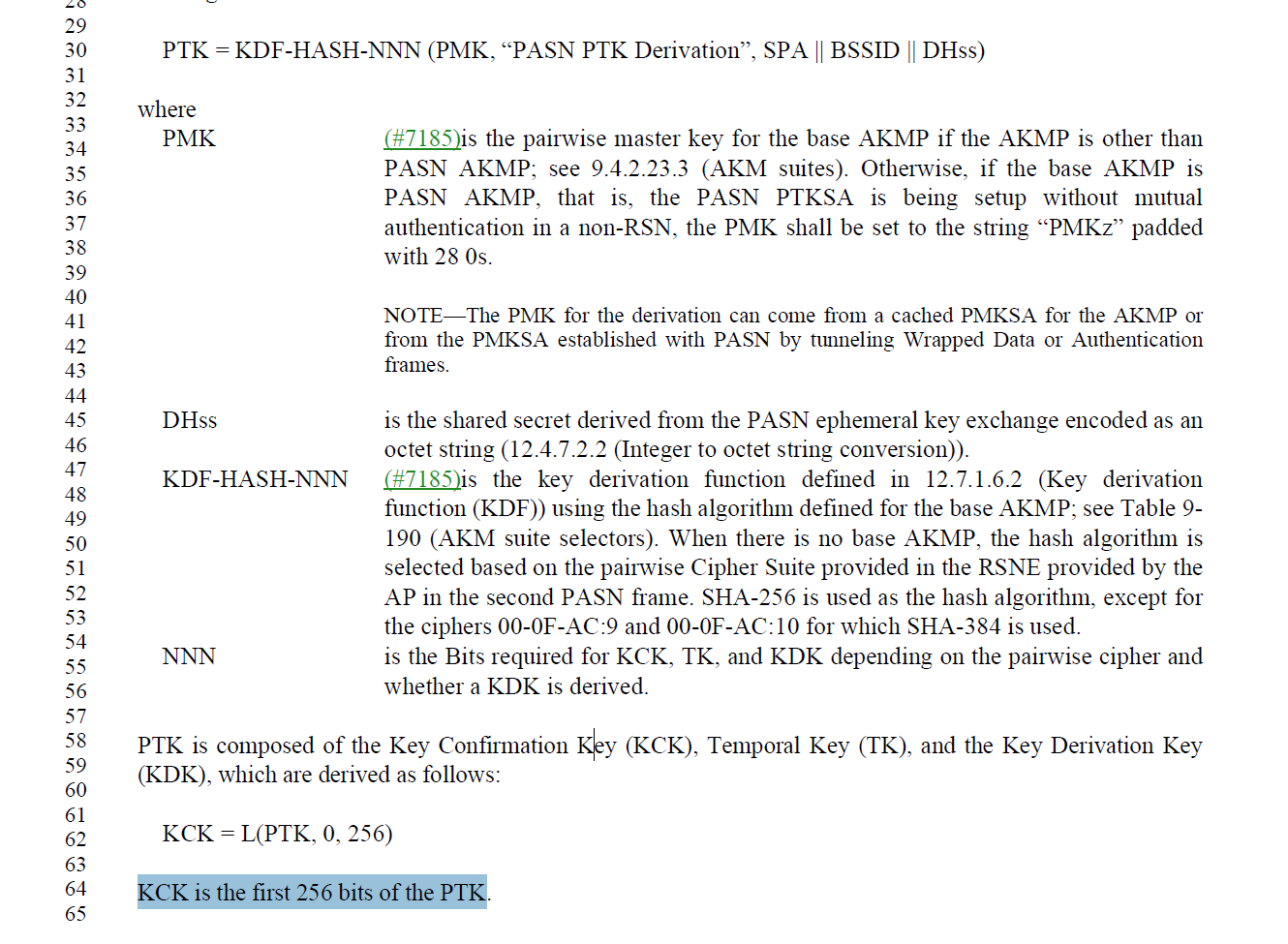
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8206 | 3173.00 | 12.13.8 |  |  | "KCK is the first 256 bits of the PTK." duplicates the line immediately above | Delete the cited text |

### Discussion:

* The cited text in the comment is:



* Clause 12.7.1.3 does not have these statements so it’s OK to remove.

### Proposed Resolution: (8206)

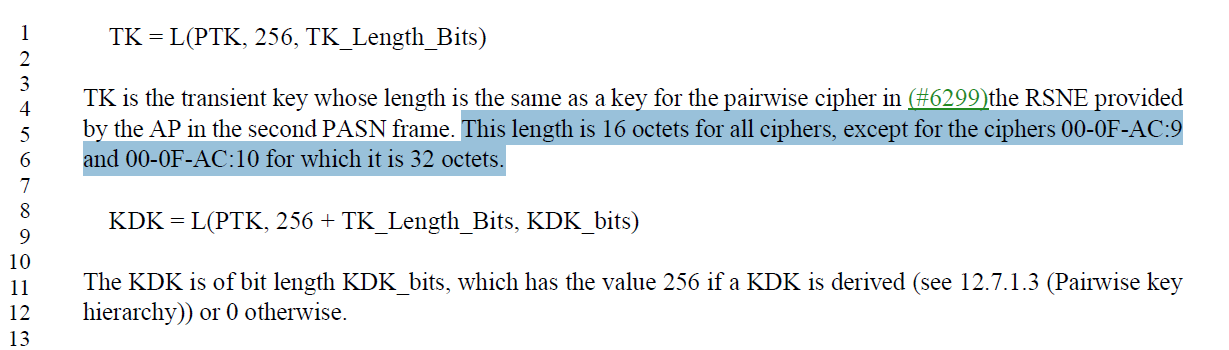
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8207 | 3174.00 | 12.13.8 |  |  | "This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets." either duplicates or contradicts existing normative text | Delete the cited text |

### Discussion:

* The cited text in the comment is:



* This text is duplicative.

### Proposed Resolution: (8207)

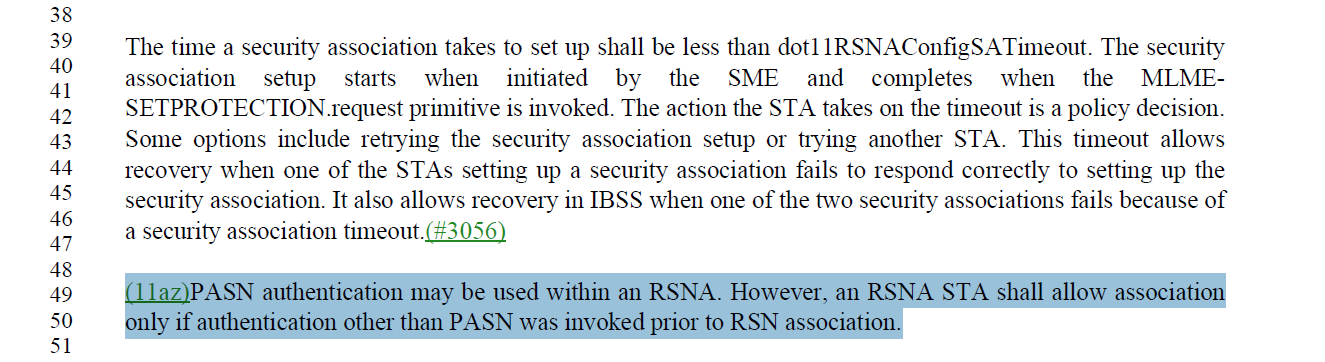
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8208 | 2978.00 | 12.2.4 |  |  | "RSN association" is not defined | Delete "RSN " in the cited text |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8208)

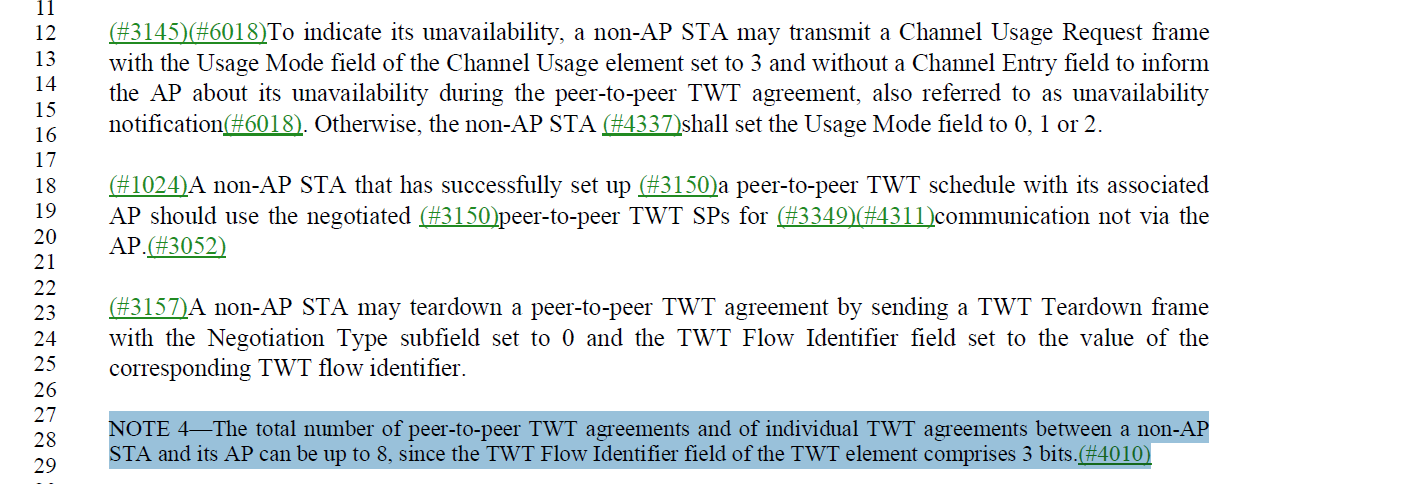
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8070 | 2789.00 | 11.21.15 |  |  | Total number cannot be 8 +8 =16. | delete "of" before "individual TWT agreements". |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8070)

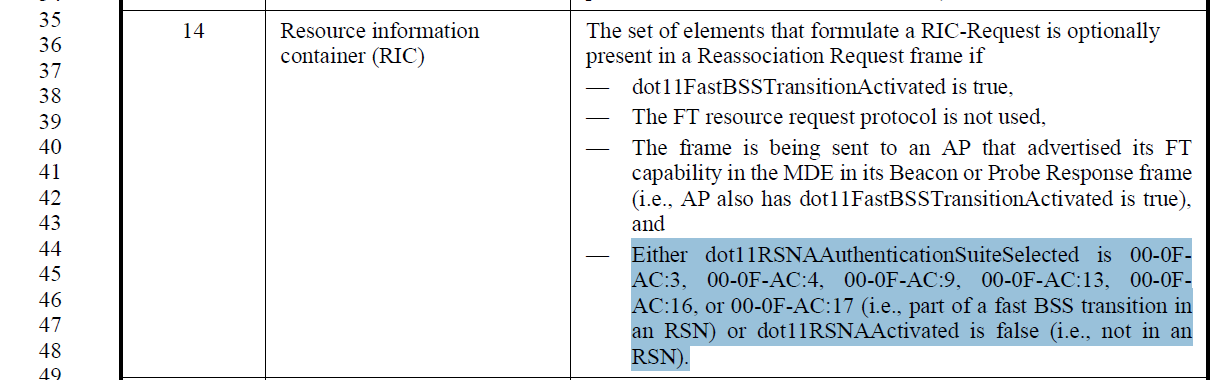
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8088 | 749.00 | 9.3.3.7 |  |  | "Either dot11RSNAAuthenticationSuiteSelected is 00-0F-AC:3, 00-0F-AC:4, 00-0F-AC:9, 00-0F-AC:13, 00-0F-AC:16, or 00-0F-AC:17 (i.e., part of a fast BSS transition in an RSN) " is prone to spec rot | Change to "dot11RSNAAuthenticationSuiteSelected is equal to an AKM suite selector value for which the Authentication type column indicates FT authentication, or dot11RSNAActivated is false (i.e., not in an RSN). See Table 9-190 (AKM suite selectors) (i.e., part of a fast BSS transition in an RSN)." (cf. cell above) |

