IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 editorial comments |
| Date: 2025-03-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission resolves the following CIDs:

 778, 144, 163, 145, 370, 571, 508, 574, 503, 371,

 984, 963, 12, 305, 377, 380, 324, 10, 302, 928,

 13, 14, 15, 16, 402, 191, 404, 406, 408, 411,

 412, 400, 422, 419, 456, 461, 40, 41, 42, 43,

 44, 45, 46, 453, 155, 1003, 468,1004, 977, 61,

 935,1009, 494, 754, 498, 334, 1010, 557, 679, 664, 665,

 666, 668, 159, 669, 670, 776, 138, 844, 671, 672,

 673, 674, 765, 677, 682, 647, 651, 652, 653, 175,

 271, 272, 686, 766, 276, 277, 278, 279, 282, 688,

 689, 691, 692, 693, 694, 695, 162, 702, 704, 705,

 709, 710, 711, 712, 713, 714, 715, 716, 718, 719,

 852, 298, 743, 768, 6, 8, 421, 455, 460, 734,

 737, 591, 424, 748, 458,

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Add comment 458, 468, 754. Update resolution with latest ANA document reference.

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 D1.0 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D1.0 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** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 778 | Abstract: | 3.01 | The description is unclear. | suggest to modify "This amendment defines modifications to both the IEEE 802.11 physical layer (PHY) and the medium access control (MAC) sublayer for enhanced service with user privacy protection" as "This amendment defines standardized modifications to both the IEEE 802.11 physical layer (PHY) and the medium access control (MAC) that enable enhanced service with user privacy protection" | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 778 |
| 144 |   | 3.01 | The abstract refers to an "enhanced service". What is this enhanced service. I thought this amendment was about privacy protection? | Change the cited sentence to "This amendment defines modifications to both the IEEE 802.11 physical layer (PHY) and the IEEE 802.11medium access control (MAC) sublayer for enhanced user privacy protection." Also make the same change for the introduction on P8L9. | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 778 |
| 163 |   | 3.01 | It is said that there are modifications to the PHY but none of the PHY sections are modified. Is the transition operation for EDP Epoch counted as PHY related part? But modifications to the PHY seems to be saying too much. | Change the sentence to "This amendment defines modifications to the IEEE 802.11 medium access control (MAC) sublayer for ..." and the same change to pp.ll 8.9. Delete "PHY, physical later, " from the Keywords. | Revised – We note that one of the feature introduced in 11bi is to encrypt the beamforming/CSI/CQI report which is related to sounding, a physical layer feature. However, agree that physical layer needs to be removed from the keywords because it is already there in the baseline. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 145 |
| 145 |   | 3.04 | Why are MAC and PHY defined as keywords? These are also keywords in the baseline. | Delete the keywords for PHY and MAC. | Revised –Agree that MAC and PHY are already keywords in the baseline. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 145 |
| 370 |   | 1.50 | Copyright should be 2025 | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 370 |
| 571 |   | 0.00 | There should not be a space before a closing paren | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 571 |
| 508 |   | 0.00 | "management frame" should be "Management frame" unless followed by "protection" | Fix at 73.32/58, 96.9 | Revised – Agree in principle with the commenter. Also robust management frame does not have upper case M in the baseline.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 508 |
| 574 |   | 0.00 | There are two \s | Delete both of them | Revised – Agree in principle with the commenter. Also robust management frame does not have upper case M in the baseline.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 574 |
| 503 |   | 0.00 | There are sexless quotes (') all around the places that need to become sexy (first one at 72.30). Ditto double sexless quotes | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 503 |
| 371 | 3.2 | 21.17 | Technically speaking, "AP" has not been expanded on first use, only "non-AP" has | Raise in Editors' group | Rejected –We note that in the baseline, only the first instance of AP is expanded as shown in the following example.***directed multicast service:*** *[DMS] A service in which the access point (AP) transmits group addressed**frames as individually addressed frames to the requesting non-AP station (STA).****traffic filtering service:*** *[TFS] A service provided by an access point (AP) to a non-AP station (STA) to**reduce the number of frames sent to the non-AP STA by not forwarding individually addressed frames**addressed to the non-AP STA that do not match traffic filters specified by the non-AP STA.* |
| 984 | 3.2 | 21.18 | The text "indicated by an enhanced data privacy (EDP) non-access point (non-AP) station (STA) to an EDP AP or anEDP non-AP multi-link device (MLD) to an EDP AP MLD and" is not needed in a definition | Update definition to "A MAC address used by an enhanced data privacy (EDP) AP or EDP AP multi-link device as the address to notify the DS and establish the destination mapping for an EDP non-access point (non-AP) STA or EDP non-STA MLD after (re)association. | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 984 |
| 963 | 4.10.2 | 25.20 | Baseline does not use normative verb "may" in Clause 4 and I see no reason to change that in P802.11bi. | Revert the change from "are" to "may be", i.e., change "EAPOL PDUs may be transmitted" back to "EAPOL PDUs are transmitted" | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 963 |
| 12 | 4.10.7 | 25.55 | "A STA can supply a list of PMK identifiers in the (Re)Association Request frame or first FILS Authentication frame or first IEEE 802.1X Authentication frame or first EDPKE Authentication frame." Needs some definite articles | Edit cited as follows: "A STA can supply a list of PMK identifiers in the (Re)Association Request frame or the first FILS Authentication frame or the first IEEE 802.1X Authentication frame or the first EDPKE Authentication frame." | Accepted -  |
| 305 | 4.10.7 | 25.55 | The text "A STA can supply a list of PMK identifiers in the (Re)Association Request frame or first FILS Authentica-tion frame or first IEEE 802.1X Authentication frame or first EDPKE Authentication frame. Each PMKidentifier names a PMKSA. The Authenticator can specify the selected PMK identifier in message 1 of the4-way handshake or the second FILS Authentication frame or the second IEEE 802.1X Authenticationframe or the second EDPKE Authentication frame. The selection of the PMK identifiers to be included bythe STA and Authenticator is out of the scope of this standard." has too many first and second. Maybe it can be unify so you say "A STA can supply a list of PMK identifiers in the (Re)Association Request frame or on the first Authentication frame of the FILS, IEEE 802.1X , or EDPKE Authentication procedures."Same for second | as in the comment | Rejected – It is important that the first Authentication frame has a list and the second Authentication frame has the selected one. |
| 377 | 4.2.5 | 23.16 | "Within IEEE Std 802.11, EAPOL PDUs are carried as MSDUs within one or more Data frames or are carried within Authentication frames (see 12.16.5 (IEEE 802.1X authentica-tion utilizing Authentication frames))" -- xref not needed here (not used in baseline text) | Delete the parenthesis | Accepted - |
| 380 | 4.2.5 | 23.60 | Missing full stop at end of sentence | As it says in the comment | Accepted -  |
| 324 | 4.5.4.2 | 23.60 | missing period | add period at the end of sentence. | Accepted - |
| 10 | 4.5.4.2 | 23.36 | Now we have so many authentication methods (7), for easier reading I suggest that they be bulleted. | Re-write this clause. List the 7 Authentication methods in bulleted form. Then add the descriptions to each bullet. May need to consult the 11mf editor(s). | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 10 |
| 302 | 4.5.4.2 | 23.36 | At the beginning of clause 4.5.4.2 Authentication, the two initial paragraphs do say the same, but with different words, although one looks like is generic for IEEE 802.11 and the other for RSNA. Maybe it would be good to integrate both paragraphs in a single one. | Integrate paragraph starting in 36 with the one in 53. | Rejected – We note that for the second paragraph, the RSNA does not support open authentication.  |
| 928 | 4.5.4.2 | 24.07 | The changes that are made do not appear to be correct. I thought it should be, "A or B is" or "A and B are" | Please check if the change si accurate | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 928 |
| 13 | 6.5.5.2.2 | 27.44 | "dot11EDPIEEE8021XAuthenticationUtilizi ngAuthenticationFrameActivated. " Incorrect space | Delete space between Utilizi" and "ng" | Accepted |
| 14 | 6.5.5.3.2 | 28.56 | "dot11EDPIEEE8021XAuthenticationUtilizi ngAuthenticationFrameActivated. " Incorrect space | Delete space between Utilizi" and "ng" | Accepted |
| 15 | 6.5.5.4.2 | 29.56 | "dot11EDPIEEE8021XAuthenticationUtilizi ngAuthenticationFrameActivated. " Incorrect space | Delete space between Utilizi" and "ng" | Accepted |
| 16 | 6.5.5.5.2 | 30.42 | "dot11EDPIEEE8021XAuthenticationUtilizi ngAuthenticationFrameActivated. " Incorrect space | Delete space between Utilizi" and "ng" | Accepted |
| 402 | 9.3.3 | 0.00 | Sometimes it's "otherwise, it is not present" sometimes "otherwise not present" | Pick one (the most popular baseline one) throughout 9.3.3 | Revised – We note that in baseline there are 17 instances of otherwise not present and 139 instances of otherwise, it is not present. We change only the part that are added by 11bi.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 402 |
| 191 | 9.3.3.11 | 39.05 | extra Not word. | Delete "Not". | Rejected –Search “not” in 9.3.3.11 and does not have extra Not word. |
| 404 | 9.3.3.11 | 37.55 | "the number of octets of the Encapsulation field" would be more canonical as "the length in octets of the Encapsulation field" | As it says in the comment | Rejected – We note that “the number of octets” is the typical description of length field. *The Length field indicates the number of octets in the element excluding the Element ID and Length fields.* |
| 406 | 9.3.3.11 | 37.59 | Missing full stop at end of sentence | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 406 |
| 408 | 9.3.3.11 | 37.55 | "The Encapsulation Length field indicatesthe" should for consistency with other rows be "This field indicates" or just "The" | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 408 |
| 411 | 9.3.3.11 | 0.00 | Inconsistent "may be present" or "is optionally present" | Pick one (the most popular baseline one) throughout 9.3.3.11 | Revised – Agree in principle with the commenter. We change to “is optionally present”.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 411 |
| 412 | 9.3.3.11 | 42.57 | "wrapped data format in PASN Parameters element is nonzero" missing article | Change to "wrapped data format in the PASN Parameters element is nonzero", also next 2 rows | Revised – Agree in principle with the commenter. We change to “is optionally present”TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 412 |
| 400 | 9.3.3.8 | 37.11 | "; or if" spurious semicolon | Delete said semicolon | Revised –Agree in principle with the commenter. In the baseline, there are 7 instances of “; or if” and 34 instances of “, or if”. We use “, or if”.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 400 |
| 422 | 9.4.1.82 | 46.55 | "The Encapsulation field carries the EAPOL PDU." -- no antecedent | Change to "The Encapsulation field carries an EAPOL PDU." | Accepted |
| 419 | 9.4.1.9 | 45.14 | Inconsistent presence or absence of full stop at end of each cell | Match baseline | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 419 |
| 456 | 9.4.2.1 | 50.56 | Leftmost cell should not have "element" but should have xref (3x) | Fix last 3 rows | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 456 |
