IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D0.4 CR for 12.14.4 |
| Date: 2024-07-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

1155, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434,

1435, 1436, 1437, 1438, 1439, 1440, 1441, 1181, 1390, 1393,

1394, 1395, 1396, 1397, 1398, 1399, 1183, 1129, 1179, 1182,

1193, 1195, 1036, 1037, 1038, 1039, 1040, 1207, 1208, 1209,

1130, 1047, 1196, 1197, 1220, 1210, 1211, 1212, 1403, 1213,

1214, 1215, 1216, 1219, 1221, 1226, 1194, 1149, 1228

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Editorial fix for CID number
* Rev 2: Changes based on the discussion durin the teleconference call
* Rev 3: Revision based on the disucsion during the teleconference call

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D0.4 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.4 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1155 | Po-Kai Huang | 12.14.4 | 74.09 | Clarify what is the algorithm number of the authentication frame | As in comment | Rejected – This is already clarified in the first bullet of each Authenticaton frame constricuton.  |
| 1426 | Mark RISON | 12.14.4 | 74.63 | "supports IEEE 802.1X Authentication Utilizing Authentication Frame" case and articles wrong | As it says in the comment | Revised – We ue the MIB dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated.TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1426 |
| 1427 | Mark RISON | 12.14 | 0.00 | I don't think introducing vague terminology like "authentication originator/responder" is a good idea. Stick to Authenticator/Supplicant and AP/non-AP STA | As it says in the comment | Rejected – We note that FT originator and FT responder are defined for FT. This is useful to generalize for MLO and non-MLO cases.  |
| 1428 | Mark RISON | 12.14.4 | 74.32 | "one 802.1X AKM" is weird. Change to "an 802.1X AKM" | As it says in the comment | Accetped –  |
| 1429 | Mark RISON | 12.14.4 | 74.40 | "The encapsulation field" -- field names start with uppercase letters. Also missing article in "carries EAPOL PDU" | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1429 |
| 1430 | Mark RISON | 12.14.4 | 74.42 | "Including the AKM Suite Selector element indicating the selected 802.1X AKM" is not a sentence | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1430 |
| 1431 | Mark RISON | 12.14.4 | 74.49 | "Validates that the selected 802.1X AKM indicated in AKM Suite Selector element is supported." -- why not just "Validates that the AKM indicated in the AKM Suite Selector element is supported."? | As it says in the comment | Revised –This authenticaton frame exchange using authentication algorithm number equal to <ANA> (IEEE 802.1X authentication). Hence, the AKM needs to be 802.1X AKM.We add one bullet to clarify this point.TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1431 |
| 1432 | Mark RISON | 12.14.4 | 74.51 | " Extracts EAPOL PDU" missing article | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1432 |
| 1433 | Mark RISON | 12.14.4 | 74.51 | "processes it according to the behaviordescribed in a later subclause specific to the AKMP." -- too vague. Also next page | Refer to specific subclauses | Revised –This is copied from PASN, where it has specific behavir for FT or FILS, etc. In our case, simply says process it. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1433 |
| 1434 | Mark RISON |   | 0.00 | Article frequently missing before "EAPOL PDU" | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1434 |
| 1435 | Mark RISON | 12.14.4 | 74.60 | "Status code indicates the processing status." should be "Status Code field..." Also next page | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1435 |
| 1436 | Mark RISON | 12.14.4 | 74.62 | "The Length of Encapsulation field indicates the length of the Encapsulation field." duplicates Clause 9. Also next page | Delete | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1436 |
| 1437 | Mark RISON | 12.14.4 | 75.01 | " Includes the AKM Suite Selector element indicating the selected 802.1X AKM indicated in the firstAuthentication frame." is rather waffly | Change to " Includes the same AKM Suite Selector element as in the firstAuthentication frame." | Revised –We change “the selected” to “the same”.TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1437 |
| 1438 | Mark RISON | 12.14.4 | 75.11 | "hat 802.1X AKM indicated in AKM Suite Selector elemen" missing articles and also 802.1X is superfluous | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1438 |
| 1439 | Mark RISON | 12.14.4 | 0.00 | This subclause repeatedly makes the same mistake, so please fix them all per comments made on the first part of the subclause | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1429, 1434, 1435, 1436 |
| 1440 | Mark RISON | 12.14.4 | 75.41 | "constructs the Authentication frame of the exchange [...] responder sends the Authentication frame" missing 2x "fourth"s | As it says in the comment | Revised –The paragraph is described for any of general value which is X+1, where X is larger than or equal to 3. This is needed because the number of authentication frame exchange depends on the EAP method.We add a note to clarify this point. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1440 |
| 1441 | Mark RISON | 12.14.4 | 75.55 | "(if needed by the EAP method)" not clear | Clarify | Revised –The paragraph is described for any of general value which is X+1, where X is larger than or equal to 3. This is needed because the number of authentication frame exchange depends on the EAP method.We add a note to clarify this point. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1440 |
| 1181 | Stephen McCann | 12.2.4 | 63.38 | Typo missing "IEEE" | Insert "IEEE" before "802.1X" at the cited location and P67L39, P67L43, P68L15, P68L19, P68L61, P69L7, P69L19, P69L61, P74L31 & P74L32. | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1181 |
| 1390 | Mark RISON | 12.2.4 | 63.32 | "or IEEE 802.1X authentication" -- I'm not sure this is correct, since it's in 4) below. If it is kept, then it should be a comma not or | As it says in the comment | Revised –Agree in principle with the commenter. Note that 4th bullet is 802.1X after association frame exchange. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1390 |
| 1393 | Mark RISON | 12.6.1.2.2 | 67.37 | "A non-DMG STA performing authentication with IEEE 802.1X authentication after using Open System authentication or 802.1X authentication utilizing Authentication frames." is not a valid sentence | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1393 |
| 1394 | Mark RISON | 12.6.1.2.2 | 67.60 | "authentication or IEEE 802.1X authentication utilizing Authentication frames or IEEE 802.1X" -- too many "or"s | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1394 |
| 1395 | Mark RISON | 12.6.7 | 68.38 | "carrying EAPOL PDU" should be "carrying EAPOL PDUs". Ditto line 41. And the "frame" in the parenthesis | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1395 |
| 1396 | Mark RISON | 12.6.7 | 68.47 | "EAPOL PDUs shall be carried in individually addressed MSDUs or individually addressed Authentication frames." -- I'm a bit worried this is too general. The auth frame option is only for EDPKE | As it says in the comment | Rejected – This represents the two options for performing 802.1X authentication.  |
| 1397 | Mark RISON | 12.6.8.1 | 69.18 | should not be sexless. Other locations too | As it says in the comment | Rejected –We note that this mimics the baseline texts ” *If a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a**member, a STA may signal its Supplicant to use IEEE Std 802.1X-2020 to preauthenticate with that**AP*” |
| 1398 | Mark RISON | 12.6.8.1 | 69.18 | "If a STA's MLME-SCAN.confirm primitive finds another AP" -- primitives don't find anything | Change to "includes". Also delete "another" and just say "an" | Rejected –We note that this mimics the baseline texts ” *If a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a**member, a STA may signal its Supplicant to use IEEE Std 802.1X-2020 to preauthenticate with that**AP*” |
| 1399 | Mark RISON | 12.6.8.1 | 69.19 | "advertises support for 802.1X authentication" too vague. It's specifically about IEEE 802.1X Authentication UtilizingAuthentication Frame Support, no? | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1399 |
| 1183 | Mark RISON | 3.2 | 19.09 | EAPOL-Start Authentication frames are defined but their behaviour is essentially unspecified (just a vague hint in 4.10.3.2) | Add some behavioural detail to Clause 12 | Rejected –We note that this is the same amount of details as defined in the baseline for EAPOL-Start frame. |
| 1129 | Po-Kai Huang | 4.2.5 | 21.18 | change "or as MMPDU within one or more Authentication frames" to "or are carried within Authentication frames" because the EAPOL PDU are just part of the management frame body rather than the whole management frame body | As in comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1129 |
| 1179 | Stephen McCann | 4.2.5 | 21.18 | Typo "MMPDU" | Change "MMPDU" to "MMPDUs" | Revised –We change "or as MMPDU within one or more Authentication frames" to "or are carried within Authentication frames" because the EAPOL PDU are just part of the management frame body rather than the whole management frame bodyTGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1129 |
| 1182 | Mark RISON | 4.2.5 | 21.16 | "EAPOL PDUs are carried as MSDUs within one or more Data frames or as MMPDU" should be "... or as MMPDUs" | As it says in the comment | Revised –We change "or as MMPDU within one or more Authentication frames" to "or are carried within Authentication frames" because the EAPOL PDU are just part of the management frame body rather than the whole management frame bodyTGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1129 |
| 1193 | Mark RISON | 4.2.5 | 21.17 | "EAPOL PDUs are carried [...] as MMPDU within one or more Authentication frames" -- it is not clear how this can be done | Give a xref | Revised –We change "or as MMPDU within one or more Authentication frames" to "or are carried within Authentication frames" because the EAPOL PDU are just part of the management frame body rather than the whole management frame body. We also provide reference.TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1193 |
| 1195 | Mark RISON | 4.5.3.3 | 21.39 | "an IEEE 802.1X authentication procedure completes successfully over the Authentication frame exchanges carrying EAPOL PDUs (if using IEEE 802.1X authentication utilizing Authentication frame) and the IEEE 802.1X Uncontrolled Port" is very confusing. Similarly at 22.24 | Change to "an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port or using Authentication frame exchanges carrying EAPOL PDUs" | Revised –Essentially all EAPOL PDUs go to uncontrolled port independent of carrying in data frame or authenticaton frame. To avoud confusion, we just delete the addition. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1195 |