### Discussion:

* The cited text in the comment is:



* So, clearly the AKMs are FT AKMs

### Proposed Resolution: (8088)

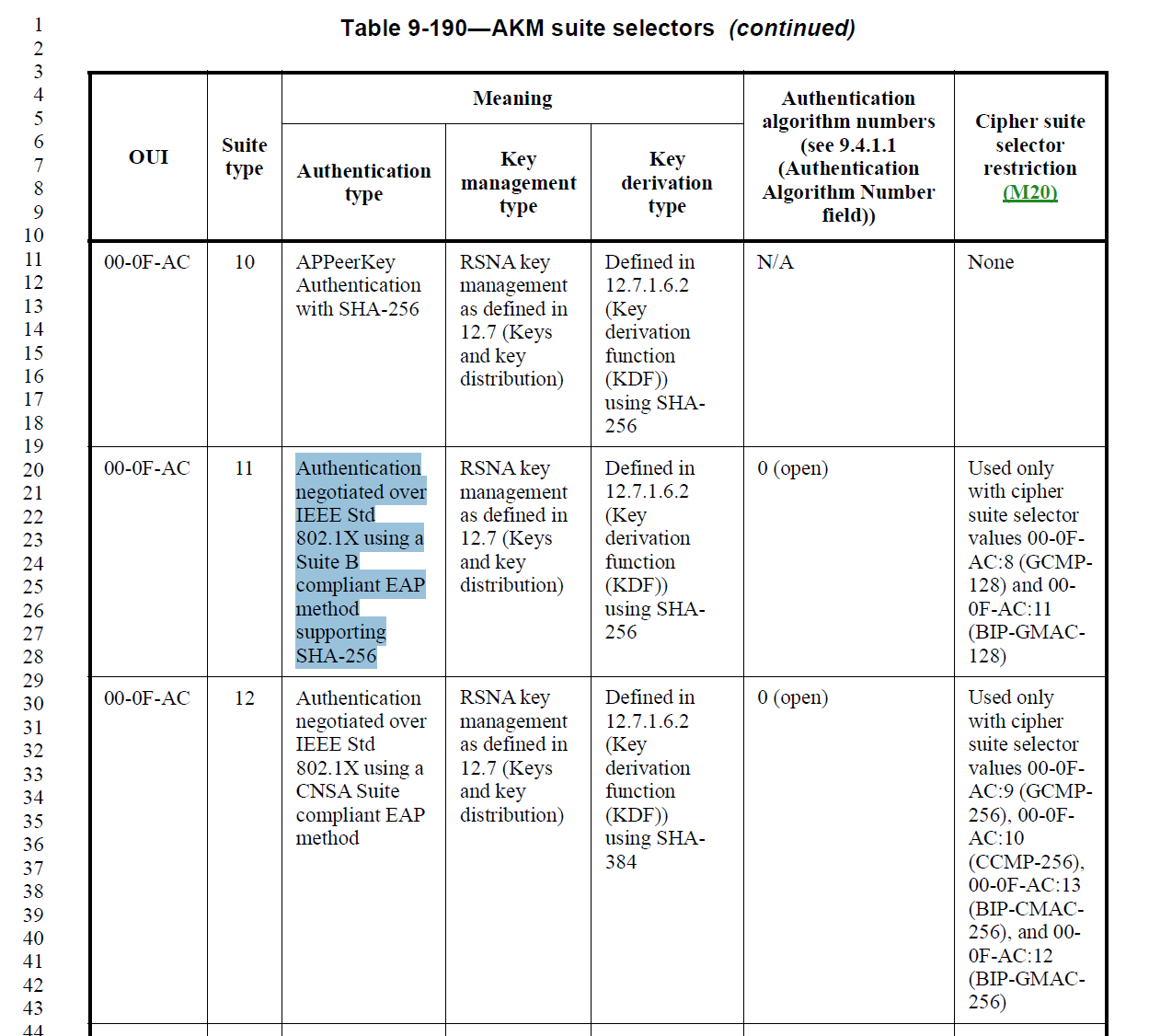
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8089 | 1024.00 | 9.4.2.23.3 |  |  | Suite B should be indicated as deprecated (cf. CNSA) | Below "11" in the second cell from the left add "(deprecated)" |

### Discussion:

* The cited text in the comment is:

=

* The CSNA Suite B algorithms are used in deployed networks today. The commenter provides no justification for deprecating CSNA suite B AKMs.

### Proposed Resolution: (8089)

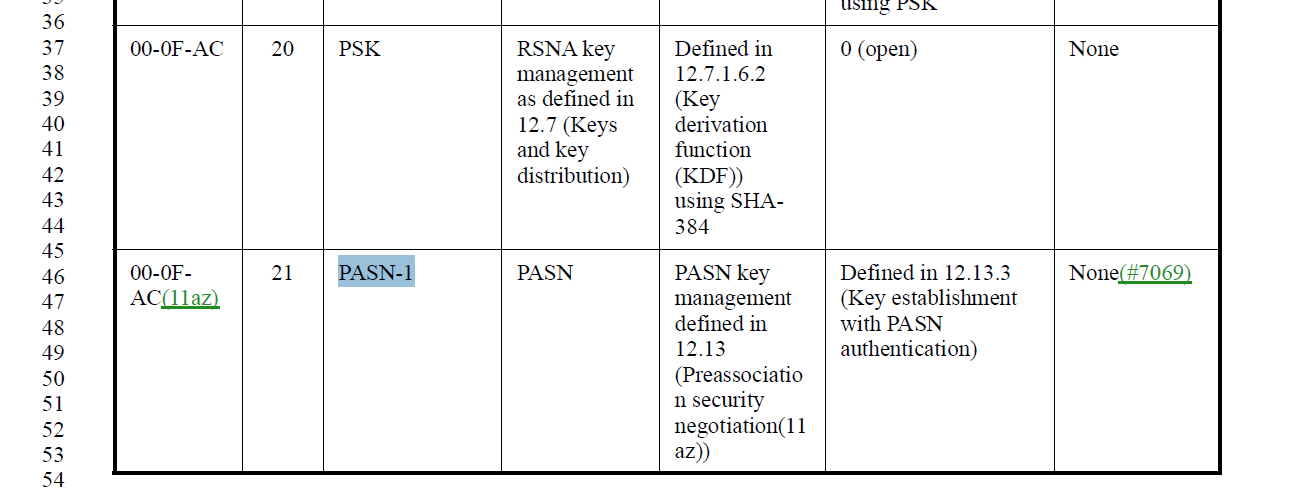
REJECTED. Suite B AKMs are used in deployed WLAN systems today. No justification has been provided to deprecate these AKMs.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8090 | 1026.00 | 9.4.2.23.3 |  |  | "PASN-1" is not defined; I surmise it's just a typo | Change to just "PASN" |

### Discussion:

* The cited text in the comment is:

= 

### Proposed Resolution: (8090)

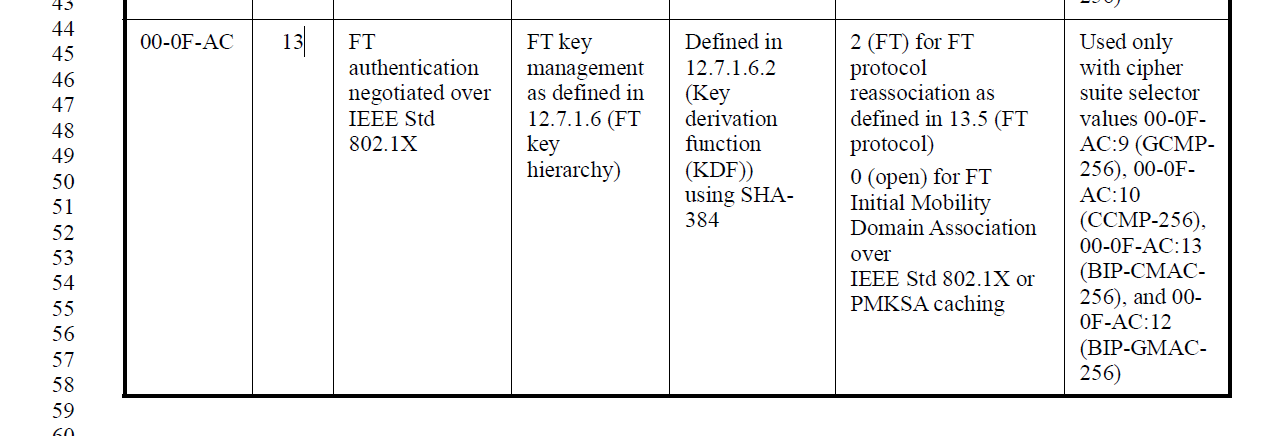
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8091 | 1024.00 | 9.4.2.23.3 |  |  | AKM :13 should be deprecated (cf. :22) | Below "13" in the second cell from the left add "(deprecated)" |

### Discussion:

* The cited text in the comment is:



* Presumably the commenter is trying to indicate that :13 is a duplicate of :22. :13 has a restriction on cipher suite selectors. The commenter provides no justification for deprecating the AKM