| 461 | 9.4.2.23.5 | 57.33 | "If PMKSA caching privacy is used, the changed PMKID" would be more consistent with other rows as "The changed PMKID, if PMKSA caching privacy is used". Ditto bullet da) | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 461 |
| 40 | 9.4.2.240 | 59.41 | "Otherwise, this subfield is set to 0." It is called the "EDP Robust Individually Addressed Management Frame Support field", hence "subfield" should be "field" | At 59.41 change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 41 | 9.4.2.240 | 59.52 | "subfield" should be "field" | At 59.52 change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 42 | 9.4.2.240 | 60.09 | "subfield" should be "field" | At 60.9 change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 43 | 9.4.2.240 | 60.16 | "An EDP STA sets the EDP CapabilitiesAnd Operation Parameters Request/Response subfield to 1" All other entries use "field" is this differenT. I think that 11m prefers field and noit subfield. | At 60.16 and 60.20, change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 44 | 9.4.2.240 | 60.28 | "subfield" should be "field" | At 60.28 change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 45 | 9.4.2.240 | 60.37 | "subfield" should be "field" | At 60.37 change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 46 | 9.4.2.240 | 60.42 | "subfield" should be "field" | At 60.42 change "subfield" to "field" | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 453 |   | 0.00 | Some instances of "subfield" have been inserted | Change to "field" throughout | Revised –Agree in principle with the commenter. We change all subfield in 9.4.2.240 to field. Usage of subfield is deprecated. See https://mentor.ieee.org/802.11/dcn/09/11-09-1034-21-0000-802-11-editorial-style-guide.docxTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 40 |
| 155 | 9.4.2.347 | 60.37 | This paragraph is almost impossible to parse and does not read well, especially the "...non-AP MLD or a non-AP MLD...". The paragraph does make sense, but it needs to be re-formatted. | Replace the cited sentence with: "The destination MAC Address element is used by either a:\* non-AP STA that is not affiliated with a non-AP MLD or\* non-AP MLD to provide the destination MAC address to the AP or an AP MLD, respectively, for the DS mapping." | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 155 |
| 1003 | 9.4.2.347 | 61.07 | "a non-AP STA that is not affiliated with a non-AP MLD or a non-AP MLD" is confusing to read since the "or" could be indicating alternatives between a "non-AP MLD" and a "non-AP MLD". | Replace with "a non-AP STA that is not affiliated with a non-AP MLD, or a non-AP MLD". That is, insert a comma ',' after the first occurrence of "non-AP MLD". | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 468 |
| 468 | 9.4.2.347 | 61.07 | "The DS MAC Address element is used by a non-AP STA that is not affiliated with a non-AP MLD or a non-AP MLD" is fantastically confusing | Change to "The DS MAC Address element is used by a non-AP MLD or by a non-AP STA that is not affiliated with a non-AP MLD" and then "AP or an AP MLD" to "AP MLD or an AP" later on in the sentence | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 468 |
| 1004 | 9.4.2.347 | 61.07 | This element is used with EDP, but this is not clear from the description | Clarify that the element is used with EDP | Rejected – Normative behavior is not described in clause 9. Corresponding normative behavior is in clause 10.71. |
| 977 |   | 0.00 | It is unclear that a non-AP STA or MLD must have a DS MAC address to use EDP. The requirement for a STA or MLD to provide the DS MAC address should be clearly stated.. | Clearly state that to use EDP features a STA or MLD must provide a DS MAC address. | Rejected – Normative behavior for using frame anonymization requires DS MAC address support and is described in clause 10.71. No specific requirement to mandate DS MAC address in other cases. For example, to reduce content in probe request frame, there is no need to support DS MAC address. |
| 61 | 9.6.32.4 | 65.06 | I notice that there are a lot of hyperliinks missing, for example, on page 65 lines 6,9,18,22,63 | Fix cited links pand check thru the document. | Rejected – If a referred clause is not modified by 11bi, then likely it will not have hyperlink since that paragraph does not exist in 11bi. The hyperlink will be there once the 11bi is incorporated into TGm draft.The cited instances fall into this specific case. |
| 935 | 9.6.42.1 | 69.03 | To avoid any confusion, I recommend adding "EDP" in front of "Capabalities and Operation Parameters Request" and "Capabilities and Operation Parameters Request in all occurences (and no, not when there is alerady an EDP in front) | As suggested in comment | Revised –Agree in principle with the commenter. Note that 12.16.4 has EDP in front of the frame in all instances.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 935 |
| 1009 | 9.6.42.2 | 69.31 | "Table ... and Table .... Only one of the tables will be used, so "and Table" is incorrect | Replace "and Table" with "or Table" | Accepted -  |
| 494 | 9.6.42.2 | 69.46 | Order should be 2 not 3 | As it says in the comment | Accepted |
| 754 | 9.6.42.2 | 70.06 | Why is dialog token 3 for non MLO, and 2 for MLO, while 2 is unused for non MLO? | Unify both tables, and simply indicate that Basic Multi link only applies to MLDs. Alternatively, change 9-658v Dialog token to '2' instead of 3. | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 494 |
| 498 | 9.6.42.3 | 71.14 | Font too small | As it says in the comment | Revised –TGbi editor to fix the font size of the instance. |
| 334 | 9.6.42.3 | 70.17 | Awkward wording: "parameters to be responded in a ...frame" | Change to: "parameters to be provided in a ...frame." | Accepted |
| 1010 | 9.6.42.3 | 70.22 | "Table ... and Table .... Only one of the tables will be used, so "and Table" is incorrect | Replace "and Table" with "or Table" | Accepted - |
| 557 | 10.71 | 0.00 | There are a bunch of "<blah> action frame"s. The "action" in all of them is spurious | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 557 |
| 679 | 12 | 0.00 | 4x "If FT protocol" missing article | Change each to "If the FT protocol" | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 679 |
| 664 | 12.16.1 | 118.53 | "Clause 12.16" should be "Subclause 12.16" | As it says in the comment | Revised –Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 664  |
| 665 | 12.16.1 | 118.53 | "when the functions in Clause 12.16 (Client Privacy Enhancement) supersede the functions in 12.2.11 (Requirements for support of MAC privacy enhancements)." -- so when is that? | Change "when" to "that" | Rejected –We note that “except when” is used per the new style to put new functionality in a separate clause in the baseline.*An HE STA (#7024)has a MAC and MLME that comprises the functions defined in Clause 26 (Highefficiency**(HE) MAC specification(11ax)) as well as the functions defined in Clause 10 (MAC sublayer**functional description), the MLME functions defined in Clause 11 (MLME), and the security functions**defined in Clause 12 (Security), except when the functions in Clause 26 (High-efficiency (HE) MAC**specification(11ax)) supersede the functions in Clause 10 (MAC sublayer functional description) or**Clause 11 (MLME).* |
| 666 | 12.16.2 | 118.60 | "a multi-link probe request to preserve privacy" -- bad case. And Probe Requests' aim isn't to preserve privacy | As it says in the comment | Revised – “multi-link probe request” is used in 11be without upper case. Agree that Probe request is not used to preserve privacy, but the subclause define the contents of the Probe Request to preserve privacy.*“This subclause defines rules for the contents of a Probe Request frame that is not a multi-link probe request**to preserve privacy.”* |
| 668 | 12.16.2 | 119.22 | Vendor-specific elements should be at the end | As it says in the comment | Revised – Agree in principle with the commenter. We adjust the order of the description in the note.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 664 |
| 159 | 12.16.3 | 119.20 | The title of clause 12.16.3 uses the word "EDP", although it a subclause to 12.16 Client Privacy Enhancement. Therefore the word "EDP" is redundant. | Rename the cited clause title to "Robust Individually Addressed Management Frame and Robust IndividuallyAddressed Beamforming/CSI/CQI Frame". The same change should be made to clause 12.16.4. | Accepted - |
| 669 | 12.16.3 | 119.40 | Font size wonky | As it says in the comment | Revised – TGbi editor fixes the font size in Table 12-13a to 9 |
| 670 | 12.16.3 | 120.09 | ", with which management frame protection is negotiated" duplicates the para before the bullets. Ditto line 63 | Delete the cited text | Accepted - |
| 776 | 12.16.3 | 119.40 | Check font size consistency in Table 12-13a, some items in the robust column seem to use a bigger one (same for Table 12-13b) | As in comment | Revised – TGbi editor fixes the font size in Table 12-13b to 9 |
| 138 | 12.16.4 | 121.12 | The frame name defined in clause 9 has no "EDP": Capabilities And Operation Parameters Request frame, Capabilities And Operation Parameters Response frame | Use a consistent name for the frame. | Revised –Agree in principle with the commenter. We have added EDP in clause 9.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 935 |
| 844 | 12.16.4 | 121.12 | Missing word "with" | Insert the word "with" in "This subclause defines rules to request and respond with capabilities and operation parameters..." | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 844 |
| 671 | 12.16.4 | 121.11 | "This subclause defines rules to request and respond capabilities and operation parameters" -- weird verb | Change "respond" to "provide" | Revised – We add “with” after respond.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 844 |
| 672 | 12.16.4.1 | 121.36 | "except Multi-Link element and Multiple BSSID element" missing article. Also 122.6 | As it says in the comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 672 |
| 673 | 12.16.4.1 | 121.34 | "The EDP Capabilities And Operation Parameters Response frame shall include all elements that will be included in a Probe Response frame except Multi-Link element and Multiple BSSID element and shall be in the order defined for a Probe Response frame. " -- this "will" makes no sense. Ditto 122.6 | Change to "would" | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 673 |
| 674 | 12.16.4.2 | 122.07 | " and shall be in the order defined for a Probe Response frame." doesn't work in the sentence | Make a new sentence: "The elements shall..." | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 674 |
| 765 | 12.16.4.2 | 121.42 | The first sentence of 12.16.4.2 seems to show a manadatory action for an MLD. So, "set" should be "shall set". | As in comment. | Accepted - |
| 677 | 12.6.6.1 | 124.39 | "If the FILS authentication" spurious article. Also 126.17 | Delete said article | Revised - In the baseline, “the” is used if we refer to “FILS authentication protocol”. To align with “the FT protocol”, we simply add protocolTGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 677 |
| 682 | 12.6.6.2 | 125.47 | "then" is spurious | Delete the cited text | Accepted - |
| 647 | 12.5.2.4.4 | 106.19 | "EDP robustBeamforming/CSI/CQI frames" missing space and bad case. Bad case at 106.29 too. And lines 45 and 51 are even more of a car crash. The same issues apply in Subclause 12.5.4.4.4 | As it says in the comment | Revised – We fixed the space. EDP robust Beamforming/CSI/CQI is the set of frames defined for protection. Does not observe further space issue in 12.5.4.4.4.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 647 |
| 651 | 12.6.7 | 111.62 | "IEEE 802.1X Authentication Utilizing Authentication Frame" should be lowercase and plural except IEEE and Authentication | As it says in the comment | Accepted |
| 652 | 12.6.7 | 112.41 | "FILS Authentication frame (when FILS authentication is used) or IEEE 802.1X Authentication frame (when PTKSA derivation with IEEE 802.1X Authentication frame exchange is used) or EDPKE Authentication frame (when EDPKE authentication is used) or (Re)Association Request frame and message 1 of the FT 4-way handshake (otherwise)" -- too many ors. Also at line 19 and 113.12 | Replace all but the last or with commas | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 652 |