| 1036 | Bo Sun | 4.5.4.2 | 21.60 | 11bi doesn't define "802.1X authentication". Instead, it's defined in IEEE 802.1X. 11bi only defines or extends the definition of how to use "802.1X authentication" in 802.11 architecture. | Either change those newly added "802.1X authentication" to "802.1X compliant authentication" or other proper term throughout the spec draft. | Revised – All the 802.1X authentication instances has IEEE in front of them, which clarifies that 802.11 does not define 802.1X authentication.TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1181 |
| 1037 | Bo Sun | 4.5.4.2 | 22.22 | The added sentence "or the Authentication frames carrying EAPOL PDUs" is unnecessary and disappropriate. The Authentication frames carrying EAPOL PDUs should get its content from the IEEE 802.1X Uncontrolled Port. The EAPOL PDUs passing from 802.1X Uncontrolled Port is either carried in MSDU as current RSN defined or in MMPDUs as defined in 11bi. Otherwise, 11bi needs to define how the MLME receives those EAPOL PDUs and generates corresponding authentication frames from 802.1X Supplicant and Authenticator. | Remove the newly added "or the Authentication frames carrying EAPOL PDUs" | Accepted - |
| 1038 | Bo Sun | 4.5.4.2 | 22.24 | The added sentence "over the Authentication frame exchanges carrying EAPOL PDUs and" is unnecessary and disappropriate. Firstly, the Authentication frame exchanges carrying EAPOL PDUs should get its content from the IEEE 802.1X Uncontrolled Port. Secondly, "and" is conflicting with "or" at P22/L22. | Remove the newly added "over the Authentication frame exchanges carrying EAPOL PDUs and" | Accepted -  |
| 1039 | Bo Sun | 4.10.2 | 23.32 | The authentication frames carrying EAPOL PDUs should get its content from the IEEE 802.1X Uncontrolled Port. And It should not be listed as an alternative to 802.1X Uncontrolled Port. | Change the text to "IEEE 802.1X EAPOL PDUs may be transmitted in one or more IEEE 802.11 Data frames or Authentication frames passed via the IEEE 802.1X Uncontrolled Port." | Accepted - |
| 1040 | Bo Sun | 4.10.2 | 23.36 | The authentication frames carrying EAPOL PDUs should get its content from the IEEE 802.1X Uncontrolled Port. It's another way to transmit EAPOL PDUs other than 802.11 data frame. It should be transparent to the 802.1X Supplicant and Authenticator whether using data frame or authentication frame in MAC layer.Thererfore the authentication frames carrying EAPOL PDUs should not be listed as an alternative to 802.1X Uncontrolled Port. | Remove the newly added sentence. | Accepted - |
| 1207 | Mark RISON | 4.10.2 | 23.31 | "802.1X EAPOL PDUs may be transmitted in one or more IEEE 802.11 Data frames and passed via the IEEE 802.1X Uncontrolled Port or may be transmitted in one or more IEEE 802.11 Authentication frames" -- it's one or the other | Change to "802.1X EAPOL PDUs are transmitted in one or more IEEE 802.11 Data frames and passed via the IEEE 802.1X Uncontrolled Port or are transmitted in one or more IEEE 802.11 Authentication frames" | Revised –We clarify EAPOL PDU all go through uncontrolled portTGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1039 |
| 1208 | Mark RISON | 4.10.2 | 23.32 | "IEEE 802.11 Authentication frames" -- we just call them Authentication frames, no? | As it says in the comment | Revised –Agree in principle with the commenter.TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1039 |
| 1209 | Mark RISON | 4.10.2 | 23.33 | "and passed between the Supplicant and the Authenticator" -- that's always the case for .1X, no? Ditto at 23.60 | Delete the cited text | Revised –We clarify EAPOL PDU all go through uncontrolled portTGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1039 and 1209 |
| 1130 | Po-Kai Huang | 4.10.2 | 23.36 | change "IEEE 802.1X authentication utilizing Authentication frame" to "IEEE 802.1X authentication utilizing Authentication frames" and change other places with similar editorial change | As in comment | Revised –We clarify EAPOL PDU all go through uncontrolled portTGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1040 |
| 1047 | Antonio DeLaOlivaDelgado | 4.5.4.2 | 21.59 | There are seven mechanisms listed and not six | Modify "IEEE Std 802.11 defines seven IEEE 802.11 authentication methods:" to "IEEE Std 802.11 defines seven IEEE 802.11 authentication methods:" | Revised –Agree in principle with the commenter. We just change to “the following”, so we do not need to keep updating the number in the future. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1047 |
| 1196 | Mark RISON | 4.5.4.2 | 21.58 | "IEEE Std 802.11 defines six IEEE 802.11 authentication methods:" -- you've added two. 5+2=7 | As it says in the comment | Revised –Agree in principle with the commenter. We just change to “the following”, so we do not need to keep updating the number in the future. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1047 |
| 1197 | Mark RISON | 4.5.4.2 | 22.01 | "utilizes the EAP to authenticate" -- EAP is not followed by a noun here, so is a noun here, and is an acronym, so no article | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1197 |
| 1220 | Mark RISON | 9 | 0.00 | "Clause Clause" | "Clause" (2x) | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1220 |
| 1210 | Mark RISON | 9.3.3.11 | 29.03 | Is "Length of Encapsulation field" the name of a field (i.e. it's a Length of Encapsulation field field)? Ditto "Encapsulation field" | Delete "field" or make it uppercase, throughout | Revised –Agree in principle with the commenter. We change the name to “Encapsulation Length”TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1210 |
| 1211 | Mark RISON | 9.3.3.11 | 29.03 | "Length of Encapsulation" -- all words in field names should start with an uppercase letter | Change to " ... Of ... " throughout | Revised –Agree in principle with the commenter. We change the name to “Encapsulation Length”TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1210 |
| 1212 | Mark RISON | 9.3.3.11 | 29.15 | Is "FILS" being deleted before "Nonce" in all locations in the baseline | Make sure no locations have been missed | Rejected –I search all instances of “FILS Nonce” in the baseline to do the change.  |
| 1403 | Mark RISON | 12 | 0.00 | The places that have "FILS" deleted in "FILS Nonce" always leave me worried that there's some other more substantive change that I'm missing. Could we e.g. list all the "FILS" deletions in one place, or state that the only change in those subclauses is deletion of "FILS"? | As it says in the comment | Rejected –I search all instances of “FILS Nonce” in the baseline to do the change. |
| 1213 | Mark RISON | 9.3.3.11 | 29.11 | "indicates a non-zero value" is weirdly verbose. Also hyphens verboten. Many instances | Change to "is nonzero" | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1213 |
| 1214 | Mark RISON | 9.3.3.11 | 29.09 | "The field is used to carry EAPOL PDU." -- we don't say this in this table (and it's missing an article too) | Delete the cited text | Revised –We add the article and add the reference similar to descriptions of other fields. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1214 |
| 1215 | Mark RISON | 9.3.3.11 | 29.03 | I don't think it's safe to insert new fields in the order | Move 9a and 9b to be at the end (27 and 28) | Rejected – Field can not be after element. Also, this is only sent between devices that support this feature. |
| 1216 | Mark RISON | 9.3.3.11 | 0.00 | "is present as defined in 12.14.7.2 " is not clear. Does it mean that 12.14.7.2 says it's always present? if so, delete "as defined in 12.14.7.2". Does it mean 12.14.7.2 says it's sometimes but not always present? If so say "is optionally present as defined in 12.14.7.2". Many instances | As it says in the comment | Revised –Agree in principle with the commenter. We add optionally. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1216 |
| 1219 | Mark RISON | 9.4.1.74 | 35.39 | "The Length of Encapsulation field indicates the number of octets of the Encapsulation field." -- maybe, but where is the format specified. Need the boilerplate "The format of the xxx is shown in xxx" or whatever. Also "the Encapsulation field" makes no sense here since no such field is described in this subclause | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1219 |
| 1221 | Mark RISON | 9.4.1.74 | 35.56 | "The Encapsulation field carries the EAPOL PDU." -- maybe, but where is the format specified. Need the boilerplate "The format of the xxx is shown in xxx" or whatever. Also "the EAPOL PDU" makes no sense here since no such PDU is described in this subclause. Also, does the field always carry the entire EAPOL PDU; can't it be fragmented? | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1221 |
| 1226 | Mark RISON | 9.4.1.74 | 35.39 | The field shouldn't be called "field", else we end up with an x field field. Ditto line 61 | Delete the "field" in the figure cell | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1226 |
| 1194 | Mark RISON |   | 0.00 | Should it be "EAPOL-Start Authentication frames" or should it be "EAPOL-Start authentication frames"? Cf. "EAPOL-Key request frames" | As it says in the comment | Rejected – We use Authentication frame. Baseline has precendece like the following. Note that baseline probably has errors because excep the introduction, all other places use FILS Authentication frmae or SAE Authentiaction frame. *References in this standard to “FILS authentication frame” or “SAE authentication frame” are to be**understood as references to an Authentication frame that contains fields and elements for FILS or SAE**(respectively) operation per Table 9-71 (Presence of fields and elements in Authentication frames).*We have the following for the explanation.*Within IEEE Std 802.11, EAPOL PDUs are carried as MSDUs within one or more Data frames or are carried within Authentication frames(#1129) (see 12.14.4)(#1193), as described in Clause 12 of IEEE Std 802.1X-2020. Within this standard, Data frames used for this purpose are generally referred to as EAPOL-Key frames, EAPOL-Key request frames, and EAPOL-Start frames. Authentication frames used for this purpose are generally referred to as EAPOL-Start Authentication frames.* |
| 1149 | Po-Kai Huang | 9.4.2.23.3 | 37.15 | Need to add the new algorithm number for 802.1X | As in comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1149 |
| 1228 | Mark RISON | 9.4.2.188 | 37.60 | Deleting "FILS" in " in the FILS authentication exchange" makes the sentence strange: in what authentication exchange? | Change "the" to "an" | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1121r3 under all headings that include CID 1228 |