### Proposed Resolution: (8091)

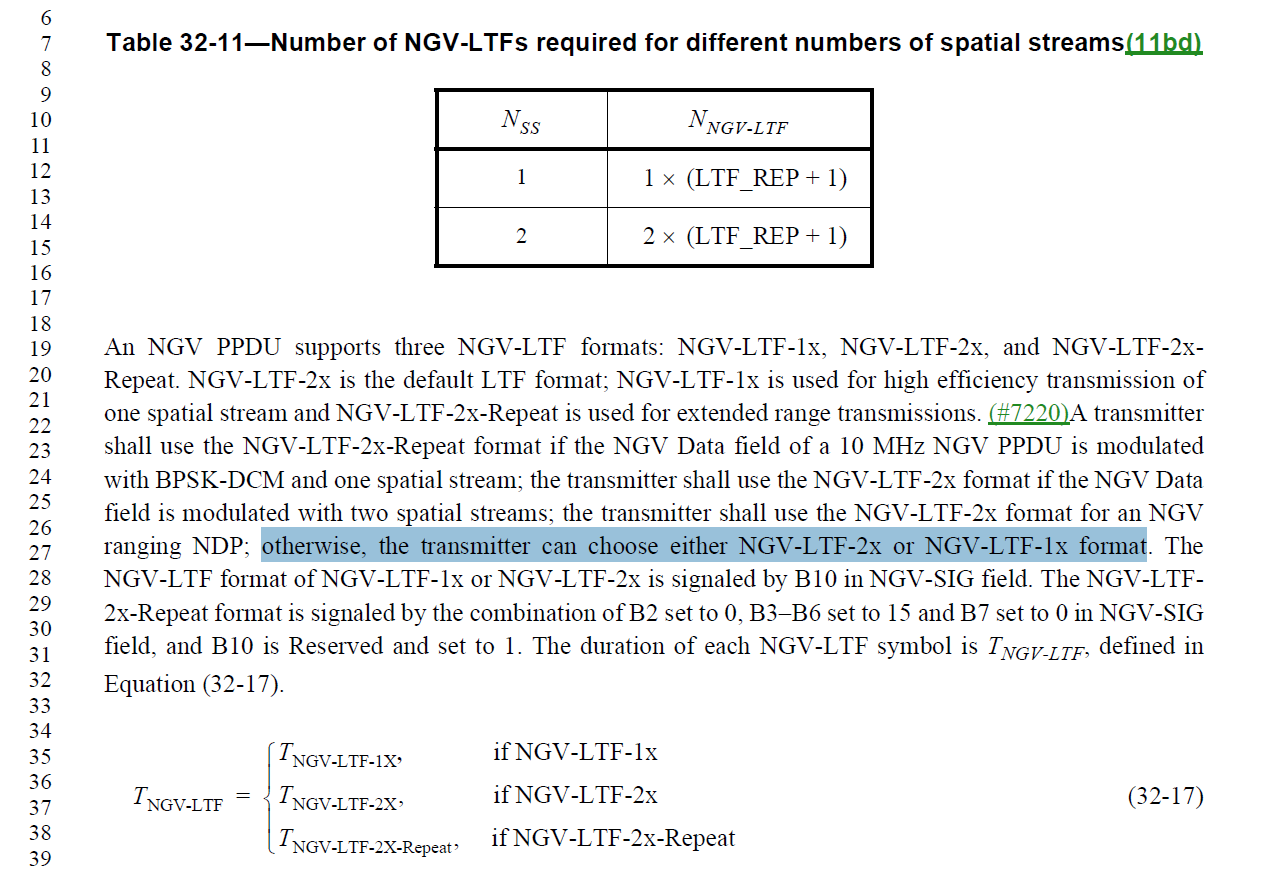
REJECTED. The AKM provides an FT AKM that uses SHA-384 with restrictions on cipher suite selectors. The commenter provides no justification for marking the AKM deprecated.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8147 | 4921.00 | 32.3.8.10 |  |  | "the transmitter can choose either NGV-LTF-2x or NGV-LTF-1x format" -- it has to choose one of them | Change to "… shall choose…" |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8147)

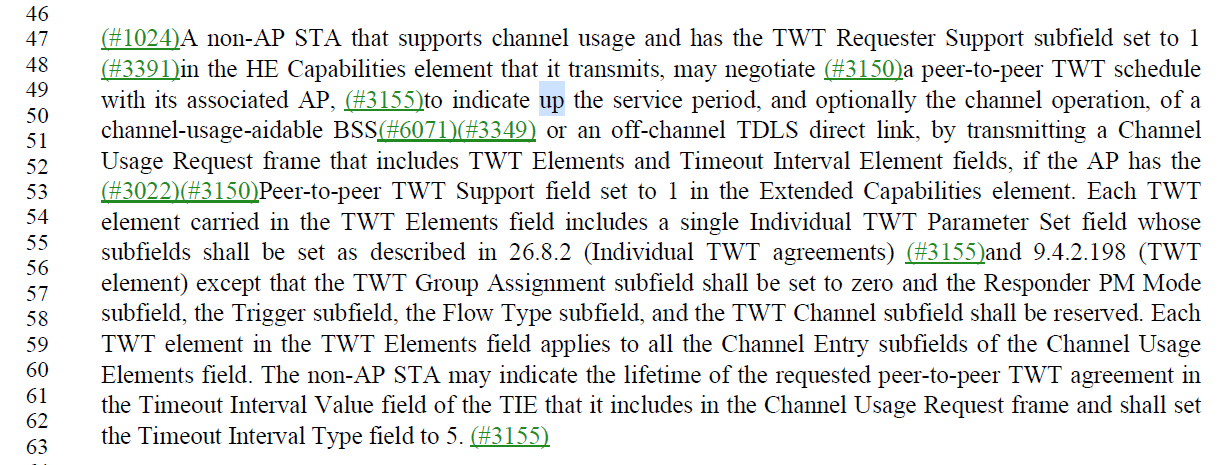
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8077 | 2788.00 | 11.21.15 |  |  | delete "up" | as in comment |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8177)

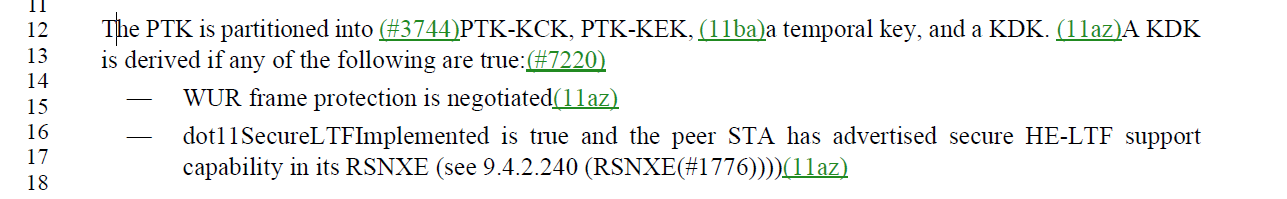
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8135 |  | 12 |  |  | "a KDK shall be derived if any of the following are true:(11az) — WUR frame protection is negotiated(11az) — dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support capability in its RSNXE (see 9.4.2.241 (RSN Extension element (RSNXE)))(11az); otherwise it shall not be derived. " is stated four times (3084.12, 3093.44, 3155.64, 3174.14) | Delete all but the first |

### Discussion:

* The cited text in the comment is:
* (3084.12)



* (3093.44)



* It looks like the most appropriate place to keep the text is 3093.44, but it should be a paragraph

### Proposed Resolution: (8135)

REVISED. Delete the cited text at 3084.12, 3155.64, and 3174.14

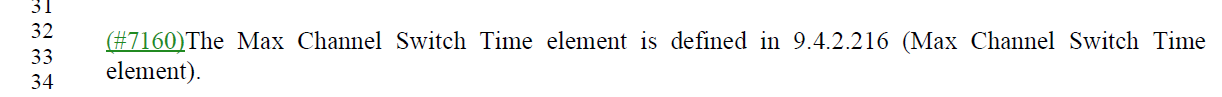
At 3093.44, add a line break to make the text a separate paragraph.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8094 | 1628.00 | 9.6.2.6 |  |  | "The Max Channel Switch Time element is defined in 9.4.2.216 " -- OK, but actually first need to say the the Max Channel Switch Time Element field contains this element | Prepend the sentence "The Max Channel Switch Time Element field, if present, contains a Max Channel Switch Time element." Also at 1654.38. Alternatively, change "Element" to "element" in Figure 9-1180—Channel Switch Announcement frame Action field format (2x) (cf. Figure 9-1193—Extended Channel Switch Announcement frame Action field format), though this is bending the conventions for content figures |

### Discussion:

* The cited text in the comment is:



* The cited text is also at 1654.38.

### Proposed Resolution: (8094)

REVISED. Prepend the cited sentence

Change “The Max Channel Switch Time element is defined"

To

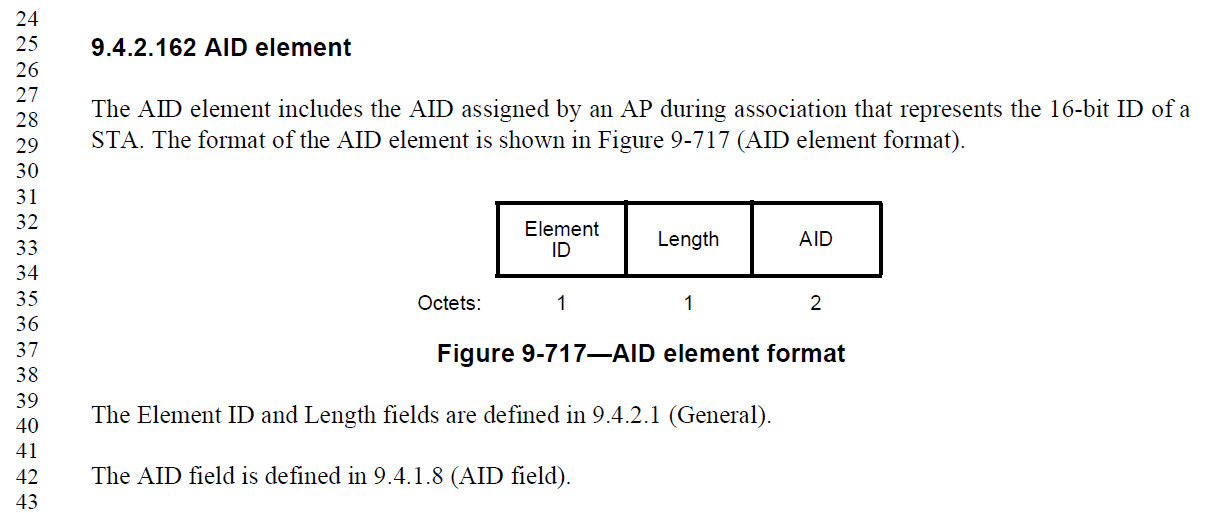
“The Max Channel Switch Time Element field, if present, contains a Max Channel Switch Time element as defined". Also make the same change at 1654.38.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8127 | 1292.00 | 9.4.2.162 |  |  | "The AID element includes the AID assigned by an AP during association that represents the 16-bit ID of a STA. " -- it doesn't just include it, that's all it includes. And size is in element. And AID is defined elsewhere Change to "The AID element contains the AID assigned by the AP during association." | As it says in the comment |

### Discussion:

* The cited text in the comment is:



* The commenter is suggesting a simplification to the first sentence.

### Proposed Resolution: (8127)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8121 |  |  |  |  | There are references to a "Full SSID", which is not a defined term | Delete at 1373.51 (2x), 1863 (7x), 2481.41, 3896 (2x) |

### Discussion:

* An example cited text is below:

A screenshot of a computer

Description automatically generated

* We typically avoid changing field names.

### Proposed Resolution: (8121)

REVISED. Change Full SSID to SSID when not referring to the field name.

At 1373.51, change “Full SSID” to “SSID” in third column.

At 1863.27, change “Full SSID” to “SSID” in the second occurrence.