| 653 | 12.6.7 | 113.01 | "The procedure for the PTKSA derivation with IEEE 802.1X Authentication frame exchange and PMKSA caching is defined in 12.16.8.2 (IEEE 802.1X).The procedure for EDPKE authentication exchange and PMKSA caching is defined in 12.16.9 (Enhanced Data Privacy Key Exchange)." -- the "the" from the first sentence needs to be moved to the second | Replace all but the last or with commas | Rejected –Not clear on why “the” in two different sentences are related. The suggested change also does not match the comment. |
| 175 | 12.16.7 | 127.35 | Additional "time" in "to be used next time time to the" | As in comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 175 |
| 271 | 12.16.7.1 | 131.54 | The sentence does not read well. | Now the if statement is immediately after shall which does not read well. Please reorder the sentence. | Rejected – The page and line number is in 12.16.8.2 IEEE 802.1X and there is no if after shall in the referenced page and line number. |
| 272 | 12.16.7.1 | 131.62 | The sentence does not read well. | Upon immediate after shall does not read well. Please reorder the sentence. | Rejected – The page and line number is in 12.16.8.2 IEEE 802.1X and there is no if after shall in the referenced page and line number. |
| 686 | 12.16.7.2 | 127.65 | "wher" should be "where" | As it says in the comment | Accepted – |
| 766 | 12.16.7.2 | 127.65 | "wher:" must be "where:". | As in comment. | Accepted – |
| 276 | 12.16.8.1 | 132.30 | The list does not read well, if statement is immediately after shall. | Please restructure the bullets so that if statement is not immediately after shall statement. | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 276 |
| 277 | 12.16.8.1 | 132.57 | The second last bullet does not read well. | Change to :" verify the MIC in FTE by using the S1KH of FTE. | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 277 |
| 278 | 12.16.8.1 | 132.57 | The last bullet should be combined with the second last bullet. | Please add:" if the verification of the MIC in FTE fails". | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 278 |
| 279 | 12.16.8.1 | 133.08 | All bullets discuss on the elements and fields of the first Authentication frame. The first authentication frame should be moved to the first sentence before the list to avoid repetition for each bullet separately | Please include to the end of line 8 that first Authentication frame shall contain the following elements:" and reduce the repetition on the bullets. | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 279 |
| 282 | 12.16.8.1 | 133.33 | The bulleted list talks first on the first authentication frame rejection. Then the bullets talk about the content of the second Authentication frame.These operations should be described in the separate lists.The second authenticaiton frame should be moved to the common sentence of the second list. | Please split the list into two lists:1) RX and validation of the authentication frame 1,2) Content of the second authentication frame. | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 282 |
| 688 | 12.16.8.1 | 128.38 | "receives the RSNXE" should be "receives an RSNXE". Ditto at 130.21 | As it says in the comment | Accepted -  |
| 689 | 12.16.8.1 | 0.00 | There are 9x "message of the FT protocol" but the protocol doesn't really have a message, the exchange performed per the protocol has messages | Change to "... FT exchange" | Rejected – In 13.8 FT authentication sequence, the descriptions uses message. |
| 691 | 12.16.8.1 | 0.00 | Sometimes it's "first message", sometimes "message 1". This makes it harder to identify the requirements. Ditto 2 and second | Pick one and stick to it | Revised - Agree in principle with the commenter. We use first/second message.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 691 |
| 692 | 12.16.8.1 | 129.05 | "the message 1" should be just "message 1". Also at 130.1 | As it says in the comment | Revised - Agree in principle with the commenter. We revise message 1 with the first message.TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 691 |
| 693 | 12.16.8.1 | 129.13 | "Upon completion of PTK generation, the shared secret, DHss, shall be irretrievably deleted." does not follow "shall" | Change to "Irretrievably delete the shared secret, DHss, upon completion of PTK generation." | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 276 |
| 694 | 12.16.8.1 | 129.17 | "Indicate chosen finite cyclic group" missing article. Also at 131.28. Also "Calculate MIC" at line 21 and "Include MIC" at line 38 | As it says in the comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 694 |
| 695 | 12.16.8.1 | 129.21 | "Calculate MIC in the FTE as follows:\* Use the key, the algorithm, and the MIC size as defined in 13.8.5 (FT authentication sequence:contents of fourth message).\* On the concatenation of the following data, in the order given here as the input:" is weird | Change to "Calculate the MIC in the FTE by using the key, the algorithm, and the MIC size as defined in 13.8.5 (FT authentication sequence: contents of fourth message) on the concatenation of the following data, in the order given here as the input:" | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 695 |
| 162 | 12.16.8.2 | 131.43 | Optional elements of a negated list use "nor" | Change the cited sentence to "Otherwise, a responder shall not include a Diffie-Hellman Parameter element nor a Nonce element nor anRSNE in the second Authentication frame for IEEE 802.1X authentication". A similar change should be made to P130L46. | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 162 |
| 702 | 12.16.8.2 | 130.26 | "Include an RSNE in the first Authentication frame to indicate AKM and pairwise cipher suite. Ver-sion field shall be set to 1. Pairwise Cipher Suite Count field shall be set to 1. AKM Suite Count field shall be set to 1. PMKID count and PMKID list set corresponding to PMKSA identifiers if exists. " is missing zillions of articles and the last sentence is not clear | As it says in the comment | Revised - Agree in principle with the commenter.The last sentence has been used in the baseline “All other fields shall be as specified in 9.4.2.23 (RSNE)”. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 702 |
| 704 | 12.16.8.2 | 130.63 | "in the first Authentication frame" -- duplication, since whole list is about this. Similarly 131.3 | Delete the cited text | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 279 |
| 705 | 12.16.8.2 | 131.07 | "Verify that a PMKSA named via a PMKID in the RSNE exists for the specified AKM." -- the PMKID list is optional | Change to "If one or more PMKIDs are included, verify that at least one of them exists for the specified AKM" | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 705 |
| 709 | 12.16.8.2 | 131.28 | "Indicate chosen finite cyclic group" missing article | As it says in the comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 694 |
| 710 | 12.16.8.2 | 131.38 | "Derive PTK" missing article. Also at 132.26/34 | As it says in the comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 710 |
| 711 | 12.16.8.2 | 131.37 | "a responder" should be "the responder" | As it says in the comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 282 |
| 712 | 12.16.8.2 | 0.00 | "AKM suite selector element" should be "AKM Suite Selector element" (3x) | As it says in the comment | Accepted - |
| 713 | 12.16.8.2 | 131.65 | "The validation of AKM is based on the AKM indication in RSNE rather than AKM suite selector element as defined 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames).", well, yeah, duh, since there is no AKM suite selector (sic) element | Delete the cited text | Accepted - |
| 714 | 12.16.8.2 | 132.08 | " one or more PMKID" should be " one or more PMKIDs" | As it says in the comment | Accepted |
| 715 | 12.16.8.2 | 132.12 | "If verification succeeds, use PMKSA caching with the PMKSA identified by the PMKID indicated in the second Authentication frame and does not con-tinue the IEEE 802.1X Authentication frame exchange" -- grammar all over the place | Change to "If verification succeeds, the originator shall use PMKSA caching with the PMKSA identified by the PMKID indicated in the second Authentication frame and shall not continue the IEEE 802.1X Authentication frame exchange" | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 715 |
| 716 | 12.16.8.2 | 132.31 | "If a PMKSA is not identified due to PMKSA caching" ambiguous. Also line 38 | Change to "If a PMKSA is not identified through PMKSA caching" | Accepted - |
| 718 | 12.16.8.2 | 132.47 | "PMKID list" should be "PMKID List". Also line 54 | As it says in the comment | Accepted - |
| 719 | 12.16.8.2 | 132.50 | "Responder shall" missing article | As it says in the comment | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 719 |
| 852 | 12.16.8.2 | 132.10 | Typo: "Encapulation" should be "Encapsulation" | Replace "Encapulation" with "Encapsulation" | Accepted - |
| 298 | C.3 | 139.29 | Allocation for "dot11EDPStationConfigTable ::= { dot11smt 50 }" is not recorded on dot11smt sheet of the latest ANA database (11-11/0270r76) | Please get allocation for it | Revised –This is updated in <https://mentor.ieee.org/802.11/dcn/11/11-11-0270-77-0000-ana-database.xls> |
| 743 | C.3 | 141.37 | "support EDP robust individually addressed Management frame" should be plural | As it says in the comment | Accepted - |
| 768 | C.3 | 140.12 | A comma is missing after "TruthValue". | Please add a comma after "TruthValue". | Accepted - |
| 6 |   | 0.00 | No commentsLooks good to me |   | Rejected –Thanks for participating the ballot. |
| 8 |   | 0.00 | no comment |   | Rejected –Thanks for participating the ballot. |
| 421 | 9.4.1.9 | 45.14 | Status codes need to be assigned by ANA | As it says in the comment | Revised –This is updated in <https://mentor.ieee.org/802.11/dcn/11/11-11-0270-77-0000-ana-database.xls> |
| 455 | 9.4.2.1 | 0.00 | Element IDs need to be assigned by ANA | As it says in the comment | Revised –11bi editor has requested all numbers from ANA handler. 11bi editor to contact the ANA database handler to update the ANA database document to the latest version. |
| 460 | 9.4.2.23.3 | 57.10 | AKM selectors should be allocated by ANA | As it says in the comment | Rejected – EDPKE AKM assignment is in the latest ANA database. See https://mentor.ieee.org/802.11/dcn/11/11-11-0270-76-0000-ana-database.xls |
| 734 | C.3 | 0.00 | Don't MIB node numbers have to be allocated by ANA? | As it says in the comment | Revised –This is updated in <https://mentor.ieee.org/802.11/dcn/11/11-11-0270-77-0000-ana-database.xls> |
| 737 | C.3 | 140.24 | I think there's usually a blank line between the boilerplate and other stuff in the DESCRIPTION | As it says in the comment | Revised –TGbi editor to add additional blank line in the DESCRIPTION and follows the format. |
| 591 |   | 0.00 | Use minuses not hyphens in equations | As it says in the comment | Revised –TGbi editor to update hyphen to minus sign in equations (ex in 10.71.6.4). |
| 424 |   | 0.00 | Weirdly, the font in the first cell of many figures (e.g. Figure 9-207k--EDP Epoch Settings field format) appears to be a serif font, not a non-serif one. Actually, sometimes the last cell is messed up too | Use the baseline font throughout | Revised –TGbi editor to check and fix fonts of all figures. |
| 748 |   | 0.00 | Please find out from the TGm Editors how to make hyphens soft enough not to be copied when you copy text from the document | As it says in the comment | Revised –Thanks for the suggestion. The current best approach is to copy the entire texts and select raw texts when copy to framemaker. It is possible that the original text is not minus sign but hyphen. TGbi editor to double check copied minus sign and quotation in the future. |
| 458 |   | 0.00 | "Enhanced Data Privacy (EDP) element " -- elements have exactly one name | Either "EDP element" or "Extended Data Privacy element" throughout | Revised - Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0295 under all headings that include CID 458 |