**Discussion:**

**Proposal:**

*TGbi editor: Modify Clause 9.4.2.240 as follows (track change on):*

* RSNXE

***Insert the following new rows to Table 9-373 while maintaining the numerical order and updating the reserved range (not all lines shown):***

* Extended RSN Capabilities field

|  |  |  |
| --- | --- | --- |
| Bit | Information | Notes |
| … |  |  |
| <ANA>(#0031r4) | IEEE 802.1X Authentication Utilizing Authentication Frame Support | A EDP STA sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support subfield to 1 if dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated is true. Otherwise, this subfield is set to 0. (#1426) |

*TGbi editor: Modify Clause 12.14.4 as follows (track change on):*

* IEEE 802.1X authentication utilizing Authentication frames(#0031r4)

If an AP sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support subfield(#Ed) in the RSNXE that it transmits to 1, then a non-AP STA (authentication originator) with dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated equal to true(#1426) may signal its Supplicant to authenticate with the AP (authentication responder) using IEEE Std 802.1X-2020(#Ed) utilizing Authentication frames.

If any AP affiliated with an AP MLD sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support subfield(#Ed) in the RSNXE that it transmits to 1, then a non-AP MLD (authentication originator) wih dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated equal to true(#1426) may signal its Supplicant to authenticate with the AP MLD (authentication responder) using IEEE Std 802.1X-2020(#Ed) utilizing Authentication frames by transmitting the Authentication frames to the AP through a non-AP STA affiliated with the non-AP MLD.