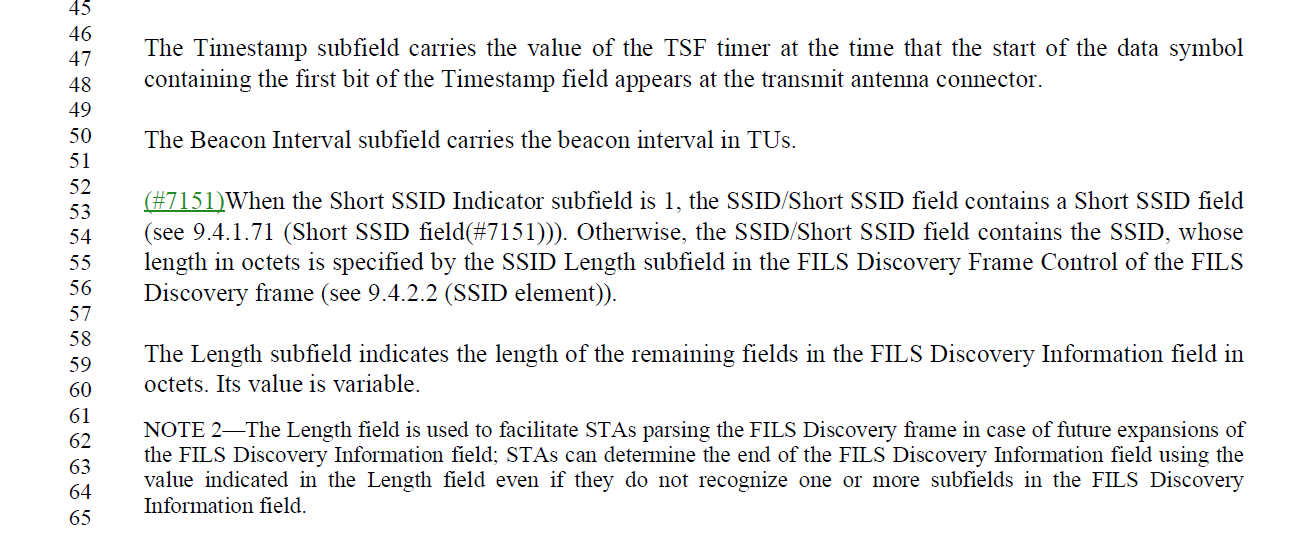
At 3896.7 and 3896.50, change “Full SSID” to “SSID”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8137 | 1684.00 | 9.6.7.36 |  |  | "Otherwise, the SSID/Short SSID field contains the SSID" -- does it contain the SSID or the SSID element (I think the former, but the xref is to the latter; also what if the SSID itself is zero-len?) | Add a "NOTE---The SSID/Short SSID field does not contain an SSID element." |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8137)

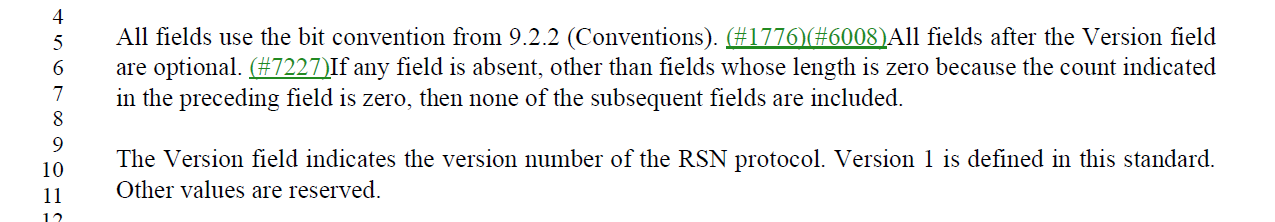
ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8103 | 1018.00 | 9.4.2.23.1 |  |  | "If any field is absent, other than fields whose length is zero because the count indicated in the preceding field is zero, then none of the subsequent fields are included." is still not very clear | Make it explicit: "If the Group Data Cipher Suite, Pairwise Cipher Suite Count, AKM Suite Count, RSN Capabilities or PMKID Count field is absent, then all of the subsequent fields are also absent." and mark the RSNE as not extensible |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8103)

ACCEPTED.

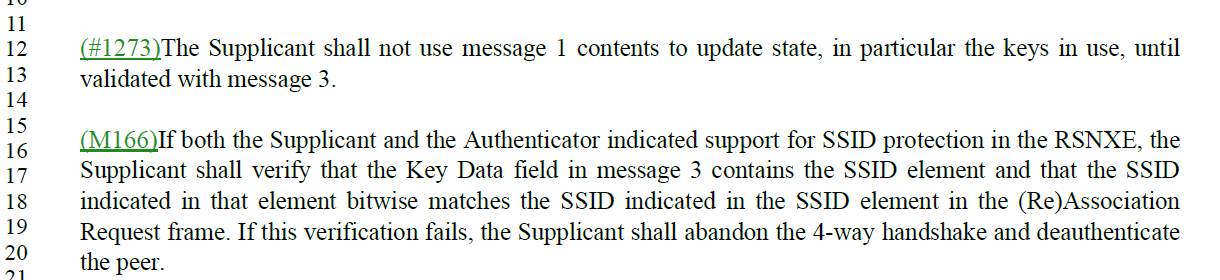
Note to Editor: Change the Extensible column value from “Yes” to “No” in Table 9-130.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8106 | 3117.00 | 12.7.6.6 |  |  | "the SSID indicated in that element bitwise matches the SSID indicated in the SSID element in the (Re)Association Request frame" -- the SSID is an opaque octet string anyway | Change to "the SSID element is the same as in the (Re)Association Request frame" |

### Discussion:

* The cited text in the comment is:



### Proposed Resolution: (8106)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8109 |  | 9.6 |  |  | There are references to MLME-FINETIMINGSMSMT and MLME-TIMINGSMSMT primitives, but these do not exist (in Clause 6) | Change "TIMINGSMSMT" to "TIMINGMSMT" (6x) |

### Discussion:

* The 6 locations are 1678.46, 1678.47 (x2), 1760.64, 1760.65 (x2)

### Proposed Resolution: (8109)

ACCEPTED

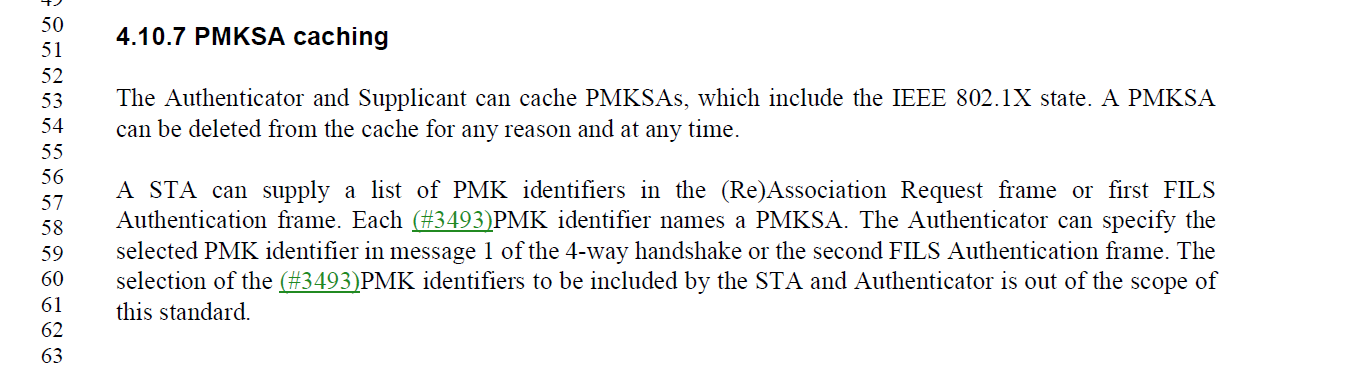
Note to Editor: The locations are 1678.46, 1678.47 (x2), 1760.64, 1760.65 (x2)

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8115 | 361.00 | 4.10.7 |  |  | "A PMKSA can be deleted from the cache for any reason and at any time." -- shouldn't that be a "may"? | As it says in the comment |

### Discussion:

* The cited text is



* Generally the style for clause 4 has been descriptive. Likely that’s why its “can”. Normative requirements are given in Clause 12.

### Proposed Resolution: (8109)

ACCEPTED

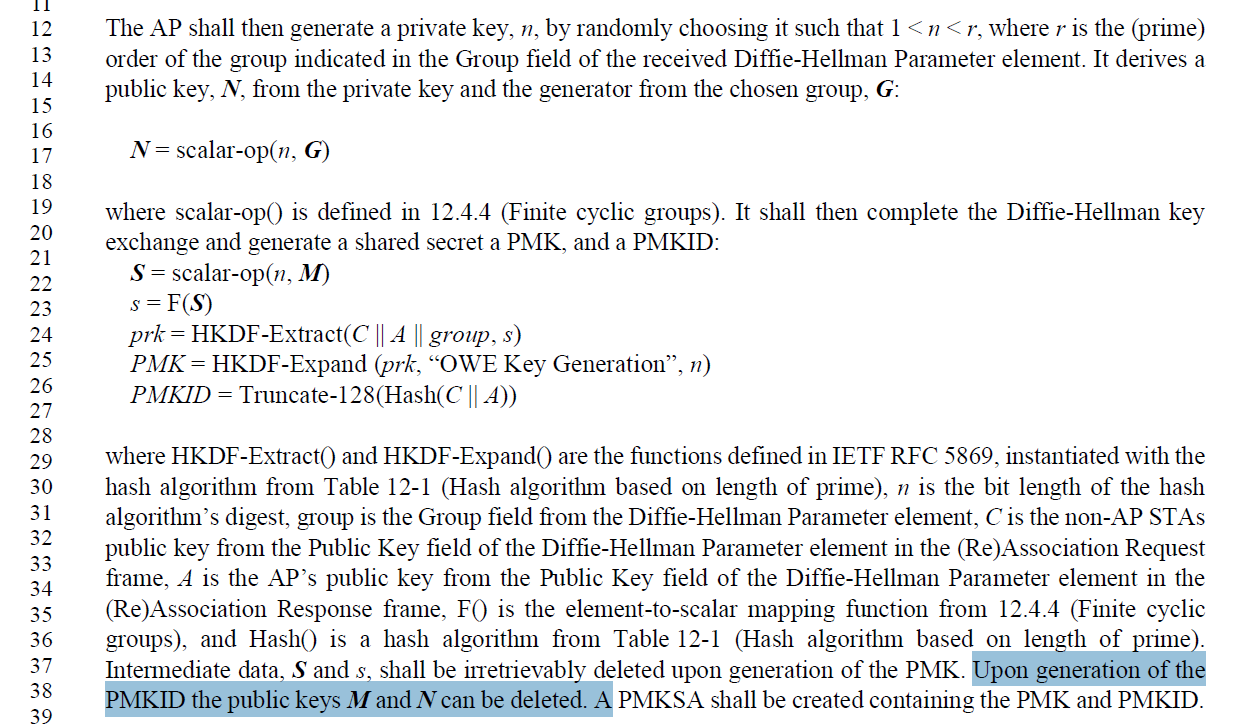
Note to Editor: The locations are 1678.46, 1678.47 (x2), 1760.64, 1760.65 (x2)

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8116 | 3176.00 | 12.14.2 |  |  | "Upon generation of the PMKID the public keys M and N can be deleted. " should be "… may be deleted." Ditto at 3177.14 | As it says in the comment |

### Discussion:

* The cited text is



### Proposed Resolution: (8116)

ACCEPTED

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8224 | 5719.00 | C.3 |  |  | It's not clear how you can have 0 taps | Change to 1 here and at line 12 |
| 8223 | 5719.00 | C.3 |  |  | dot11ChanMeasFBCKNtaps -- err, I don't think you can have 64 million taps | How about 65535 or 255 taps? |

### Discussion:

* The cited text in context is as follows:

A computer screen shot of text

Description automatically generated

* Other text of note:

A screenshot of a computer

Description automatically generated

A close-up of a text

Description automatically generated

* The default value and the range were specified in IEEE 802.11ad-2012 and was not modified by 11ay.
* Feedback from Assaf:

  The dot11ChanMeasFBCKNtaps cannot be 0, because the FBCK-TYPE field description says

|  |
| --- |
| Number of taps in each channel measurement:0 x 0 – 1 tap0 x 1 – 4×*NCB*+ 1 taps(11ay)0 x 2 – 14×*NCB*+ 1 taps(11ay)0 x 3 – 62×*NCB*+ 1 taps(11ay) |

so in 11ad the valid values were 1,5,15, and 63.  In 11ay these values are extended to be 1, 5,9,13,17, 15,29,43, 57, 63, 125, 187 and 249.