***Proposal:***

**TGbi Editor: *Instruction: Modify Abstract as shown below***

**Abstract:** This amendment defines modifications to both the IEEE 802.11 physical layer (PHY) and the medium access control (MAC) sublayer that enhance user privacy protection.(#778)

**TGbi Editor: *Instruction: Modify Keywords as shown below***

**Keywords:** EDP, enhanced data privacy(#145)

**TGbi Editor: *Instruction: Modify first page Copyright year as shown below***

Copyright © 2025 by the IEEE.(#370)

**TGbi Editor: *Instruction: Modify C.3 MIB detail as shown below***

…(existing texts)…

dot11EDPGroupEpochCurrentGroup OBJECT-TYPE

SYNTAX Unsigned32 (0..255)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

This attribute indicates the current EDP epoch group to which the non-AP

MLD is assigned. A value of zero (0) indicates the non-AP MLD is assigned

to the default group. A null value indicates that the non-AP MLD is not

currently assigned to an epoch group."

DEFVAL { NULL }(#571)

::= { dot11EDPStationConfigEntry 5 }(#571)

…(existing texts)…

dot11DSMACAddressActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable. It is written by an external management

entity or the SME. Changes take effect for the next MLME-START.request

primitive or MLME-JOIN.request primitive. This attribute, when true, indicates

the capability to support DS MAC Address is enabled. The capability

is disabled otherwise."

DEFVAL { false }

::= { dot11EDPStationConfigEntry 11 }(#571)

**TGbi Editor: *Instruction: change management frame to Management frame in the following instances.(#508)***

**9.6.42.8 Privacy Beacon Solicit Request frame format**

The Privacy Beacon Solicit Request frame is transmitted as non-protected Management frame to the broadcast address. The frame solicits unprotected Privacy Beacon frame transmissions as a response to the frame as described in 10.71.8.1 (BPE AP MLD Discovery).

**9.6.42.9 AID Assignment frame format**

The AID Assignment frame is transmitted as a protected Management frame by a CPE AP. The frame assigns AID values to the receiving CPE STA for the coming epochs.

**10.71.8.3 Group addressed frames anonymization**

To improve the BPE AP privacy, the BPE AP shall use GTK to encrypt the payload of the group addressed Management frames.

**TGbi Editor: *Instruction: Modify 10.71.4 as shown below***

**10.71.4 Establishing BPE frame anonymization parameter sets**

KDF-*Hash*-*Length* is the key derivation function as defined in 12.7.1.6.2 (Key derivation

function (KDF)) using the hash algorithm identified by the AKM suite (#574)

selector (see Table 9-190 (AKM suite selectors))

**TGbi Editor: *Instruction: Modify 10.71.3 as shown below***

**10.71.3 Establishing frame anonymization parameter sets**

n is the current number of the EDP epoch in the EDP epoch sequence as (#574)

defined in 10.71.2.4 (EDP Epoch Start Time Computation)

**TGbi Editor: *Instruction: Modify “`” to “’” across the specification(#503)***

**TGbi Editor: *Instruction: Modify 3.2 as shown below.***

**distribution system (DS) medium access control (MAC) address**: [DS MAC address] A MAC address used by an enhanced data privacy (EDP) access point (AP) or an EDP AP multi-link device (MLD) as the address to notify the DS and establish the destination mapping for an EDP non-AP STA or an EDP non-AP MLD after (re)association. ***(#984)***

**TGbi Editor: *Instruction: Modify 4.10.2 as shown below***

***4.10.2 IEEE 802.11 usage of IEEE Std 802.1X-2020***

***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 are~~are~~ (#963)transmitted in one or more IEEE 802.11 Data frames or Authentication frames and passed via the 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 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.

**TGbi Editor: *Instruction: Modify 4.10.7 as shown below***

* PMKSA caching

***Change the second paragraph as follows (not all lines are shown):***

A STA can supply a list of PMK identifiers in the (Re)Association Request frame or the first FILS Authentication frame or the first IEEE 802.1X Authentication frame or the first EDPKE Authentication frame.(#12) Each PMK identifier names a PMKSA. The Authenticator can specify the selected PMK identifier in message 1 of the 4-way handshake or the second FILS Authentication frame or the second IEEE 802.1X Authentication frame or the second EDPKE Authentication frame. The selection of the PMK identifiers to be included by the STA and Authenticator is out of the scope of this standard.

**TGbi Editor: *Instruction: Modify 4.2.5 as shown below***

* Interaction with other IEEE 802® layers

***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(#377), 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: *Instruction: Modify 4.5.4.2 as shown below***

* Authentication

IEEE Std 802.11 defines the following ~~five~~ IEEE 802.11 authentication methods:.