When the authentication originator is non-AP MLD and the authentication responder is AP MLD, the RA field of an Authentication frame in response to an Authentication frame from the peer shall be set to the TA field of the Authentication frame from the peer.

If an authentication originator chooses to initiate IEEE(#1181) 802.1X authentication utilizing Authentication frames, it first selects an(#1428) IEEE(#1181) 802.1X AKM that is supported by the authentication responder.

The authentication originator then constructs the first Authentication frame of the exchange as follows:

* Authentication Algorithm Number field is(#Ed) set to <ANA> (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is(#Ed) set to 1.
* (#1436)The Encapsulation field carries an(#1429) EAPOL PDU.
* Include(#1430) the AKM Suite Selector element indicating the selected IEEE(#1181) 802.1X AKM.

The authentication originator sends the first Authentication frame to the authentication responder.

Upon receiving the first Authentication frame, the authentication responder:

* Validates that the AKM indicated in AKM Suite Selector element is an IEEE(#1181) 802.1X AKM(#1431)
* Validates that the selected IEEE(#1181) 802.1X AKM indicated in AKM Suite Selector element is supported. Otherwise processing status is set to STATUS\_INVALID\_AKMP.
* Extracts an(#1432) EAPOL PDU from the Encapsulation field, and processes it (#1433).

The authentication responder then constructs the second Authentication frame of the exchange as follows:

* Authentication Algorithm Number field is set to <ANA> (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is(#Ed) set to 2.
* Status Code field(#1435) indicates the processing status.
* (#1436) The Encapsulation Length field(#1210) indicates 0 if the status is set to STATUS\_INVALID\_AKMP.
* The Encapsulation(#1429) field (if present) carries an(#1434) EAPOL PDU.
* Includes the AKM Suite Selector element indicating the same(#1437) IEEE(#1181) 802.1X AKM indicated in the first Authentication frame.

Once the processing is complete, the authentication responder sends the second Authentication frame to the authentication originator. If the processing status returned in the frame was not SUCCESS, the authentication responder shall terminate the authentication.

Upon receiving the second Authentication frame, the authentication originator:

* Validates that the(#1438) AKM indicated in AKM Suite Selector element is the same as the one indicated in the first Authentication frame. Otherwise processing status is set to STATUS\_INVALID\_AKMP.
* Extracts an(#1434) EAPOL PDU from the Encapsulation field, and processes it(#1433).

The authentication originator then constructs the third Authentication of the exchange as follows:

* Authentication Algorithm Number field is(#Ed) set to <ANA> (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is(#Ed) set to 3.
* Status Code field(#1435) indicates the processing status.
* (#1436) The Encapsulation Length (#1210)field indicates 0 if the status is set to STATUS\_INVALID\_AKMP.

Once the processing is complete, the authentication originator sends the third Authentication frame to the authentication responder. If the processing status returned in the frame was not SUCCESS, the authentication originator shall terminate the authentication.

Upon receiving the Authentication frame with Authentication Transaction Sequence Number field set to X, where X is larger than or equal to 3, the authentication originator or the authentication responder:

* Extracts an(#1434) EAPOL PDU from the Encapsulation field, and processes it (#1433).

The authentication originator or the authentication responder then constructs the Authentication frame of the exchange in response to the Authentication frame with Authentication Transaction Sequence Number field set to X, where X is larger than or equal to 3, (#1440)as follows:

* Authentication Algorithm Number field is(#Ed) set to <ANA> (IEEE 802.1X authentication).
* Authentication Transaction Sequence Number field is(#Ed) set to X+1.
* Status Code field(#1435) indicates the processing status.
* (#1436)
* The Encapsulation(#1429) field (if present) carries an(#1434) EAPOL PDU.

NOTE – The number of Authentication frame exchanges depends on the EAP method in use. Hence, X is a value as defined by the EAP method.(#1440)

Once the processing is complete, the authentication originator or the authentication responder sends the Authentication frame to its peer (if needed by the EAP method). If the processing status returned in the frame was not SUCCESS, the authentication originator or the authentication responder shall terminate the authentication.

*TGbi editor: Modify Clause 12.2.4 as follows (track change on):* (#1079r1)

* RSNA establishment

***Change the second and fourth sub-bullet of the first bullet and add a new bullet of the first paragraph as follows (not all lines are shown):***

An SME establishes an RSNA in one of seven ways:

* If an RSNA uses authentication negotiated over IEEE Std 802.1X or FILS authentication in an infrastructure BSS, an SME establishes an RSNA as follows:
* It identifies the AP as an RSNA AP from the AP’s Beacon, DMG Beacon, Announce, Information Response, FILS Discovery, or Probe Response frames.
* It shall invoke Open System, IEEE 802.1X authentication(#0031r4),(#1390) or FILS authentication if the STA is a non-DMG STA.
* It negotiates cipher suites during the association process, as described in 12.6.2 (RSNA selection) and 12.6.3 (RSNA policy selection in an infrastructure BSS).
* It uses IEEE Std 802.1X-2020 to authenticate if IEEE(#1181) 802.1X authentication is not performed before association,(#0031r4) as described in 12.6.8 (RSNA establishment in an infrastructure BSS) and 12.6.9 (RSNA authentication in an IBSS), FT protocol to authenticate as described in 13.5 (FT protocol) or uses FILS authentication to authenticate as described in 12.11 (Authentication for FILS).
* If an RSNA uses PASN authentication, an RSNA capable the STA establishes an RSNA asdescribed in 12.13 (Preassociation security negotiation(11az)).
* If an RSNA uses EDPKE authentication, an RSNA capable STA establishes an RSNA as described in 12.14.8 (Enhanced Data Privacy Key Exchange).(#0068r4)

*TGbi editor: Modify Clause 12.6.1.2.2 as follows (track change on):*

* Security association in an ESS(#0031r4)

***Change item b) and item c) of the second paragraph (not all shown) as follows:***

A STA and AP establish an initial security association via the following steps:

* The STA then performs IEEE 802.11 authentication followed by association to the chosen AP. Confirmation of security parameters takes place during association. A non-DMG STA performing IEEE 802.1X authentication uses~~es~~(#1393) Open System authentication or IEEE(#1181) 802.1X authentication utilizing Authentication frames. A STA performing password-based authentication can use SAE authentication. A STA performing FILS uses FILS authentication. A non-DMG STA executing the OWE exchange uses Open System authentication.
* SAE authentication, IEEE(#1181) 802.1X authentication, and FILS authentication provides mutual authentication and derivation of a PMK. If Open System authentication is chosen instead, the Authenticator or the Supplicant initiates IEEE 802.1X authentication after (re)association. The EAP method used by IEEE Std 802.1X-2020 needs to support mutual authentication, as the STA needs assurance that the AP is a legitimate AP.