Limitting dot11ChanMeasFBCKNtaps to 1..255 will probably be fine.

### Proposed Resolution:

**(8224)** ACCEPTED

**(8223)** REVISED. Make changes in line with those provided by the commenter. At 5719.21, change “64000000” to “255”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8221 | 5717.00 | C.3 |  |  | The description for dot11BFTXSSTime has no mention of BF | As it says in the comment |

### Discussion:

* The cited text is

### 

* See Figure 10-107

### Proposed Resolution: (8221)

REVISED. At 5717.26, change “non-AP STA” to “non-AP STA for a transmit sector sweep”.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8092 | 1024.00 | 9.4.2.23.3 |  |  | There is no AKM for FT with .1X and SHA-1 (cf. 00-0f-ac:1 for .1X with SHA-1) | Add a selector for this |
| 8093 | 1024.00 | 9.4.2.23.3 |  |  | There is no AKM for FT with PSK with SHA-256 (cf. 00-0f-ac:6 for PSK with SHA-256) | Add a selector for this |

### Discussion:

* For CID 8092, P802.11r was the first project in IEEE 802.11 to introduce the use of SHA-256 for AKMs. As a result, there were no FT AKMs defined to support SHA-1.
* From context, CID incorrectly asks for SHA-256 when it was intended to ask for an FT AKM for SHA-1.

### Proposed Resolution: (8092, 8093)

REJECTED. There are no AKMs using SHA-1 defined for FT due to concerns with security vulnerabilities associated with SHA-1. SHA-1 has been deprecated by NIST so there is no need to add the AKM.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8008 |  |  |  |  | Preview and Safari for Apple Macintosh render some (non-ASCII) symbols incorrectly. For example, Subclause 12.7.1.6.2, Page 3083, Lines 7-26: Preview displays Greek letters where other symbols are expected. |  |

### Discussion:

* None.

### Proposed Resolution: (8008)

REJECTED. This standard will be professionally edited prior to publication. The issue will be brought to the attention of the publication editor.

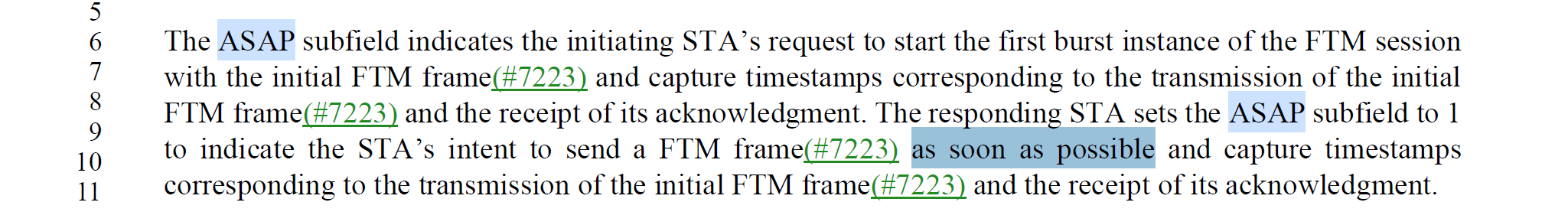
Note: The referenced text is page 3090, lines 20-35 (left arrow is displayed incorrectly).

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8011 |  |  |  |  | “ASAP” should be listed in the acronyms section. | As in comment |

### Discussion:

* ASAP stands for “as soon as possible”. Do we really need an acronym?



### Proposed Resolution: (8011)

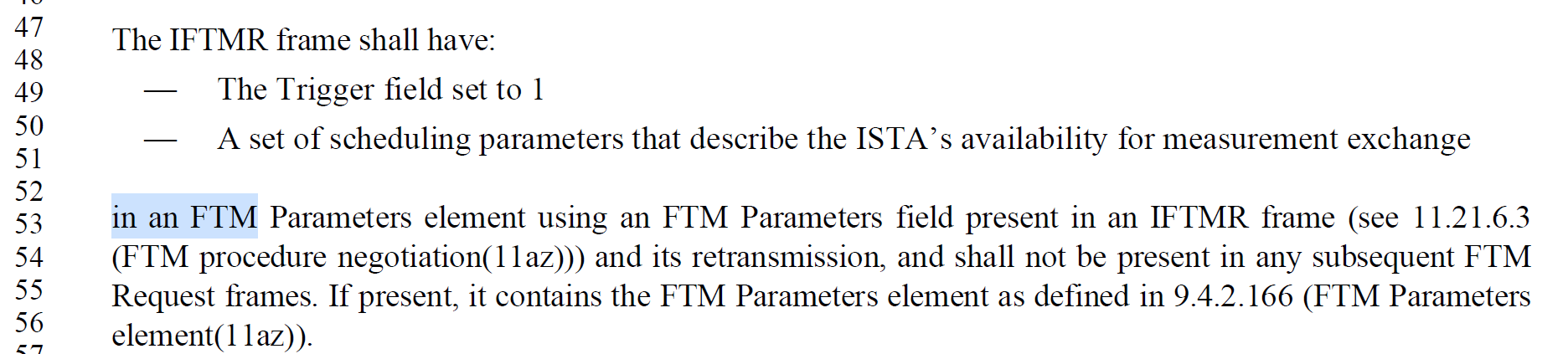
REJECTED. ASAP is only used as a field name.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8013 | 2727.00 |  |  |  | “in an FTM …” should begin with a capital letter. It seems to be part of the bulleted list above or a separate paragraph. | Restructure the sentence to eliminate the list. The formatting is confusing to see the list and the text continue. |

### Discussion:

* The location is on page 2707, not 2727 and is shown here.



### Proposed Resolution: (8013)

REVISED. Change the cited paragraph as shown in <this> under “Proposed Resolution: (8013)”:

***Restructure the cited paragraphs as follows:***

“The IFTMR frame (see 11.21.6.3 (FTM procedure negotiation(11az)) and its retransmission(s) shall include an FTM Parameters element (see 9.4.2.166 (FTM Parameters element(11az))) with:

— the Trigger field set to 1, and

— a set of scheduling parameters that describe the ISTA’s availability for measurement exchange, in the FTM Parameters field.

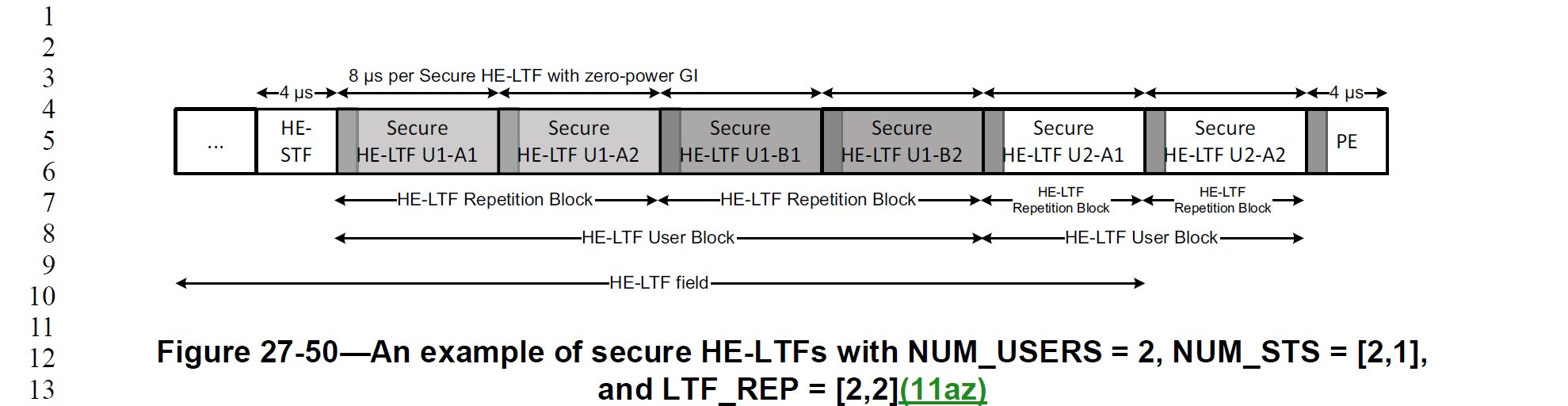
The FTM Parameters field shall not be present in any subsequent FTMR frames.”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8014 | 4398.00 |  |  |  | Subclause 27.3.19.1, Page 4398, Figure 27-50: The double-headed arrow for the HE-LTF field appears to be incorrectly left shifted. | Shift to right |

### Discussion:

* The cited figure is shown here:



### Proposed Resolution: (8014)

ACCEPTED

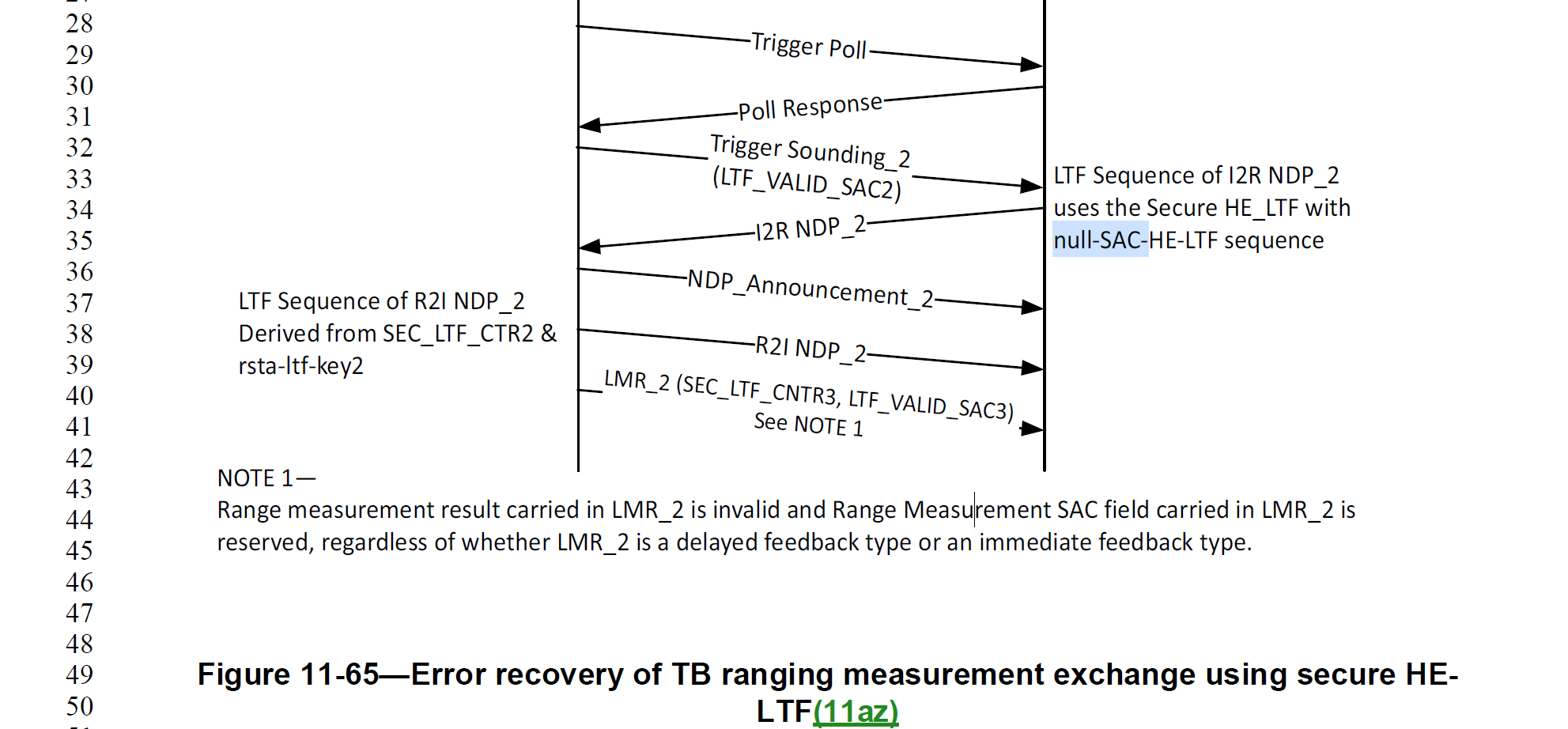
Note to Editor: Shift the HE-LTF field arrow to align with the beginning of Secure HE-LTF U1-A1 and to the end of Secure HE-LTF U2-A2.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8015 | 2751.00 |  |  |  | Change "null-SAC" to "Null-SAC" | As in comment |

### Discussion:

* The cited text is:



* The “null-SAC-…” should be “Null-SAC-…” in figure 11-65 and figure 11-67 (2x)

### Proposed Resolution: (8015)

REVISED. Change “null-SAC” to “Null-SAC” in Figure 11-65 (2751.35) and Figure 11-67 (2755.28 and 2755.29)

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8019 | 2747.00 |  |  |  | In the text for LMR\_1 SEC…there is a missing open parenthesis before "SEC" . See the parenthesis placement in LMR\_2 line 40 for an example to match. | Add the missing open parenthesis. |

### Discussion:

* The cited text is in Figure 11-64

A close-up of a graph

Description automatically generated

### Proposed Resolution: (8019)

ACCEPTED.

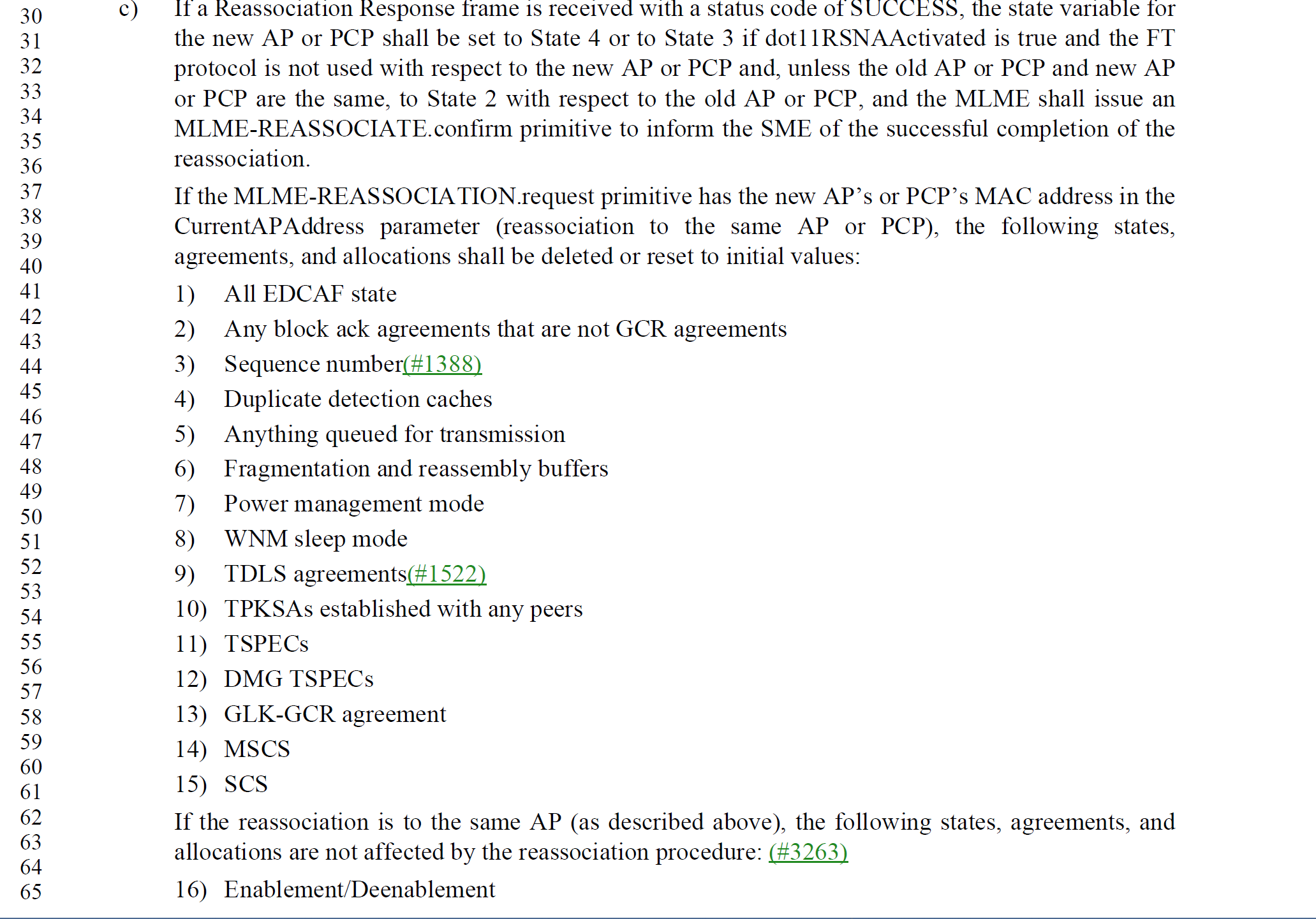
Note to Editor. The cited text is in Figure 11-64. At cited location, change “LMR\_1 SEC..” to LMR\_1 (SEC…”

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8233 | 2258.00 | 11.3.5.4 |  |  | 11.3.5.4 c) should list the PMKSA as something that "is reset" at same AP reassociation. | Add PMKSA to the first list, here (as new item 16?) and renumber the list below. |

### Discussion:

* The cited text is shown in context



### Proposed Resolution: (8233)

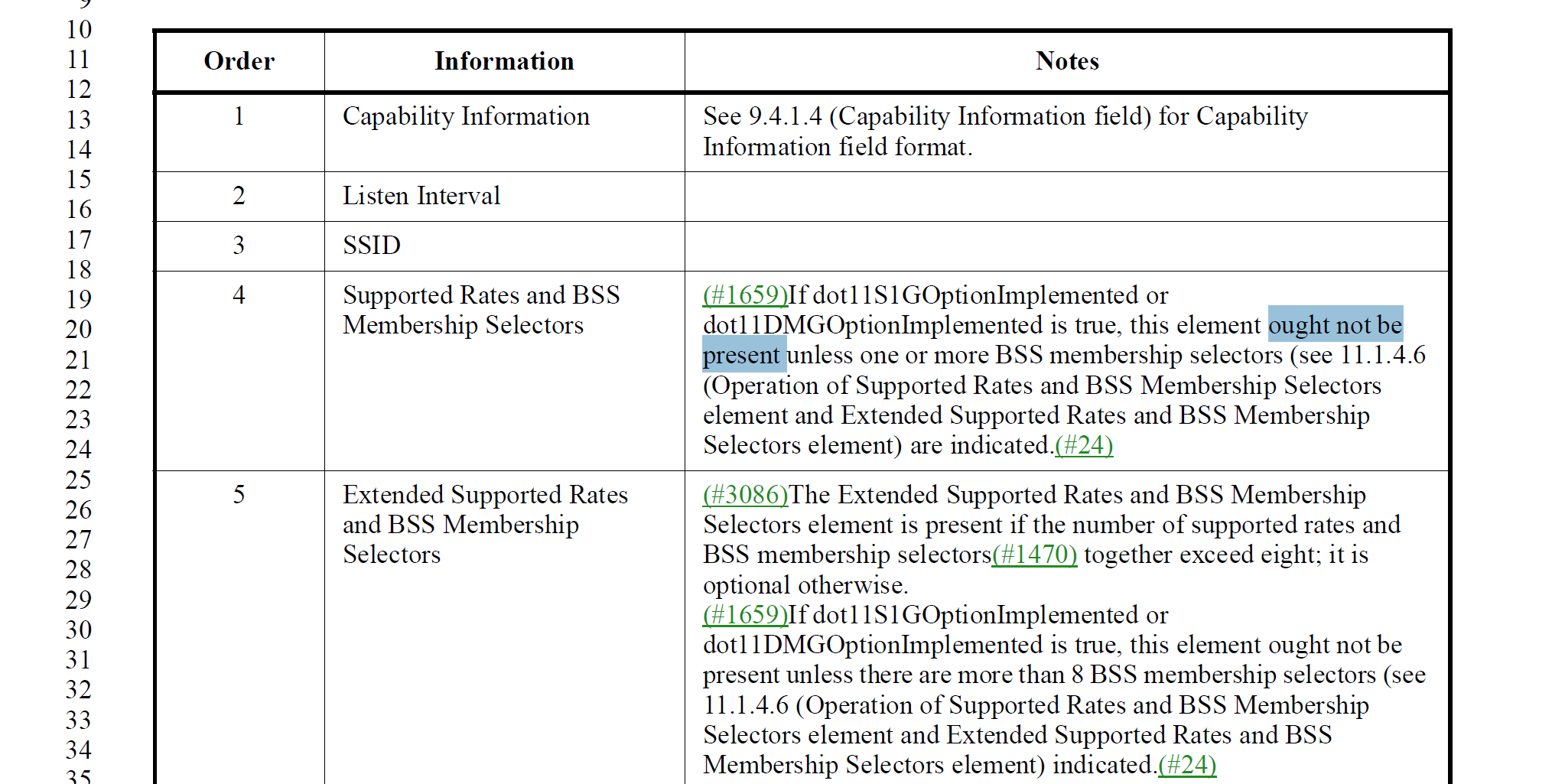
REJECTED. PMKSA is not reset under these conditions. The PTKSA (and possibly the PMKSA) would be established in the transition from State 3 to State 4.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8229 | 740.00 | 9.3.3.5 |  |  | What does "ought" mean in this context (738.20, D5.0)? "Should"?? "Shall"?? Something non-normative?? Also, this is already stated in 11.1.4.6, "An S1G or CMMG STA should not include supported rates in frames it transmits since its MCS capabilities are indicated in its Capabilities element." Make this an understandable xref. Same thing at P740.31, P743.57, P744.11, P748.48, P748.59, P754.17, P754.28, P759.16, P759.29, P762.16, and P763.11. | At P740.19, P743.56, P748.47, P754.16, P759.15, and P762.14, replace the entire content of the Notes box, with "See 11.1.4.6 for details on the inclusion of this element when dot11S1GOptionImplemented or dot11DMGOptionImplemented is true. At P740.30, P744.10, P748.58, P754.27, P759.27, and P763.10, replace the similar sentence in the Notes box, with the same change. |