* 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 EAP to authenticate STAs and the AS with one another.
* 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 authentication allows for the protection of Management frames without association by establishing a PTKSA using authentication frames. (#10)

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, FILS authentication, ~~or~~ PASN authentication, or EDPKE authentication. 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.~~ 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.(#380)

(..existing texts…)

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

PASN authentication or EDPKE authentication is~~is~~ (#928)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: *Instruction: Delete space between Utilizi" and "ng" in 6.5.5.2.2, 6.5.5.3.2, 6.5.5.4.2, 6.5.5.5.2 (#13, #14, #15, #16)***

**TGbi Editor: *Instruction: change “, otherwise, not present” to “; otherwise, it is not present”(#402)***

**TGbi Editor: *Instruction Modify 9.3.3.11 as shown below.***

* 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 | Encapsulation Length | This(#408) field indicates the number of octets of the Encapsulation field. This is present only in certain Authentication frames as defined in Table 9-71.(#406) |
| 9b | Encapsulation | The field is used to carry an EAPOL PDU as described in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames). This is present only when the Encapsulation Length field is nonzero. |
| ... |  |  |

***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 elementsindicated as conditional in Table 9-70 (Authentication frame body) |
| EDPKE authentication | 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 is optionally (#411)present.Wrapped Data element is present if the wrapped data format in the(#412) PASN Parameters element is nonzero and not reserved. |
| EDPKE authentication | 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 is optionally present.(#411)Wrapped data element is present if wrapped data format in the(#412) PASN Parameters element is nonzero and not reserved and Status Code field is 0.MIC element is present. |
| EDPKE authentication | 3 | Status | PASN Parameters element is present if Status Code field is 0.Wrapped data element is present if wrapped data format in the(#412) PASN Parameters element is nonzero and not reserved; and Status Code field is 0.MIC element is present. |

**TGbi Editor: *Instruction Modify 9.3.3.8 as shown below.***

* Reassociation Response frame format

***Change rows in Table 9-67 as follows (not all lines shown):***

* Reassociation Response frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 10 | RSN | An RSNE is present in a Reassociation Response frame if dot11FastBSSTransitionActivated is true, dot11RSNAActivated is true, and this frame is a response to a Reassociation Request frame that contained an FTE (i.e., part of a fast BSS transition in an RSN), or if dot11FILSActivated is true, or ifperforming OWE, or if the Reassociation Response frame is encrypted. Otherwise, not present.(#400) |
| ... |  |  |
| 41 | Key Delivery | The Key Delivery element is present if dot11FILSActivated is true and FILS authentication is used or if the Reassociation Response frame is encrypted; otherwise not present.  |
| ... |  |  |
| <Last assigned+1> | EDP | The EDP element carrying configuration and Group Epoch ID for the assigned group epoch. This element is present if the Ressociation Response frame is encrypted and dot11EDPGroupEpochActivated is true; otherwise, it is not present. |

**TGbi Editor: *Instruction modify 9.4.1.82 as shown below.***

**9.4.1.82 Encapsulation field**

The Encapsulation field carries an(#422) EAPOL PDU.

**TGbi Editor: *Instruction modify 9.4.1.9 as shown below.***

* Status code field

***Insert the following new rows to Table 9-80 while maintaining the numerical order and updating the reserved range (not all lines shown):***

* Status codes

|  |  |  |
| --- | --- | --- |
| Status code | Name | Meaning |
| … |  |  |
| 145 | SUCCESS\_SIMILAR\_EPOCH | The request to join or create a group epoch is successful but the epoch parameters are not exactly the requested.(#419) |
| 146 | FAILURE\_ALREADY\_EXISTING\_EPOCH | The creation of the group epoch fails because the group already exists.(#419) |
| 147 | FAILURE\_MAX\_NUM\_EPOCH\_REACH | Failure to create a group epoch because the maximum number of group epochs at the AP has been reached.(#419) |
| 148 | SUCCESS\_AID\_LIST\_PARTIALLY\_STORED | The AID List is too large and the CPE non-AP MLD has stored it only partially.  |
| 149 | FAILURE\_AID\_LIST\_NOT\_STORED | No AID value has been stored. |
| 150 | FAILURE\_AID\_STORAGE\_TOO\_SMALL | The request to join or create a group epoch has failed, because the AID storage of the non-AP MLD is too small.(#419) |
| 151 | NO\_ASSIGNED\_AID | The non-AP MLD has no AID value for the current epoch.  |

**TGbi Editor: *Instruction Modify 9.4.2.1 as shown below***

* General

***Modify Table 9-130 (Element IDs) as follows:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| ...... |  |  |  |  |
| ~~FILS~~ Nonce (see 9.4.2.188 (FILS Nonce element)) | 255 | 13 | No | No |
| ..... |  |  |  |  |
| DS MAC Address (see 9.4.2.347 (DS MAC Address element)) | 255 | 146 | No | No |
| EDP(#458)(see 9.4.2.348 (EDP element))(#456) | 255 | 147 | Yes | No |
| OTA MAC Collision Warning (see 9.4.2.349 (OTA MAC Collision Warning element))(#456) | 255 | 148 | No | No |
| AID List (see 9.4.2.350 (AID List element))(#456) | 255 | 149 | Yes | Yes |
| ... |  |  |  |  |
| NOTE 1—See 10.28.6 (Element parsing) on the parsing of elements.NOTE 2—Yes for a Reassociation Response frame transmitted during ML resetup by an AP affiliated with an AP MLD, in response to a Reassociation Request frame received from a non-AP STA affiliated with a non-AP MLD. No otherwise. |

**TGbi Editor: *Instruction Modify 9.4.2.23.5 as shown below***

* PMKID

***Change third and fourth paragraph (not all shown) as follows:***

A PMKID in the PMKID List field can refer to

* The PMKID of a cached PMKSA that has been obtained through preauthentication with the target AP
* The PMKID of a cached PMKSA from an EAP, FILS, or SAE authentication
* The PMKID of a PMKSA derived from a PSK for the target AP
* The the changed PMKID if PMKSA caching privacy is used. (#461)
* The PMKR0Name of a PMK-R0 security association derived as part of an FT initial mobility domain association
* The recomputed PMKR0Name as part of a fast BSS transition if PMKSA caching privacy is used. (#461)
* The PMKR1Name of a PMK-R1 security association derived as part of an FT initial mobility domain association or as part of a fast BSS transition.

See 12.7.1.3 (Pairwise key hierarchy), ~~and~~ 12.7.2.6.3 (PMK-R0), and 12.16.7.1 (PMKID privacy) for the construction of the PMKID, 13.8 (FT authentication sequence) for the population of PMKID List for fast BSS transitions, 12.6.8.3 (Cached PMKSAs and RSNA key management) for the population of PMKID List when using PMKSA caching, 13.4 (FT initial mobility domain association) for the population of PMKID List for FT initial mobility domain association, 12.11.2 (FILS authentication protocol) for the population of PMKID List with FILS authentication, ~~and~~ 12.7.1.6 (FT key hierarchy), and 12.16.7.2 (PMKR0Name privacy) for the construction of PMKR0Name and PMKR1Name.

**TGbi Editor: *Instruction Modify 9.4.2.240 as shown below***

* 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 |
| … |  |  |
| 23 | EDP Robust Individually Addressed Management Frame Support | An EDP STA sets the EDP Robust Individually Addressed Management Frame Support field to 1 if dot11EDPRobustIndividuallyAddressedManagementFrameActivated is true. Otherwise, this field(#40) is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame). |
| 24 | EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Tx Support | An EDP STA sets the EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Tx Support field to 1 if dot11EDPRobustIndividuallyAddressedBeamformingCSICQIFrameTxActivated is true. Otherwise, this field(#40) is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame). |
| 25 | EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Rx Support | An EDP STA sets the EDP Robust Individually Addressed Beamforming/CSI/CQI Frame Rx Support field to 1 if dot11EDPRobustIndividuallyAddressedBeamformingCSICQIFrameRxActivated is true. Otherwise, this field(#40) is set to 0. See 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame). |
| 26 | EDP Capabilities And Operation Parameters Request/Response Support | An EDP STA sets the EDP Capabilities And Operation Parameters Request/Response field(#40) to 1 if dot11EDPCapabilitiesAndOperationParametersRequestResponseActivated is true. Otherwise, this field(#40) is set to 0. See 12.16.4 (EDP capabilities and operation parameters request and response procedure). |
| 27 | (Re)Association Frame Encryption Support | An EDP STA sets the (Re)Association Frame Encryption Support field to 1 if dot11EDPReAssociation FrameEncryptionSupportActivated is true. Otherwise, this field(#40) is set to 0. See 12.16.6 ((Re)Association Request/Response Frame Encryption). |
| 28 | IEEE 802.1X Authentication Utilizing Authentication Frame Support | An EDP STA sets the IEEE 802.1X Authentication Utilizing Authentication Frame Support field to 1 if dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated is true. Otherwise, this field(#40) is set to 0. |
| 29 | PMKSA Caching Privacy Support | An EDP STA sets the PMKSA Caching Privacy Support field to 1 if dot11EDPPMKSACachingPrivacySupportActivated is true. Otherwise, this field(#40) is set to 0. See 12.16.7 (PMKSA caching privacy). |
| 30 | Group EDP Epoch Supported | A non-AP MLD sets the Group EDP Epoch Supported field to 1 when dot11EDPGroupEpochActivated is true and sets it to 0 otherwise.  |
| 31 | DS MAC Address Support | The DS MAC Address Support field is set to 1 when dot11DSMACAddressActivated is true and is set to 0 otherwise. |

**TGbi Editor: *Instruction Modify 9.4.2.347 as shown below***

* DS MAC Address element

The DS MAC Address element is used by either(#155) a non-AP MLD or a non-AP STA that is not affiliated with a non-AP MLD to provide the DS MAC address to an AP MLD or an AP,(#468) respectively, for the DS mapping. (#155)

The format of the DS MAC Address element is shown in Figure 9-1074dp (DS MAC Address element format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Element ID | Length | Element ID Extension | DS MAC Address |
| Octets: | 1 | 1 | 1 | 6 |
| * DS MAC Address element format
 |

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

The DS MAC Address field indicates the DS MAC address.

**TGbi Editor: *Instruction Modify 9.6.42.1, 9.6.42.2, 9.6.42.3 as shown below***

* EDP Action field

An EDP Action field, in the octet immediately after the Category field, differentiates the EDP Action frame formats. The EDP Action field values associated with each frame format within the EDP category are defined in Table 9-658u (EDP Action field values).