***Change the fourth note as follows:***

NOTE 4—Prior to the completion of IEEE 802.1X authentication and the installation of keys, the IEEE 802.1X Controlled Port in the AP blocks all Data frames. The IEEE 802.1X Controlled Port returns to the unauthorized state and blocks all Data frames before invocation of an MLME-DELETEKEYS.request primitive. The IEEE 802.1X Uncontrolled Port allows EAPOL PDUs to pass between the Supplicant and Authenticator. The Supplicant and Authenticator might also use Authentication frames to pass EAPOL PDUs.

***Change item d) of the second paragraph (not all shown) as follows:***

* The last step is key management. The authentication process, whether SAE authentication, FILS authentication, or IEEE 802.1X authentication utilizing Authentication frames; or IEEE 802.1X authentication utilizing Data frames post association;(#1394) or the OWE exchange utilizing association frames creates cryptographic keys shared between the cryptographic endpoints—the AP and STA, or the IEEE 802.1X AS and the STA, when using SAE/FILS/OWE or IEEE Std 802.1X, respectively. When using IEEE Std 802.1X, the AS transfers these keys to the AP, and the AP and STA uses one of the key confirmation handshakes, e.g., the 4-way handshake or FT 4-way handshake, to complete security association establishment. When using SAE authentication or OWE there is no AS and therefore no key transfer; the 4-way handshake is performed directly between the AP and STA. The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected robust Management frames. When FILS authentication is performed, the key confirmation is performed using association frames. Hence, no additional handshake is necessary.

***Change second bullet of the third paragraph (not all shown) as follows:***

When FT is not enabled, a STA BSS transitioning within an ESS establishes a new PMKSA by one of the five schemes:

* In the case of SAE authentication or IEEE(#1181) 802.1X authentication followed by (re)association, the STA repeats the same actions as for initial contact association, but the non-AP STA also deletes the PTKSA when it roams from the old AP. Note that a STA can take advantage of the fact that it can perform SAE authentication or IEEE(#1181) 802.1X authentication to multiple APs while maintaining a single association with one AP, and then use any of the PMKSAs created during authentication to effect a fast BSS transition.

*TGbi editor: Modify Clause 12.6.7 as follows (track change on):*

* + 1. RSN management of the IEEE 802.1X Controlled Port(#0031r4)

***Change the first paragraph as follows:***

In an RSN, this standard relies on the fact that IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port or Authentication frames carrying EAPOL PDUs(#1395). The IEEE 802.1X Controlled Port is blocked from passing general data traffic between the STAs until an IEEE 802.1X authentication procedure completes successfully over the Authentication frame exchanges carrying EAPOL PDUs(#1395) (if using IEEE 802.1X authentication utilizing Authentication frames(#1395)) and the IEEE 802.1X Uncontrolled Port. The security of an RSNA depends on this being true.

***Change the seventh paragraph as follows:***

EAPOL PDUs shall be carried in individually addressed MSDUs or individually addressed Authentication frames.

*TGbi editor: Modify Clause 12.6.1.2.2 as follows (track change on):*

* General(#0031r4)

***Change the first paragraph as follows:***

When establishing an RSNA in a non-FT environment or during an FT initial mobility domain association, a STA shall use IEEE 802.11 SAE authentication, FILS authentication, IEEE(#1181) 802.1X authentication, or Open System authentication prior to (re)association. PASN authentication may be used without (re)association.

***Change the fifth paragraph as follows:***

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

* If a STA negotiates to use IEEE 802.1X authentication during (re)association, the STA’s management entity may respond to the MLME-ASSOCIATE.confirm (or indication) or MLMEREASSOCIATE.confirm (or indication) primitive by requesting the Supplicant (or Authenticator) to initiate IEEE 802.1X authentication if IEEE(#1181) 802.1X authentication is not performed before (re)association. Thus, in this case, authentication is driven by the STA’s decision to associate and the AP’s decision to accept the association.
* If a STA’s MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member, a STA may signal its Supplicant to use IEEE Std 802.1X-2020 to preauthenticate with that AP (see 12.6.8.2 (Preauthentication and RSNA key management)).

NOTE 2—A BSS transitioning STA’s IEEE 802.1X Supplicant can initiate preauthentication by sending an EAPOL-Start PDU (in one or more EAPOL-Start frames) via its old AP, through the DS, to a new AP.

* If a STA's MLME-SCAN.confirm primitive finds another AP within the ESS of which the STA is a member that advertises support for IEEE(#1181) 802.1X Authentication Utilizing Authentication frame(#1399) in its RSNXE, a STA may signal its Supplicant to use IEEE Std 802.1X-2020(#Ed) to authenticate with that AP (see 12.14.4 (IEEE 802.1X authentication utilizing Authentication frames)).
* If a STA receives an IEEE 802.1X message, it delivers this to its Supplicant or Authenticator, which may initiate a new IEEE 802.1X authentication.

*TGbi editor: Modify Clause 12.7.1.3 as follows (track change on):*

* Pairwise key hierarchy(#762r2)

***Change the seventh paragraph (not all shown) as follows:***

The following apply when not using FILS authentication:

* SNonce is a random or pseudorandom value contributed by the Supplicant; its value is taken when a PTK is instantiated and is sent to the PTK Authenticator.
* ANonce is a random or pseudorandom value contributed by the Authenticator.
* The PTK shall be derived from the PMK by

PTK = PRF-Length(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce)||DHss) if key derivation with Authentication frame exchange for IEEE(#1181) 802.1X is used as defined in 12.14.7.2 (802.1X).

Otherwise, PTK = PRF-Length(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))

*TGbi editor: Modify Clause 4.2.5 as follows (track change on):*

* Interaction with other IEEE 802® layers(#0031r4)

***Change the second paragraph as follows:***

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect Data frames, IEEE Std 802.1X-2020 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2020 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2020 to access these services. Within IEEE Std 802.11, EAPOL PDUs are carried as MSDUs within one or more Data frames or are carried within Authentication frames(#1129) (see 12.14.4)(#1193), as described in Clause 12 of IEEE Std 802.1X-2020. Within this standard, Data frames used for this purpose are generally referred to as *EAPOL-Key frames, EAPOL-Key request frames, and EAPOL-Start frames*. Authentication frames used for this purpose are generally referred to as *EAPOL-Start Authentication frames*.

*TGbi editor: Modify Clause 4.5.3.3 as follows (track change on):*

* Association(#0031r4)

***Change the fifth paragraph as follows:***

Within a robust security network (RSN), association is handled differently. In an RSNA, the IEEE 802.1X Port determines when to allow data traffic across an IEEE 802.11 link. A single IEEE 802.1X Port maps to one association, and each association maps to an IEEE 802.1X Port. An IEEE 802.1X Port consists of an IEEE 802.1X Controlled Port and an IEEE 802.1X Uncontrolled Port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over (#1195)the IEEE 802.1X Uncontrolled Port. Once the AKM completes successfully, data protection is enabled to prevent unauthorized access, and the IEEE 802.1X Controlled Port unblocks to allow protected data traffic. IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port(#1195)(#Ed). It is expected that most other protocol exchanges use the IEEE 802.1X Controlled Ports. However, a given protocol might need to bypass the authorization function and make use of the IEEE 802.1X Uncontrolled Port.