### Discussion:

* The cited text in context is



* The commenter is asking for the following:

Change

“If dot11S1GOptionImplemented or dot11DMGOptionImplemented is true, this element ought not be present unless there are more than 8 BSS membership selectors (see 11.1.4.6 (Operation of Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element) indicated.(#24)

To

“See 11.1.4.6 for details on the inclusion of this element when dot11S1GOptionImplemented or dot11DMGOptionImplemented is true.”

### Proposed Resolution: (8229)

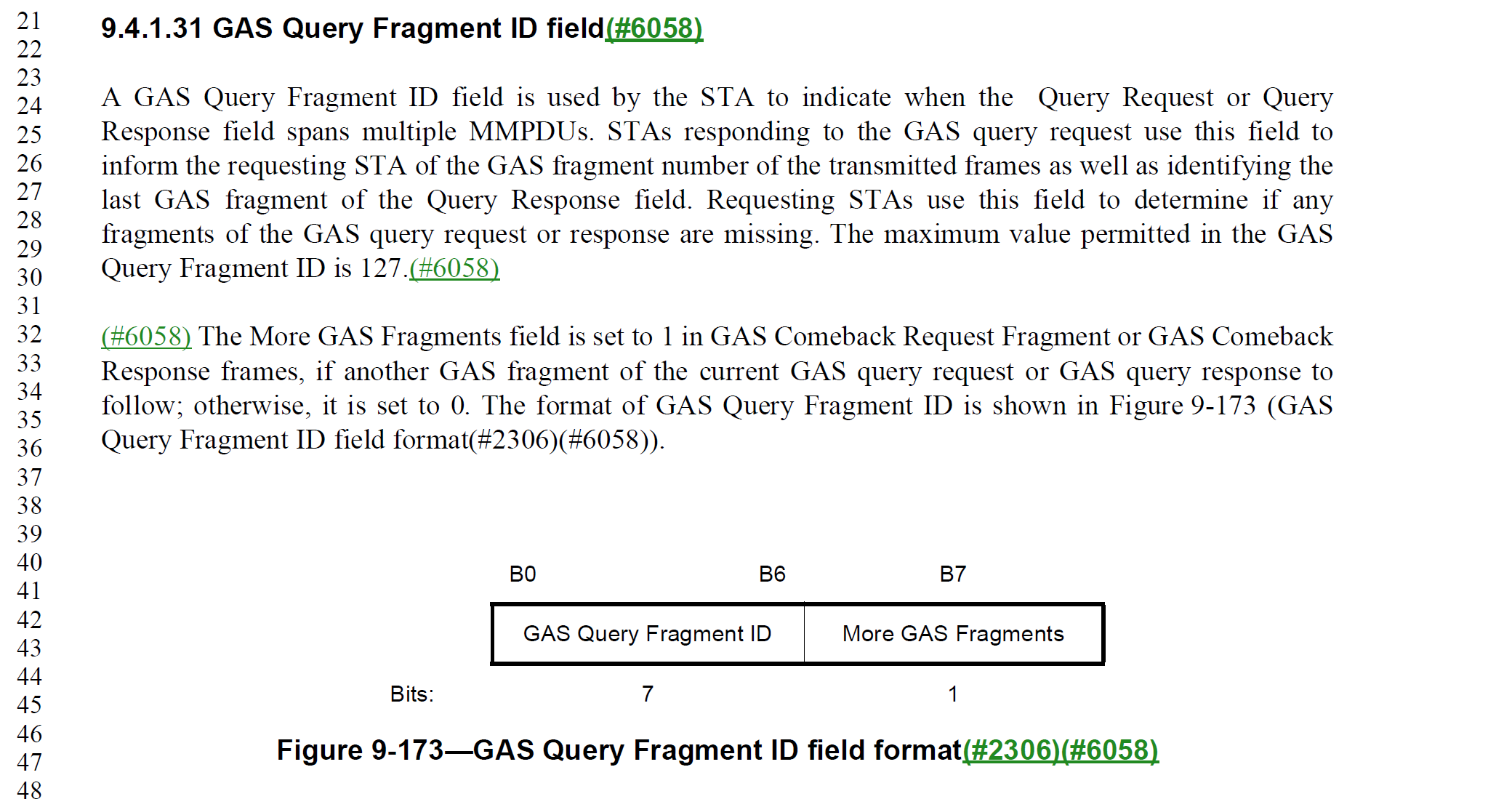
ACCEPTED or REJECTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8184 | 825.00 | 9.4.1.31 |  |  | It's very confusing for the GAS Query Fragment ID field to have a GAS Query Fragment ID (sub)field, especially since the contents of the latter are not described. Also "The format of GAS Query Fragment ID is shown in Figure 9-173 (GAS Query Fragment ID field format(#2306)(#6058))." is missing "the" and "field" | Rename the subfield to something else, and describe what it contains |

### Discussion:

* The cited text in context



### Proposed Resolution: (8184)

REVISED.

Change the sentence at P825L34 to “The format of the GAS Query Fragment ID field is shown in Figure 9-173”.

Change the “GAS Query Fragment ID” in Figure 9-173 to “GAS Fragment ID”.

Change “Fragment ID” to “GAS Fragment ID” at P1662L1 and P1663L8.

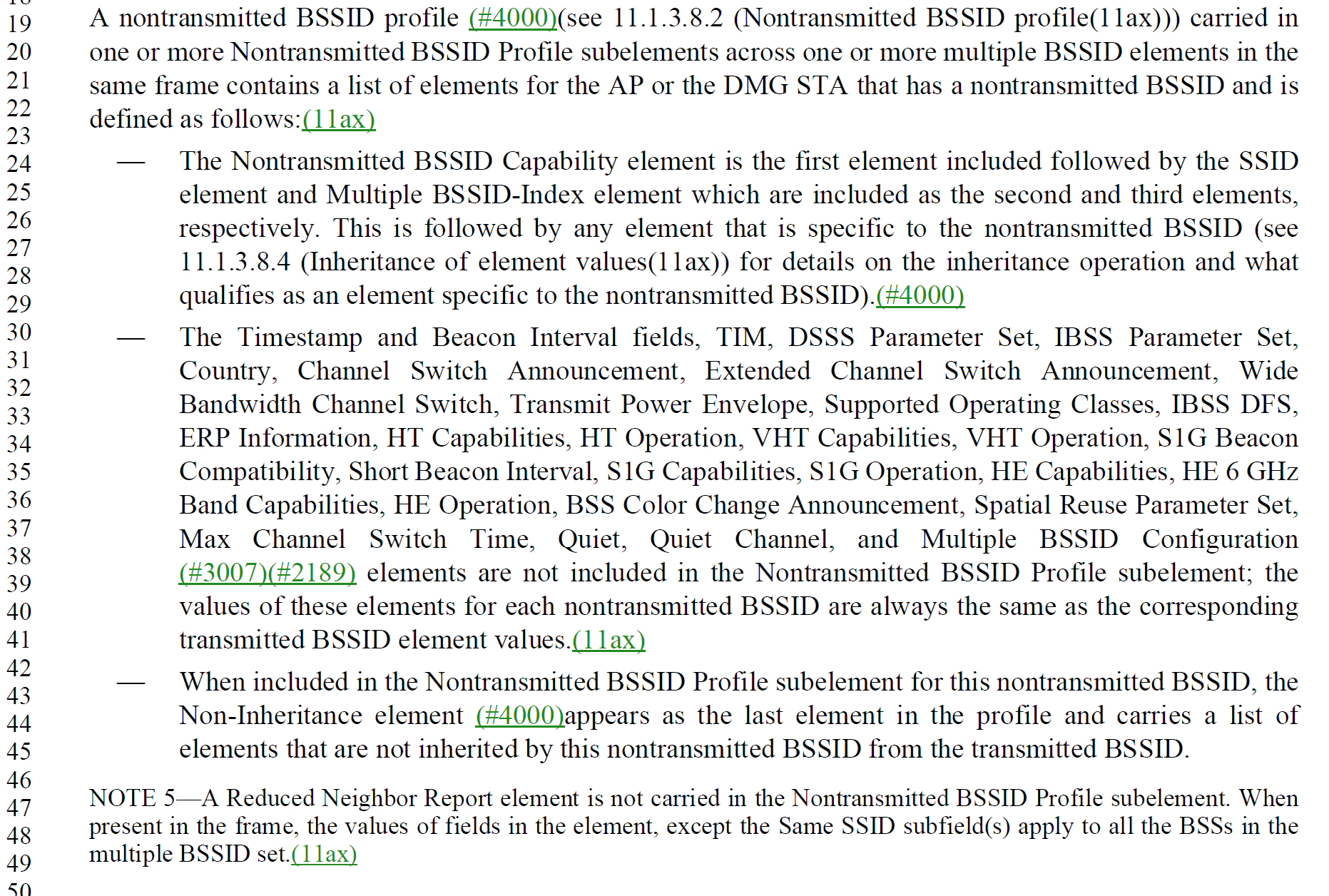
Insert the following text as a second paragraph in Clause 9.4.1.31 (P825L31) “The GAS Fragment ID field contains the value of the GAS fragment”.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8038 | 1087.00 | 9.4.2.44 |  |  | The following note "NOTE 5—A Reduced Neighbor Report element is not carried in the Nontransmitted BSSID Profile subelement. When present in the frame, the values of fields in the element, except the Same SSID subfield(s) apply to all the BSSs in the multiple BSSID set." creates confusion on how inheritance work for reduced neighbore report, which has the following "shall" requirement. "(#4)If an element, identified by (#3195)Element ID and Element ID Extension fields (if applicable), is carried in a Probe Response frame, Beacon frame, DMG Beacon frame, or S1G Beacon frame transmitted by an AP corresponding to the transmitted BSSID and there is no element having the same Element ID and Element ID Extension (if applicable) present in a nontransmitted BSSID profile, and the element is not listed in the NonInheritance element (if included) in the nontransmitted BSSID profile for that BSS, then a non-AP STA receiving the frame shall consider the element to be part of that nontransmitted BSSID’s profile and the contents of the Information field shall apply to the nontransmitted BSSID. Otherwise, a non-AP STA receiving the frame shall not consider the element to be part of the nontransmitted BSSID profile." If reudced neighbore report is indicated as inherited, then it conflicts with the note saying Same SSID does not apply to nontransmitted BSSID. If reudced neighbore report is indicated as noninherited, then it conflicts with the note saying every field except Same SSID apply to nontransmitted BSSID. Propose change to clarify that indication of inheritance does not apply for reduced neighbor report. [Po-Kai] | In page 2464 L31, change "Otherwise, a non-AP STA receiving the frame shall not consider the element to be part of the nontransmitted BSSID profile." to "Otherwise, for an element except Reduced Neighbor Report element, a non-AP STA receiving the frame shall not consider the element to be part of the nontransmitted BSSID profile." In page 2464 L31, change "If an element, identified by (#3195)Element ID and Element ID Extension fields (if applicable), is carried in a Probe Response frame, Beacon frame, ..." to "If an element except Reduced Neighbor Report element, identified by (#3195)Element ID and Element ID Extension fields (if applicable), is carried in a Probe Response frame, Beacon frame," Add the following sentence in P2464 L33, "For Reduced Neighbor Report element, the element is neither inherited nor non-inherited. A Reduced Neighbor Report element shall not be carried in the Nontransmitted BSSID Profile subelement. When present in the frame, the values of fields in the element, except the Same SSID subfield(s) apply to all the BSSs in the multiple BSSID set, and the Same SSID subfield(s) is interpreted with respect to the Transmitted BSSID." In P1087L 47, add "In addition, the Same SSID subfield(s) is interpreted with respect to the Transmitted BSSID. See 11.1.3.8.4." |