* EDP Action field values

|  |  |
| --- | --- |
| Value | Meaning |
| 0 | EDP(#935) Capabilities And Operation Parameters Request |
| 1 | EDP(#935) Capabilities And Operation Parameters Response |
| 2 | EDP Group Parameter frame |
| 3 | EDP Epoch Request |
| 4 | EDP Epoch Response |
| 5 | otaMAC Collision Warning |
| 6 | Privacy Beacon Solicit Request |
| 7 | AID Assignment |
| 8-255 | Reserved |

* EDP(#935) Capabilities And Operation Parameters Request frame format

The EDP(#935) Capabilities And Operation Parameters Request frame allows capabilities and operation parameters to be requested in a protected Action frame.

The Action field of the EDP(#935) Capabilities And Operation Parameters Request frame contains the information shown in Table 9-658v (Capabilities And Operation Parameters Request frame Action field format for non-MLO) or(#1009) Table 9-658w (Capabilities And Operation Parameters Request frame Action field format for MLO).

* EDP(#935) Capabilities And Operation Parameters Request frame Action field format for non-MLO

|  |  |
| --- | --- |
| Order | Meaning |
| 0 | Category |
| 1 | EDP Action |
| 2(#494) | Dialog Token |

* EDP(#935) Capabilities And Operation Parameters Request frame Action field format for MLO

|  |  |
| --- | --- |
| Order | Meaning |
| 0 | Category |
| 1 | EDP Action |
| 2 | Dialog Token |
| 3 | Basic Multi-Link element |

The Category field is defined in 9.4.1.11 (Action field).

The EDP Action field is defined in 9.6.42.1 (EDP Action field).

The Dialog Token field is defined in 9.4.1.12 (Dialog Token field) and is set to a nonzero value to identify the request/response transaction.

The Basic Multi-Link element is defined in 9.4.2.322 (Multi-Link element) and is optionally present (see 12.16.4 (EDP capabilities and operation parameters request and response procedure)).

* EDP(#935) Capabilities And Operation Parameters Response frame format

The EDP(#935) Capabilities And Operation Parameters Response frame allows capabilities and operation parameters to be provided(#334) in a protected Action frame.

The Action field of the EDP(#935) Capabilities And Operation Parameters Response frame contains the information shown in Table 9-658x (Capabilities And Operation Parameters Response frame Action field format for non-MLO) or(#1010) Table 9-658y (Capabilities And Operation Parameters Response frame Action field format for MLO).

* EDP(#935) Capabilities And Operation Parameters Response frame Action field format for non-MLO

|  |  |
| --- | --- |
| Order | Meaning |
| 0 | Category |
| 1 | EDP Action |
| 2 | Dialog Token |
| 3 | Beacon Interval  |
| 4 | Capability Information |
| 5 | Elements in order as defined in Table 9-67 (Probe Response frame body) excluding Multi-Link element and Multiple BSSID element |

* EDP(#935) Capabilities And Operation Parameters Response frame Action field format for MLO

|  |  |
| --- | --- |
| Order | Meaning |
| 0 | Category |
| 1 | EDP Action |
| 2 | Dialog Token |
| 3 | Basic Multi-Link element |

The Category field is defined in 9.4.1.11 (Action field).

The EDP Action field is defined in 9.6.42.1 (EDP Action field).

The Dialog Token field is defined in 9.4.1.12 (Dialog Token field) and is set to a nonzero value to identify the request/response transaction.

The Beacon Interval field is defined in 9.4.1.3 (Beacon Interval field).

The Capability Information field is defined in 9.4.1.4 (Capability Information field).

The Basic Multi-Link element is defined in 9.4.2.322 (Multi-Link element) and is optionally present (see 12.16.4 (EDP capabilities and operation parameters request and response procedure)).

**TGbi Editor: *Instruction Modify 10.71 as shown below(#557)***

***Change “OTA MAC Collision Warning action frame” to “OTA MAC Collision Warning frame”***

***Change “AID Assignment action frame” to “AID Assignment frame”***

***Change “AID Assignment Response action frame” to “AID Assignment Response frame”***

**TGbi Editor: *Instruction change “If FT protocol” to “If the FT protocol”(#679)***

**TGbi Editor: *Instruction modify 12.16.1 as follows***

**12.16.1 Introduction**

When dot11MACPrivacyActivated is true, an EDP STA or an EDP MLD has a MAC that comprises the

functions defined in 12.2.11 (Requirements for support of MAC privacy enhancements) except when the

functions in (#664)12.16 (Client Privacy Enhancement) supersede the functions in 12.2.11 (Requirements

for support of MAC privacy enhancements).

**TGbi Editor: *Instruction modify 12.16.2 as follows***

**12.16.2 Contents of Probe Request frame**

NOTE 1—The inclusion of the Request element, the SSID List element, the Extended Request element, the FILS

Request Parameters element, the Short SSID List element, the Known BSSID element, and the Vendor Specific elements(#668) is optional as described in Table 9-66 (Probe Request frame body) and an EDP non-AP STA can omit these elements to preserve privacy.

**TGbi Editor: *Instruction modify 12.16.3 as follows***

**12.16.3 (#159)Robust Individually Addressed Management Frame and Robust Individually**

**Addressed Beamforming/CSI/CQI Frame**

When performing operations that need to use any individually addressed Management frame that is not

robust described in Table 12-13a (EDP robust individually addressed Management frame and its corresponding

individually addressed Management frame that is not robust), if management frame protection is

negotiated and both STAs set the EDP Robust Individually Addressed Management Frame Support field in

the RSNXE that they transmit to 1, the STAs shall

**…….**

— discard any individually addressed Management frame that is not robust described in Table 12-13a

(EDP robust individually addressed Management frame and its corresponding individually

addressed Management frame that is not robust) from the peer STA(#670)

**TGbi Editor: *Instruction modify 12.16.4 as follows***

**12.16.4 (#159)Capabilities and operation parameters request and response procedure**

This subclause defines rules to request and respond with(#844) capabilities and operation parameters using an EDP

Capabilities And Operation Parameters Request frame and an EDP Capabilities And Operation Parameters

Response frame.

* Non-MLO

For non-MLO, a non-AP STA that sets the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1 may send an EDP Capabilities And Operation Parameters Request frame without a Basic Multi-Link element to request capabilities and operation parameters from an associated AP that sets the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1.

An AP that sets the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1 and receives an EDP Capabilities And Operation Parameters Request frame without a Basic Multi-Link element shall respond with an EDP Capabilities And Operation Parameters Response frame without a Basic Multi-Link element. An AP that sets the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1 may transmit an unsolicited EDP Capabilities And Operation Parameters Response frame without a Basic Multi-Link element to an associated non-AP STA that sets the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1. The EDP Capabilities And Operation Parameters Response frame shall include all elements that would(#673) be included in a Probe Response frame except the(#672) Multi-Link element and the(#672) Multiple BSSID element, and the elements(#674) shall be in the order defined for a Probe Response frame.

* MLO

For MLO, all STAs affiliated with an MLD shall(#765) set the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to the same value.

A non-AP STA affiliated with a non-AP MLD that sets the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1 may send an EDP Capabilities And Operation Parameters Request frame with a Basic Multi-Link element to request capabilities and operation parameters of APs affiliated with an associated AP MLD if APs affiliated with the associated AP MLD set the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1.

If APs affiliated with an AP MLD set the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1 and the AP MLD receives through a setup link from an associated non-AP MLD an EDP Capabilities And Operation Parameters Request frame with a Basic Multi-Link element, then the AP MLD shall respond with an EDP Capabilities And Operation Parameters Response frame through an affiliated AP over a setup link to the non-AP MLD. If APs affiliated with an AP MLD set the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1, the AP MLD may send an unsolicited EDP Capabilities And Operation Parameters Response frame to an associated non-AP MLD through a setup link, where non-AP STAs affiliated with the non-AP MLD set the EDP Capabilities And Operation Parameters Request/Response Support field in the RSNXE to 1. The EDP Capabilities And Operation Parameters Response frame shall include a Basic Multi-Link element, and the Basic Multi-Link element shall include a Per-STA Profile subelement with the Complete Profile subfield set to 1 for each AP affiliated with the AP MLD (see 9.4.2.321.2.4 (Link Info field of the Basic Multi-Link element)). The STA profile field in the Per-STA Profile subelement for each AP affiliated with the AP MLD includes the following in order and does not follow 35.3.3.3 (Advertisement of complete or partial per-link information):

* The Capability Information field as defined in 9.4.1.4 (Capability Information field).
* All elements that would(#673) be included in a Probe Response frame except the(#672) Multi-Link element and the(#672) Multiple BSSID element, and the elements(#674) shall be in the order defined for a Probe Response frame.

**TGbi Editor: *Instruction modify 12.16.6.1 and 12.16.6.2 as follows***

**12.16.6.1 Non-MLO**

If the FILS authentication protocol(#677) and the FT protocol are not used, the EDP AP shall include a Key Delivery element in the (Re)Association Response frame.

**12.16.6.2 MLO**

(…existing texts…)

After a pairwise cipher is indicated by the EDP non-AP MLD and a TK is derived during Authentication

frame exchange between the EDP non-AP MLD and an EDP AP MLD, (#682)the EDP non-AP MLD shall

encrypt the (Re)Association Request frame transmitted to the EDP AP MLD using the TK and the pairwise

cipher indicated in the Authentication frame exchange.

(…existing texts…)

If the FILS authentication protocol(#677) and the FT protocol are not used, the EDP AP MLD shall include a Key Delivery element in the (Re)Association Response frame.