*TGbi editor: Modify Clause 4.5.4.2 as follows (track change on):*

* Authentication

***Change the third, fourth, fifth, sixth paragraph as follows:***

IEEE Std 802.11 defines the following(#1047)~~five~~(#0031r4) IEEE 802.11 authentication methods: Open System authentication, FT authentication, simultaneous authentication of equals (SAE), IEEE 802.1X authentication,(#0031r4) FILS authentication, ~~and~~ preassociation security negotiation (PASN) authentication and enhanced data privacy key exchange authentication.(#0068r4) Open System authentication admits any STA to the DS. FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 13 (Fast BSS transition). SAE authentication uses finite field cryptography to prove knowledge of a shared password. IEEE 802.1X authentication utilizes (#1197)EAP to authenticate STAs and the AS with one another.(#0031r4) FILS authentication allows for faster connection to the network for FILS non-AP STAs by providing authentication, association, and key confirmation information in an efficient number of frame exchanges (see 4.10.3.6 (AKM operations using FILS authentication)). PASN and EDPKE (#0068r4)authentication allows for the protection of Management frames without association by establishing a PTKSA using authentication frames. The IEEE 802.11 authentication mechanism also allows definition of new authentication methods, or any combination of these authentication methods.

An RSNA might support one or more of the following authentication methods: SAE authentication, IEEE 802.1X authentication,(#0031r4) FILS authentication, ~~or~~ PASN authentication or EDPKE authentication(#0068r4). An RSNA also supports authentication based on IEEE Std 802.1X-2020, or preshared keys (PSKs) after Open System authentication. ~~IEEE 802.1X authentication utilizes the EAP to authenticate STAs and the AS with one another.~~(#0031r4) This standard does not specify an EAP method that is mandatory to implement. See 12.6.4 (RSNA policy selection in an IBSS) for a description of the IEEE 802.1X authentication and PSK usage within an IEEE 802.11 IBSS

In an RSNA, IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port(#1037)(#Ed)(#0031r4). The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over (#1037)the IEEE 802.1X Uncontrolled Port.

SAE authentication, IEEE 802.1X authentication,(#0031r4) and Open System IEEE 802.11 authentication are used by STAs in an RSN for an infrastructure BSS. FILS authentication can be used by FILS STAs in an RSN for an infrastructure BSS. SAE authentication, Open System IEEE 802.11 authentication, or no IEEE 802.11 authentication is used in an RSN for an IBSS. SAE authentication is used for an MBSS. In an RSN for DMG BSS, Open System IEEE 802.11 authentication is not used (12.2.4 (RSNA establishment)).

***Change the last paragraph as follows:***

PASN authentication or EDPKE authentication(#0068r4) is used in an RSN for an infrastructure BSS when it is based on a PMKSA established by another RSN authentication protocol. Otherwise, it does not guarantee mutual authentication, and can be used as a non-RSN protocol in an infrastructure BSS.

*TGbi editor: Modify Clause 4.10.2 as follows (track change on):*

* IEEE 802.11 usage of IEEE Std 802.1X-2020(#0031r4)

***Change the first paragraph as follows:***

IEEE Std 802.11 depends upon IEEE Std 802.1X-2020 to control the flow of MAC service data units (MSDUs) between the DS and STAs by use of the IEEE 802.1X Controlled/Uncontrolled Port model. IEEE 802.1X EAPOL PDUs may be~~are~~ transmitted in one or more IEEE 802.11 Data frames or Authentication frames and passed via the IEEE 802.1X Uncontrolled Port .(#1039) The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an IEEE 802.1X authentication procedure completes successfully over (#1040)the IEEE 802.1X Uncontrolled Port. It is the responsibility of both the Supplicant and the Authenticator to implement port blocking. Each association between a pair of STAs creates a unique pair of IEEE 802.1X Ports, and authentication takes place relative to those ports alone.

* AKM operations with AS(#0031r4)

***Change item b) of the first paragraph as follows (not all lines are shown):***

The following AKM operations are carried out when an IEEE 802.1X AS is used:

* A STA discovers the AP’s security policy through passively monitoring Beacon frames or through active probing. If IEEE 802.1X authentication is used, the EAP authentication process starts when the Authenticator sends the EAP-Request or the Supplicant sends the EAPOL-Start PDU (in one or more EAPOL-Start frames or EAPOL-Start Authentication frames). EAP messages pass between the Supplicant and AS via the Authenticator and Supplicant’s Uncontrolled Ports as described in 12.7 (Keys and key distribution)(#1209).

*TGbi editor: Modify Clause 9.4.1.74 as follows (track change on):*

***Insert the following new subclauses at the end of (#1220)Clause 9.4.1:***

* Encapsulation Length (#1210)field(#0031r4)

The Encapsulation Length (#1210)field indicates the number of octets of the Encapsulation field (See 9.4.1.75). The format of the Encapsulation Length field is shown in Figure 9-189h.(#1219)

|  |  |
| --- | --- |
|  | Encapsulation Length (#1210)(#1226) |
| Octets: | 2 |
| * Encapsulation Length (#1210)field format
 |

* Encapsulation field(#0031r4)

The Encapsulation field carries the EAPOL PDU. The format of the Encapsulation field is shown in Figure 9-189i. (#1221)

|  |  |
| --- | --- |
|  | Encapsulation(#1226) |
| Octets: | variable |
| * Encapsulation field format
 |

*TGbi editor: Modify Clause 9.6.36 as follows (track change on):*

***Insert the following new subclauses at the end of (#1220)Clause 9.6:***

* Protected HT Action frame details(#1975r4)
* Authentication frame format

***Modify Table 9-70 as follows (not all lines shown):***

* Authentication frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 9 | Confirm | An unsigned integer encoded as described in 12.4.7.4 (Encoding and decoding of SAE Confirm messages). This is present only in certain Authentication frames as defined in Presence of fields and elements in Authentication frames. |
| 9a(#0031r4) | Encapsulation Length (#1210) | The Encapsulation Length (#1210) field indicates the number of octets of the Encapsulation field. This is present only in certain Authentication frames as defined in Table 9-71 |
| 9b(#0031r4) | Encapsulation(#1210) | The field is used to carry an(#1214) EAPOL PDU as described in 12.14.4. This is present only when the Encapsulation Length (#1210)field is nonzero(#1213).  |
| ... |  |  |
| 17 | ~~FILS~~ Nonce(#762r2) | The ~~FILS~~ Nonce(#762r2) element is present in ~~FILS~~ Authentication(#762r2) frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| ... |  |  |
| 25 | PASN Parameters | A PASN Parameters (#68r4)element is present only in certain Authentication framesas defined in Table 9-71 (Presence of fields and elements in Authentication frames). |
| 26(#150r5) | Diffie-Hellman Parameter | A Diffie-Hellman Parameter element is present only in certain Authentication frames as defined in Table 9-71 (Presence of fields and elements in Authentication frames). |