### Discussion:

* The cited text in context is



* The comment proposes making changes to 11.1.3.8.4 which describes normative requirements for inheritance. The changes are:

In page 2464 L31, change

"Otherwise, a non-AP STA receiving the frame shall not consider the element to be part of the nontransmitted BSSID profile."

to

"Otherwise, for an element except Reduced Neighbor Report element, a non-AP STA receiving the frame shall not consider the element to be part of the nontransmitted BSSID profile."

In page 2464 L31, change

"If an element, identified by (#3195)Element ID and Element ID Extension fields (if applicable), is carried in a Probe Response frame, Beacon frame, ..."

to

"If an element except Reduced Neighbor Report element, identified by (#3195)Element ID and Element ID Extension fields (if applicable), is carried in a Probe Response frame, Beacon frame,"

Add the following sentence in P2464 L33,

"For Reduced Neighbor Report element, the element is neither inherited nor non-inherited. A Reduced Neighbor Report element shall not be carried in the Nontransmitted BSSID Profile subelement. When present in the frame, the values of fields in the element, except the Same SSID subfield(s) apply to all the BSSs in the multiple BSSID set, and the Same SSID subfield(s) is interpreted with respect to the Transmitted BSSID."

In P1087L 47 (in clause 9), add "In addition, the Same SSID subfield(s) is interpreted with respect to the Transmitted BSSID. See 11.1.3.8.4."

### Proposed Resolution: (8038)

REJECTED. Commenter has withdrawn the comment.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8125 | 3098.00 | 12.7.2 |  |  | CID 7027 change "In an EAPOL-Key request frame, the Secure bit is set to 1, the Key MIC Present bit is set to 1 if not using an AEAD cipher and is set to 0 otherwise, and the Install bit is is set to 0. " has left the setting of the Encrypted Key Data bit undefined | As it says in the comment |

### Discussion:

* The cited text in context is:

A close up of a text

Description automatically generated

* The setting of the Encrypted Key Data description was removed in the resolution to CID 8125 to clarify the EAPOL-Key request settings. The Encrypted Key Data subfield setting is defined and is dependent whether the AEAD cipher is being used (see 3101.19).
* Response from Jouni Malinen with respect to this CID: “*Encrypted Key Data is set to 1 whenever using AEAD ciphers (i.e., the FILS cases) if the PTK is available. This includes cases where there is no actual plaintext Key Data contents, i.e., also the EAPOL-Request frame case. The text that was added in an earlier REVme draft broke this and that’s why I asked this conflicting definition to be removed. Sure, we could come up with even more complex language here to describe all different variants, but I don’t think that is valuable use of our time and as such, that “removal of information” is the best approach here.”*

### Proposed Resolution: (8125)

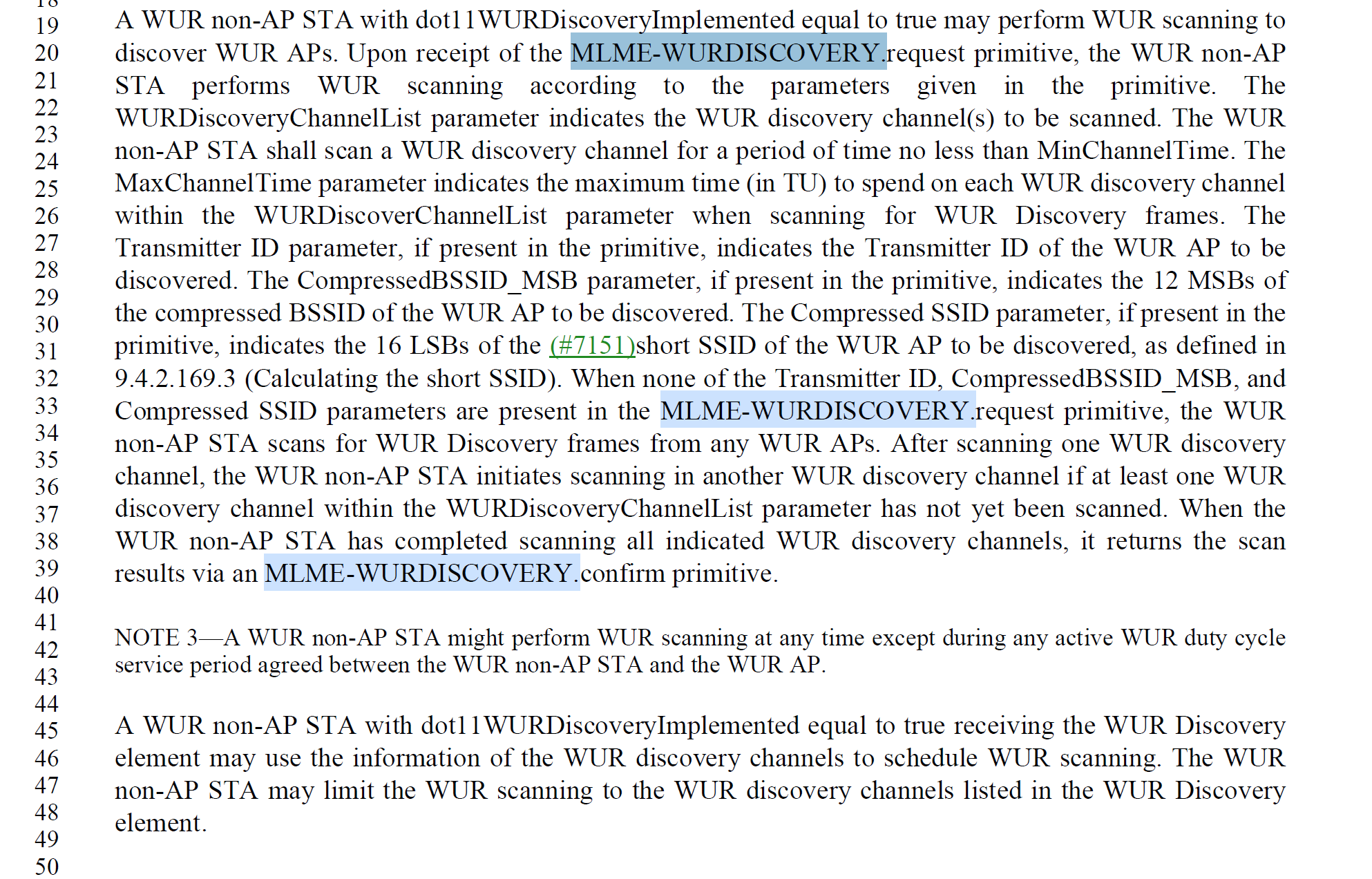
REJECTED. The setting of the Encrypted Key Data field is defined in the EAPOL-Key request and as with other EAPOL-Key frames, it is dependent on the presence of Key Data and whether the AEAD cipher is negotiated as part of the AKM.

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8139 | 4842.00 | 29.12 |  |  | There are references to MLME-WURDISCOVERY primitives, with various parameters, but these parameters are not given anywhere (not in C6) | As it says in the comment |

### Discussion:

* The cited text in context:



And from clause 6:

A screenshot of a computer

Description automatically generated

### Proposed Resolution: (8139)

REVISED. Restore the MLME primitives for WUR Discovery.

Restore the clause and subclauses from REVme D1.0 clause 6.3.125 (page 843) into the current draft as a clause and subclauses following 6.5.24.

In Table 6-1 at 403.48 for WUR Discovery, change the text in the References to include the new WUR Discovery clause 6.5.25

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 8174 | 3128.00 | 12.7.8.4.3 |  |  | (#6149)If the (#3488)Information field of the RSNE, with the exception of the pairwise cipher suite count and pairwise cipher suite list, is not the same as that sent by the TDLS initiator STA in mes-sage 1 of this sequence, then the TDLS initiator STA shall reject the response with status code INVALID\_RSNE. -- also need to ignore the version as it could in theory differ (see above "(#3241)The Version field shall be set to the minimum of the maximum version supported by the TDLS responder STA and the version number received in the RSNE of message 1(#6163).") | Change to "… with the exception of the version, pairwise cipher suite count …" |
| 8175 | 3128.00 | 12.7.8.4.3 |  |  | (#6149)If the (#3488)Information field of the RSNE, with the exception of the pairwise cipher suite count and pairwise cipher suite list, is not the same as that sent by the TDLS initiator STA in mes-sage 1 of this sequence, then the TDLS initiator STA shall reject the response with status code INVALID\_RSNE. -- count has to be 1 anyway so can delete the "with the exception" bit | Delete ", with the exception of the pairwise cipher suite count and pairwise cipher suite list," |

### Discussion:

* As CID 8174 says, the Version field could (in theory) differ between T1 and T2, though presumably version 0 is not valid.
* As CID 8175 says, the pairwise cipher list in T1 now only contains a single selector.The comment appears to be a set of locations with no comment or a proposed change.

### Proposed Resolution: (8174, 8175)

REVISED. Change

“(#6149)If the (#3488)Information field of the RSNE, with the exception of the pairwise cipher suite count and pairwise cipher suite list, is not the same as that sent by the TDLS initiator STA in message 1 of this sequence, then the TDLS initiator STA shall reject the response with status code INVALID\_RSNE.”

to

“(#6149)If the (#3488)Information field of the RSNE, is not the same as that sent by the TDLS initiator STA in message 1 of this sequence, except that the version may be lower as long as it is nonzero, then the TDLS initiator STA shall reject the response with status code INVALID\_RSNE.”