(…existing texts…)

**TGbi Editor: *Instruction modify 12.5.2.4.4 as follows***

* CCMP decapsulation
* PN and replay detection

***Change item c) and d) of the third paragraph (not all shown) and create new items as follows:***

See 12.5.2.2 (CCMP MPDU format) for a description of how the PN is encoded in the CCMP header. The following processing rules are used to detect replay:

* If management frame protection is negotiated, the receiver shall maintain a single replay counter for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 0, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details)), ~~and~~ Protected Sensing frames (see 9.6.36 (Protected Sensing frame details)), and EDP robust (#647)Beamforming/CSI/CQI frames (see 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame)), and (S1G STA only) a single replay counter for received individually addressed robust PV1 Management frames.
* If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the receiver shall maintain an additional replay counter for each ACI for received individually addressed robust PV0 Management frames that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), ~~and~~ Protected Sensing frames (see 9.6.39 (Protected Sensing frame details)), and EDP robust Beamforming/CSI/CQI frames (see 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame)).
* If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing frame details(11az))) and shall use the PN from the received frame to detect replays.
* If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Sensing frames (see 9.6.39 (Protected Sensing frame details)) and shall use the PN from the received frame to detect replays.

***Insert the following paragraph after item f):***

* For non-MLO, if dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving EDP robust individually addressed Beamforming/CSI/CQI frames (see 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame)) and shall use the PN from the received frame to detect replays.
* For MLO, if dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter in each setup link for receiving EDP robust individually addressed Beamforming/CSI/CQI frames (see 12.16.3 (EDP Robust Individually Addressed Management Frame and Robust Individually Addressed Beamforming/CSI/CQI Frame)) and shall use the PN from the received frame to detect replays.

**TGbi Editor: *Instruction modify 12.6.8.1 as follows***

**12.6.8.1 General**

— 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 802.1X Authentication uitilizing Authentication frames(#651) in

its RSNXE, a STA may signal its Supplicant to use IEEE Std 802.1X-2020 to authenticate with that

AP (see 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames)).

**TGbi Editor: *Instruction modify 12.6.8.3 as follows***

* Cached PMKSAs and RSNA key management

***Change the fourth paragraph as follows:***

If a cached PMKSA is used in FT Initial Mobility Domain Association, the cached MPMK is used to derive the PMK-R0 of a new FT key hierarchy (see 12.7.1.6 (FT key hierarchy)). The PMKID indicated by the STA in the ~~(Re)Association Request frame and message 1 of the FT 4-way handshake (when FILS authentication is not used) or~~ FILS Authentication frame (when FILS authentication is used), IEEE 802.1X Authentication frame (when PTKSA derivation with IEEE 802.1X Authentication frame exchange is used), EDPKE Authentication frame (when EDPKE authentication is used),(#652) or (Re)Association Request frame and the first message(#691) of the FT 4-way handshake (otherwise) is the PMKID of the cached PMKSA as defined in 12.7.1.6.3 (PMK-R0) (i.e., not the PMKR0Name or PMKR1Name of the FT key hierarchy that was derived when the PMKSA was originally established). The PMKR1Name indicated in the RSNE in messages 2 and 3 of the FT 4 way handshake (when FILS authentication is not used) or in (Re)Association Request and Response frames (when FILS authentication is used) is the PMKR1Name of the newly derived FT key hierarchy (see 13.4 (FT initial mobility domain association)).

***Change the eighth paragraph as follows:***

If both sides assert possession of a cached PMKSA, but the 4-way handshake, FILS authentication, encrypted (re)association exchange with 802.1X Authentication frame exchange, or(#652) EDPKE authentication fails, both sides may delete the cached PMKSA for the selected PMKID.

**TGbi Editor: *Instruction modify 12.16.7.1 as follows***

* PMKID privacy

After the indicated PMKID in an RSNE identifies a cached PMKSA (see 12.6.8.3 (Cached PMKSAs and RSNA key management)), and a PTKSA is established using the identified PMKSA,

* For non-MLO, if the EDP non-AP STA and the EDP AP set the PMKSA Caching Privacy Support field in the RSNXE to 1, the EDP AP shall deliver the PMKID for the identified PMKSA to be used next time to the non-AP STA in the PMKID KDE included in the Key Delivery element of the encrypted (Re)Association Response frame.
* For MLO, if the EDP non-AP STA(s) affiliated with an EDP non-AP MLD and the EDP AP(s) affiliated with an EDP AP MLD set the PMKSA Caching Privacy Support field in the RSNXE to 1, the EDP AP MLD shall deliver the PMKID for the identified PMKSA to be used next time (#175)to the non-AP MLD in the PMKID KDE included in the Key Delivery element of the encrypted (Re)Association Response frame.

NOTE 1—For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

NOTE 2—For a different PMKID to ensure privacy, the SPA needs to be randomized in the frame indicating the PMKID to identify the cached PMKSA. As a result, tracking cannot be done on the MAC address.

**TGbi Editor: *Instruction modify 12.16.7.2 as follows***

**12.16.7.2 PMKR0Name privacy**

The PMKR0Name shall be recomputed as follows:

PMKR0Name = Truncate-128(HMAC-Hash( XXKey, "FT-R0N" || ANonce || SNonce))

where(#686):

**TGbi Editor: *Instruction modify 12.16.8 as follows***

* Key derivation with Authentication frame exchange

This subclause defines rules to derive a temporal key (TK) through Authentication frame exchange to encrypt the Frame Body field of the (Re)Association Request/Response frame.

* FT

If an FTO or FTR (see 13 (Fast BSS transition)) sets the (Re)Association Frame Encryption Support field in the RSNXE to 1, then the FTO or FTR supports the additional rules defined in this subclause.

An FTO that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 and receives an(#688) RSNXE from the FTR with the (Re)Association Frame Encryption Support field set to 1 shall:

* Include a Diffie-Hellman Parameter element in the first message of the FT protocol (see 13.8 (FT authentication sequence)).
* Select a finite cyclic group in the Diffie-Hellman Parameter element from the dot11RSNAConfigDLCGroupTable that is at least of the security strength provided by the AKM and cipher suites.
* Generate an ephemeral (random) private key with the chosen finite cyclic group,(#276) use the selected group's scalar operation (see 12.4.4.1 (General)) with the private key to generate its ephemeral public key, and indicate the ephemeral public key in the Diffie-Hellman Parameter element.

Otherwise, an FTO shall not include a Diffie-Hellman Parameter element in the first message of the FT protocol.

For the purpose of interoperability, an FTO or an FTR shall support group 19, an ECC group defined over a 256-bit prime order field.

An FTR that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 and receives the first message of the FT protocol with the (Re)Association Frame Encryption Support field in the RSNXE set to 1 shall:

* Validate that finite cyclic group indicated in the Diffie-Hellman Parameter element in the first message (#691)is supported (present in dot11RSNAConfigDLCGroupTable). Otherwise, the FTR shall reject the first message(#691) with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP.
* Verify the public key indicated in the Diffie-Hellman Parameter element in the first message(#691) as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the FTR shall reject the first message(#691) with status code set to INVALID\_PUBLIC\_KEY.
* Generate an ephemeral (random) private key with the chosen finite cyclic group and use the selected group's scalar operation with the private key to generate its ephemeral public key if the first message(#691) is not rejected. Perform the group's scalar-op (see 12.4.4.1 (General)) with the FTO's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.(#276)
* Derive PTK with DHss as defined in 12.7.1.6.5 (PTK).
* , Irretrievably delete the shared secret, DHss, upon completion of PTK generation. (#276)
* Include a Diffie-Hellman Parameter element in the second message of the FT protocol (see 13.8 (FT authentication sequence)).
* Indicate the(#694) chosen finite cyclic group in the Diffie-Hellman Parameter element of the second message(#691), which is the same as the finite cyclic group in the Diffie-Hellman Parameter element of the first message(#691).
* Indicate its ephemeral public key in the Diffie-Hellman Parameter element of the second message(#691).
* Calculate the(#694) MIC in the FTE by (#695)

using the key, the algorithm, and the MIC size as defined in 13.8.5 (FT authentication sequence: contents of fourth message) (#695)

On the concatenation of the following data, in the order given here as the input: (#695)

* FTO's MAC address.
* FTR's MAC address.
* RSNE sent in the Beacons transmitted by the AP with MAC address equal to A1 field of the first message(#691).
* RSNXE sent in the Beacons transmitted by the AP with MAC address equal to A1 field of the first message(#691).
* the body of the second message with MIC field of the FTE set to 0.
* Include the(#694) MIC in the FTE rather than set it to 0 as described in 13.8.3 (FT authentication sequence: contents of second message).

Otherwise, an FTR shall not include a Diffie-Hellman Parameter element in the second message of the FT protocol.

After receiving the second message of the FT protocol with the status code set to SUCCESS, an FTO shall:

* Validate that there is a Diffie-Hellman Parameter element included in the second message of the FT protocol if the FTO includes a Diffie-Hellman Parameter element in the first message of the FT protocol,. If the validation fails, the FTO shall discard the frame and terminate further protocol processing. (#276)
* Validate that there is no Diffie-Hellman Parameter element included in the second message of the FT protocol if the FTO does not include a Diffie-Hellman Parameter element in the first message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing. (#276)
* Validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in the second message(#691) is the same as the finite cyclic group indicated in the Diffie-Hellman Parameter element in the first message(#691) if the FTO includes a Diffie-Hellman Parameter element in the first message of the FT protocol. If the validation fails, the FTO shall discard the frame and terminate further protocol processing. (#276)
* Verify the public key indicated in the Diffie-Hellman Parameter element in the second message(#691) as specified in 5.6.2.3 of NIST SP 800-56A R2. If the(#278) verification fails, the FTO shall discard the frame and terminate further protocol processing.
* Perform the group's scalar-op (see 12.4.4.1 (General)) with the FTR's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss, if the second message(#691) is not discarded. (#276)
* Derive PTK with DHss as defined in 12.7.1.6.5 (PTK).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.
* Verify the MIC in the FTE using the S1KH of the FTO(#277). If the verification fails, the FTO shall discard the frame and terminate further protocol processing.(#278)
* IEEE 802.1X

If an originator or a responder defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames) sets the (Re)Association Frame Encryption Support field in the RSNXE to 1, then the originator or the responder supports the additional rules defined in this subclause when performing IEEE 802.1X Authentication frame exchange.