***Change Table 9-71 and insert new rows at the end of Table 9-71 as follows (not all lines shown):***

* Presence of fields and elements in Authentication frames

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication algorithm | Authentication transaction sequence number | Status code | Presence of fields and elements from order 4 onward |
| FT(#150r5) | 1 | Reserved | The MDE is present. The FTE and RSNE(s) are present if dot11RSNAActivated is true.The Diffie-Hellman Parameter element is present as defined in 12.14.7.1 (FT). |
| FT(#150r5) | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | The MDE is present if the Status Code field is 0. The FTE and RSNE(s) are present if the Status Code field is 0 and dot11RSNAActivated is true.The Diffie-Hellman Parameter element is present as defined in 12.14.7.1 (FT). |
| .... |  |  |  |
| FILS Shared Keyauthenticationwithout PFS | 1 | Reserved | The RSNE is present.The MDE is present if the FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present.(#762r2)The FILS Session element is present.The FILS Wrapped Data element is present. |
| FILS Shared Keyauthenticationwithout PFS | 2 | Status | The RSNE is present.The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present if the Status Code field is 0.(#762r2)The FILS Session element is present if the Status Code field is 0.The FILS Wrapped Data element is present if the Status Code field is 0.The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Requestframe. |
| FILS Shared Keyauthentication withPFS | 1 | Reserved | The Finite Cyclic Group field is present.The FFE field is present.The RSNE is present.The MDE is present if the FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present.(#762r2)The FILS Session element is present.The FILS Wrapped Data element is present. |
| FILS Shared Keyauthentication withPFS | 2 | Status | The Finite Cyclic Group field is present if the Status Code field is 0.The FFE field is present if the Status Code field is 0.The RSNE is present.The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present if the Status Code field is 0.(#762r2)The FILS Session element is present if the Status Code field is 0.The FILS Wrapped Data element is present if the Status Code field is 0.The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| FILS Public Keyauthentication | 1 | Reserved  | The Finite Cyclic Group field is present.The FFE field is present.The RSNE is present.The MDE is present if the FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present.(#762r2)The FILS Session element is present. |
| FILS Public Keyauthentication | 2 | Status | The Finite Cyclic Group field is present if the Status Code field is 0.The FFE field is present if the Status Code field is 0.The RSNE is present.The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.The ~~FILS~~ Nonce element is present if the Status Code field is 0.(#762r2)The FILS Session element is present if the Status Code field is 0.The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| IEEE 802.1X authentication(#0031r4) | 1 | Reserved  | The Encapsulation Length (#1210) field is present.The Encapsulation field is present only when the Encapsulation Length (#1210) field is nonzero(#1213).The AKM Suite Selector element is present as defined in 12.14.4 (IEEE 802.1X authentication utilizing Authentication frames).(#762r2)The RSNE is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2)The RSNXE is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2)The Nonce element is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2)The Diffie-Hellman Parameter element is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2) |
| IEEE 802.1X authentication(#Ed)(#0031r4) | 2 | SUCCESS | The Encapsulation Length (#1210) field is present.The Encapsulation field is present only when the Encapsulation Length (#1210)field is nonzero(#1213).The AKM Suite Selector element is present as defined in 12.14.4 (IEEE 802.1X authentication utilizing Authentication frames).(#762r2)The RSNE is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2)The Nonce element is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2)The Diffie-Hellman Parameter element is optionally(#1216) present as defined in 12.14.7.2 (802.1X).(#762r2) |
| IEEE 802.1X authentication(#Ed)(#0031r4) | 2 | Not SUCCESS(#Ed) | The Encapsulation Length (#1210)field is present.The Encapsulation field is present only when the Encapsulation Length (#1210)field is nonzero(#1213). |
| IEEE 802.1X authentication(#Ed)(#0031r4) | 3 | SUCCESS | The Encapsulation Length (#1210)field is present.The Encapsulation field is present only when the Encapsulation Length (#1210)field is nonzero(#1213). |
| IEEE 802.1X authentication(#Ed)(#0031r4) | 3 | Not SUCCESS(#Ed) | The Encapsulation Length (#1210)field is present.The Encapsulation field is present only when the Encapsulation Length (#1210)field is nonzero(#1213). |
| IEEE 802.1X authentication(#0031r4) | > 3 | Status | The Encapsulation Length (#1210)field is present.The Encapsulation field is present only when the Encapsulation Length (#1210)field is nonzero(#1213). |
| EDPKE authentication(#0068r4) | 1 | Reserved | RSNE is present.RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.PASN Parameters element is present.Timeout Interval element may be present.Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved.Fragment element may be present if any of the elements are fragmented. |
| EDPKE authentication(#0068r4) | 2 | Status | RSNE is present and PASN Parameters element is present if Status Code field is 0.RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero.Timeout Interval element may be present.Wrapped data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved and Status Code field is 0.MIC element is present.Fragment element may be present if any of the elements are fragmented and Status Code field is 0.  |
| EDPKE authentication(#0068r4) | 3 | Status | PASN Parameters element is present if Status Code field is 0.Wrapped data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved; and Status Code field is 0.MIC element is present.Fragment element may be present if any of the elements are fragmented and Status Code field is 0.  |

*TGbi editor: Modify Clause 9.4.2.23.3 as follows (track change on):*

* AKM suites

(…existing texts….)