An originator that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1, has the SME to act as the Supplicant, receives an(#688) RSNXE from the responder with the (Re)Association Frame Encryption Support field set to 1, and intends to continue association after authentication shall do the following in the first Authentication frame: (#279)

* Include a Nonce element to indicate SNonce. (#279)
* Include an RSNE (#279)to indicate the AKM and the pairwise cipher suite. The Version field shall be set to 1. The Pairwise Cipher Suite Count field shall be set to 1. The AKM Suite Count field shall be set to 1. The PMKID count field and the PMKID List field is (#702)set corresponding to PMKSA identifiers if exists. All other fields shall be as specified in 9.4.2.23 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).
* Not include an AKM Suite Selector element.
* Include an RSNXE. (#279)
* Include a Diffie-Hellman Parameter element. (#279)
* Select a finite cyclic group in the Diffie-Hellman Parameter element from the dot11RSNAConfigDLCGroupTable that is at least of the security strength provided by the AKM and cipher suites.
* With the chosen finite cyclic group, generate an ephemeral (random) private key, use the selected group's scalar operation (see 12.4.4.1 (General)) with the private key to generate its ephemeral public key, and indicate the ephemeral public key in the Diffie-Hellman Parameter element.

Otherwise, an originator shall not include a Diffie-Hellman Parameter element nor(#162) an RSNE nor(#162) an RSNXE nor(#162) a Nonce element in the first Authentication frame for IEEE 802.1X authentication.

For the purpose of interoperability, an authenticator or a supplicant shall support group 19, an ECC group defined over a 256-bit prime order field.

A responder that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1, has the SME to act as the Authenticator, and receives the first Authentication frame with a Nonce element, RSNE, RSNXE, and a Diffie-Hellman Parameter element shall:

* Verify that the AKM indicated in the RSNE rather than AKM Suite Selector(#712) element as defined in 12.4.4 (IEEE 802.1X authentication utilizing Authentication frames) is supported. Otherwise, the responder shall reject the first message(#691) with status code set to STATUS\_INVALID\_AKMP.
* Verify that the pairwise cipher indicated in the RSNE is supported. Otherwise, the responder shall reject the first message(#691) with status code set to STATUS\_INVALID\_PAIRWISE\_CIPHER.
* Validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in the first Authentication frame is supported (present in dot11RSNAConfigDLCGroupTable). Otherwise, the responder shall reject the first message(#691) with status code set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP.
* Verify the public key indicated in the Diffie-Hellman Parameter element in the first message(#691) as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the responder shall reject the first Authentication frame with status code set to INVALID\_PUBLIC\_KEY.
* Verify that a PMKSA named via a PMKID in the RSNE exists for the specified AKM if one or more PMKIDs are included(#705).
* If a PMKSA is identified, use PMKSA caching, does not process the EAPOL PDU in the first Authentication frame, and does not include EAPOL PDU in the second authentication frame.
* If no PMKSA is identified, continue the IEEE 802.1X authentication.

If the first Authentication frame is not rejected, the responder shall: (#282)

* Store the indicated SNonce and generate an ephemeral (random) private key with the chosen finite cyclic group and use the selected group's scalar operation with the private key to generate its ephemeral public key.
* Perform the group's scalar-op (see 12.4.4.1 (General)) with the originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* Use PMKSA caching if a PMKSA is identified and before sending the second Authentication frame:
* Derive the(#710) PTK with the identified PMKSA and DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation. (#282)

The responder shall do the following in the second Authentication frame: (#282)

* Include an RSNE to indicate the AKM and pairwise cipher indicated in the first Authentication frame.
* If a PMKSA is identified, include the PMKID corresponding to the PMKSA in the RSNE.
* Otherwise, does not include any PMKID in the RSNE.
* Not include an AKM Suite Selector element. (#282)
* Include a Diffie-Hellman Parameter element. (#282)
* Indicate the(#694) chosen finite cyclic group in the Diffie-Hellman Parameter element, which is the same as the finite cyclic group in the Diffie-Hellman Parameter element of the first Authentication frame. (#282)
* Indicate its ephemeral public key in the Diffie-Hellman Parameter element. (#282)
* Include a Nonce element to indicate ANonce. (#282)

 (#282)Otherwise, a responder shall not include a Diffie-Hellman Parameter element nor(#162) a Nonce element nor(#162) an RSNE in the second Authentication frame for IEEE 802.1X authentication.

After receiving the second Authentication frame with the status code set to SUCCESS, an originator shall:

* If the originator includes a Diffie-Hellman Parameter element in the first Authentication frame, validate that there is a Diffie-Hellman Parameter element and an RSNE included in the second Authentication frame and there is no AKM Suite Selector(#712) element in the second Authentication frame. If the validation fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator does not include a Diffie-Hellman Parameter element in the first Authentication frame, validate that there is no Diffie-Hellman Parameter element and no RSNE included in the second Authentication frame. If the validation fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator includes a Diffie-Hellman Parameter element in the first Authentication frame, validate that the finite cyclic group indicated in the Diffie-Hellman Parameter element in the second Authentication frame is the same as the finite cyclic group indicated in the Diffie-Hellman Parameter element in the first Authentication frame, validate that the pairwise cipher suite and the AKM indicated in the second Authentication frame are the same as the pairwise cipher suite and the AKM indicated in the first Authentication frame. (#713)
* Verify the public key indicated in the Diffie-Hellman Parameter element in the second Authentication frame as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator includes one or more PMKIDs(#714) in the first Authentication frame, and the second Authentication frame includes a PMKID, validate that the Encapsulation(#852) Length field is set to 0 and validate that the PMKID included in the second Authentication frame matches one of the PMKID(s) indicated in the first Authentication frame. If verification succeeds, the originator uses(#715) PMKSA caching with the PMKSA identified by the PMKID indicated in the second Authentication frame and does not continue the IEEE 802.1X Authentication frame exchange. If verification fails, the originator shall discard the frame and terminate further protocol processing.
* If the originator does not include any PMKID in the first Authentication frame, validate that there is no PMKID included in the second Authentication frame. If verification fails, the originator shall discard the frame and terminate further protocol processing.
* If the second Authentication frame is not discarded, store the indicated ANonce, perform the group's scalar-op (see 12.4.4.1 (General)) with the originator's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
* If a PMKSA is identified, an originator shall:
* Derive the(#710) PTK with the identified PMKSA and DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.

If a PMKSA is not identified through(#716) PMKSA caching, before sending the Authentication frame carrying EAP Success, a responder shall:

* Derive the(#710) PTK with DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.

If a PMKSA is not identified through(#716) PMKSA caching, after receiving the Authentication frame carrying EAP Success, an originator shall:

* Derive the(#710) PTK with DHss as defined in 12.7.1.3 (Pairwise key hierarchy).
* Irretrievably delete the shared secret, DHss, upon completion of PTK generation.

The originator and the responder then continue the operation as defined in 12.16.6 ((Re)Association Request/Response Frame Encryption) with the following additional rules:

* The responder shall verify that the RSNE other than the PMKID Count field and the PMKID List(#718) field in the (Re)Association Request frame is identical to the RSNE included in the first Authentication frame. The responder(#719) shall also verify that the RSNXE in the (Re)Association Request is identical to the RSNXE included in the first Authentication frame. If the validation fails, the responder shall reject the association.
* The originator shall verify that the RSNE other than the PMKID Count field and the PMKID List(#718) fieldin the (Re)Association Response frame is the same as the RSNE included in the second Authentication frame. If the validation fails, the originator shall disassociate.

**TGbi Editor: *Instruction modify C.3 as follows***

C.3 MIB detail

Dot11EDPStationConfigEntry ::= SEQUENCE

 {

 dot11EPDPKEActivated TruthValue,

 dot11EDPGroupEpochActivated TruthValue,

 dot11EDPEpochStartTimeMargin Unsigned32,

 dot11EDPEpochTransitionTime Unsigned32,

 dot11EDPGroupEpochCurrentGroup Unsigned32,

 dot11EDPRobustIndividuallyAddressedManagementFrameActivated

 TruthValue,

 dot11EDPCapabilitiesAndOperationParametersRequestResponseActivated

 TruthValue,

 dot11EDPReAssociationFrameEncryptionSupportActivated TruthValue,

 dot11EDPIEEE8021XAuthenticationUtilizingAuthenticationFrameActivated

 TruthValue,

* Dot11EDPPMKSACachingPrivacySupportActivated TruthValue,(#768)

 dot11DSMACAddressActivated TruthValue,

 dot11PrivacyBeaconResponseTime Unsigned32

 }

(…existing texts…)

dot11EDPRobustIndividuallyAddressedManagementFrameActivated OBJECT-TYPE

 SYNTAX TruthValue

 MAX-ACCESS read-write

 STATUS current

 DESCRIPTION

 "This is a control variable. It is written by an external management entity or the SME. Changes take effect as soon as practical in the implementation. This attribute, when true, indicates the capability to support EDP robust individually addressed Management frames(#743) is enabled. The capability is disabled otherwise."

 DEFVAL { false }

 ::= { dot11EDPStationConfigEntry 6 }