|  |
| --- |
| * AKM suite selectors
 |
| OUI | Suite type | Meaning | Authentication algorithm numbers (see 9.4.1.1 (Authentication Algorithm Number field)) | Cipher suite selector restriction (M20) |
| Authentication type | Key management type | Key derivation type  |
| 00-0F-AC | 0 | Reserved | Reserved | Reserved | Reserved | Reserved |
| 00-0F-AC | 1 | Authentication negotiated over IEEE Std 802.1X | RSNA key management as defined in 12.7 (Keys and key distribution) | Defined in 12.7.1.2 (PRF) | 0 (open) or <ANA> (IEEE 802.1X)(#1149) | None |
| 00-0F-AC | 2 | PSK | RSNA key management as defined in 12.7 (Keys and key distribution) | Defined in 12.7.1.2 (PRF) | 0 (open) | None |
| 00-0F-AC  | 3 | FT authentication negotiated over IEEE Std 802.1X | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | 2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) or <ANA> (IEEE 802.1X) (#1149) for FT Initial Mobility Domain Association over IEEE Std 802.1X 0 (open) for FT Initial Mobility Domain Association over(#1149) PMKSA caching | None |
| 00-0F-AC  | 4 | FT authentication using PSK | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | 2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) for FT Initial Mobility Domain Association using PSK | None |
| 00-0F-AC  | 5 | Authentication negotiated over IEEE Std 802.1X | RSNA key management as defined in 12.7 (Keys and key distribution) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | 0 (open) or <ANA> (IEEE 802.1X) (#1149) | None |
| 00-0F-AC  | 6 | PSK | RSNA Key Management as defined in 12.7 (Keys and key distribution) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | 0 (open) | None |
| 00-0F-AC | 7 | TDLS | TPK handshake | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | N/A | None |
| 00-0F-AC | 8 | SAE authentication  | RSNA key management as defined in 12.7 (Keys and key distribution), or authenticated mesh peering exchange as defined in 14.6 (Authenticated mesh peering exchange (AMPE)) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm specified in 12.4.2 (Assumptions on SAE)  | 3 (SAE) for SAE Authentication0 (open) for PMKSA caching | None |
| 00-0F-AC | 9 | FT authentication over SAE | FT key management defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm specified in 12.4.2 (Assumptions on SAE)  | 3 (SAE) for FT Initial Mobility Domain Association2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol) 0 (open) for FT Initial Mobility Domain Association over PMKSA caching | None |
| 00-0F-AC | 10 | APPeerKey Authentication with SHA-256 | RSNA key management as defined in 12.7 (Keys and key distribution)  | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | N/A | None |
| 00-0F-AC | 11 | Authentication negotiated over IEEE Std 802.1X using a Suite B compliant EAP method supporting SHA-256 | RSNA key management as defined in 12.7 (Keys and key distribution)  | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | 0 (open) or <ANA> (IEEE 802.1X) (#1149) | Used only with cipher suite selector values 00-0F-AC:8 (GCMP-128) and 00-0F-AC:11 (BIP-GMAC-128) |
| 00-0F-AC | 12 | Authentication negotiated over IEEE Std 802.1X using a CNSA Suite compliant EAP method | RSNA key management as defined in 12.7 (Keys and key distribution)  | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384 | 0 (open) or <ANA> (IEEE 802.1X) (#1149) | Used only with cipher suite selector values 00-0F-AC:9 (GCMP-256), 00-0F-AC:10 (CCMP-256), 00-0F-AC:13 (BIP-CMAC-256), and 00-0F-AC:12 (BIP-GMAC-256) |
| 00-0F-AC | 13 | FT authentication negotiated over IEEE Std 802.1X | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384 | 2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) or <ANA> (IEEE 802.1X) (#1149) for FT Initial Mobility Domain Association over IEEE Std 802.1X 0 (open) for FT Initial Mobility Domain Association over (#1149) PMKSA caching | Used only with cipher suite selector values 00-0F-AC:9 (GCMP-256), 00-0F-AC:10 (CCMP-256), 00-0F-AC:13 (BIP-CMAC-256), and 00-0F-AC:12 (BIP-GMAC-256) |
| 00-0F-AC | 14 | Key management over FILS using SHA-256 and AES-SIV-256, or authentication negotiated over IEEE Std 802.1X | FILS key management defined in 12.11.2.5 (Key establishment with FILS authentication) | Defined in 12.11.2.5 (Key establishment with FILS authentication) using SHA-256 | 4, 5 or 6 (FILS) for FILS Authentication0 (open) or <ANA> (IEEE 802.1X) (#1149) for IEEE Std 802.1X | None |
| 00-0F-AC | 15 | Key management over FILS using SHA-384 and AES-SIV-512, or authentication negotiated over IEEE Std 802.1X | FILS key management defined in 12.11.2.5 (Key establishment with FILS authentication) | Defined in 12.11.2.5 (Key establishment with FILS authentication) using SHA-384 | 4, 5 or 6 (FILS) for FILS Authentication0 (open) or <ANA> (IEEE 802.1X) (#1149) for IEEE Std 802.1X | None |
| 00-0F-AC | 16 | FT authentication over FILS with SHA-256 and AES-SIV-256 or authentication negotiated over IEEE Std 802.1X | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-256 | 4, 5 or 6 (FILS) for FT Initial Mobility Domain Association over FILS2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) or <ANA> (IEEE 802.1X) (#1149) for FT Initial Mobility Domain Association over IEEE Std 802.1X 0 (open) for FT Initial Mobility Domain Association over (#1149) PMKSA caching | None |
| 00-0F-AC | 17 | FT authentication over FILS with SHA-384 and AES-SIV-512, or authentication negotiated over IEEE Std 802.1X | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384  | 4, 5 or 6 (FILS) for FT Initial Mobility Domain Association over FILS2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) or <ANA> (IEEE 802.1X) (#1149) for FT Initial Mobility Domain Association over IEEE Std 802.1X 0 (open) for FT Initial Mobility Domain Association over (#1149) PMKSA caching | None |
| 00-0F-AC(#1084) | 18 | None | RSNA key management as defined in 12.7 (Keys and key distribution) | (#6088)Defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm specified in Table 12-1 (Hash algorithm based on length of prime) | 0 (open) | None |
| 00-0F-AC | 19 | FT authentication using PSK | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384 | 2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) for FT Initial Mobility Domain Association using PSK | None |
| 00-0F-AC | 20 | PSK | RSNA key management as defined in 12.7 (Keys and key distribution) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384 | 0 (open) | None |
| 00-0F-AC(11az) | 21 | PASN-1 | PASN | PASN key management defined in 12.13 (Preassociation security negotiation(11az))  | Defined in 12.13.3 (Key establishment with PASN authentication) | None(#7069) |
| 00-0F-AC(M20) | 22 | FT authentication negotiated over IEEE Std 802.1X | FT key management as defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384 | 2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol)0 (open) or <ANA> (IEEE 802.1X) (#1149) for FT Initial Mobility Domain Association over IEEE Std 802.1X 0 (open) for FT Initial Mobility Domain Association over (#1149) PMKSA caching | None |
| 00-0F-AC(M20) | 23 | Authentication negotiated over IEEE Std 802.1X  | RSNA key management as defined in 12.7 (Keys and key distribution) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using SHA-384 | 0 (open) or <ANA> (IEEE 802.1X) (#1149) | None |
| 00-0F-AC(M21) | 24 | SAE authentication  | RSNA key management as defined in 12.7 (Keys and key distribution), or authenticated mesh peering exchange as defined in 14.6 (Authenticated mesh peering exchange (AMPE)) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm specified in 12.4.2 (Assumptions on SAE)  | 3 (SAE) for SAE Authentication0 (open) for PMKSA caching | None |
| 00-0F-AC(M21) | 25 | FT authentication over SAE  | FT key management defined in 12.7.1.6 (FT key hierarchy) | Defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm specified in 12.4.2 (Assumptions on SAE)  | 3 (SAE) for FT Initial Mobility Domain Association2 (FT) for FT protocol reassociation as defined in 13.5 (FT protocol) 0 (open) for FT Initial Mobility Domain Association over PMKSA caching | None |
| 00-0F-AC | 26–255(M21)  | Reserved | Reserved | Reserved | Reserved | Reserved |
| Other OUI or CID | Any | Vendor-specific | Vendor-specific | Vendor-specific | Vendor-specific | Vendor-specific |

*TGbi editor: Modify Clause 9.4.2.188 as follows (track change on):*

* ~~FILS~~ Nonce element(#762r2)

The ~~FILS~~ Nonce element is used for exchanging an additional source of randomness in an(#1228) ~~FILS~~ authentication exchange. The format of the ~~FILS~~ Nonce element is shown in Figure 9-767 (FILS Nonce element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | ~~FILS~~ Nonce |
| Octets: | 1 | 1 | 1 | 16 |
| * ~~FILS~~ Nonce element format
 |

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The ~~FILS~~ Nonce field contains randomly generated data.