IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 12.16.6 comments |
| Date: 2025-03-28 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission resolves the following CIDs:

167, 165, 966, 166, 139, 140, 678, 680, 681, 849,

850, 945, 4, 266, 978, 683, 684, 685, 915, 176

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision for the resolution
* Rev 2: Add CID 915 after discussing with the commenter.
* Rev 3: Improve resolution for various CIDs.
* Rev 4: revision for CID 176

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** |
| 167 | 123.61 | 12.16.6 | Clairfy Encryption of (re)association request/response reuses PMF. Have MFPC set to 1. | As in comment | Revised – Agree in principle with the commenter.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 167 |
| 165 | 123.61 | 12.16.6 | Encryption of (re)association request/response reuses PMF. We should have a sentence in 12.2.7 to say "The robust Management frames also include (Re)Association Request and Response frames when capability is negotiated" | As in comment | Revised – Agree in principle with the commenter.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 167 |
| 966 | 123.14 | 12.16.6.1 | P802.11bi/D1.0 does not seem to define clearly enough how (Re)Association Request/Response frames are encrypted. It is not sufficient to point to the TK and the indicated pairwise cipher. There needs to be addition description on how the cipher (i.e., CCMP and GCMP) can actually be used with these frames. This needs to also take into account potential CCM/GCM nonce reuse issues (i.e., same PN counter have to be used) and replay protection. The simplest way to address this would seem to be to define (Re)Association Request/Response frames to be robust Management frame. | In 12.2.7 (Requirements for management frame protection), replace"The robust Management frames are Disassociation, Deauthentication, robust Action(#8136), and robust ActionNo Ack frames."with"The robust Management frames are Disassociation, Deauthentication, robust Action(#8136), robust ActionNo Ack frames, and if (Re)Associatiion Request/Response Frame Encryption (see 12.16.6) is used, Association Request frame, Association Response frame, Reassociation Request frame, and Reassociation Response frame." | Revised – Agree in principle with the commenter.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 167 |
| 166 | 123.61 | 12.16.6 | Encryption of (re)association request/response reuses PMF. We should have a sentence in 12.6.17 to say unprotected (re)assoc req/resp frames shall be discarded when capability is negotiated | As in comment | Revised – Agree in principle with the commenter.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 167 |
| 139 | 124.32 | 12.16.6.1 | How does the EDP AP know decryption fails? There is no description of the critiria of decryption failure in the draft and baseline. Is it integrity checking failure? For AES, you always get output when you have input and key, no failure. Similar issue for MLO in P126. | Describe what is decryption failure. | Revised - Decryption failure for GCM is defined in the baseline. *“GCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as**decrypting the frame body. A MIC check is performed by comparing the received MIC with a MIC calculated**as described in 12.5.4.3 (GCMP cryptographic encapsulation). The plaintext is returned only if the MIC check is successful.**The GCM decryption algorithm yields a plaintext P or an indication of inauthenticity FAIL; from this the plaintext frame body is taken as P, if there was no indication of inauthenticity.”*Error free CCM decryption is defined in the baseline*“CCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as**decrypting the frame body. A MIC check is performed by comparing the received MIC with a MIC calculated**as described in 12.5.2.3 (CCMP cryptographic encapsulation). The plaintext is returned only if the MIC check is successful.**The CCM decryption algorithm is described in IETF RFC 3610. The key, nonce, AAD and encrypted data**described above are passed to the CCM decryption algorithm as K, N, a and c respectively. The CCM decryption algorithm yields a decrypted message m and a value T; from this the plaintext frame body described**below is taken as m, if the MIC described above matches T.**There is one output from error-free CCM recipient processing:”*We revise the sentence and add the reference.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 139 |
| 140 | 124.51 | 12.16.6.1 | How does the EDP AP know that the EDP non-AP STA fails to decrypt the (Re)Association Response frame, and how does the EDP AP reject the association after it has sent out the (Re)Association Response frame? Similar issue for MLO in P126. | Remove "If the decryption fails, then the EDP AP shall reject the association." | Revised - Decryption failure for GCM is defined in the baseline. *“GCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as**decrypting the frame body. A MIC check is performed by comparing the received MIC with a MIC calculated**as described in 12.5.4.3 (GCMP cryptographic encapsulation). The plaintext is returned only if the MIC check is successful.**The GCM decryption algorithm yields a plaintext P or an indication of inauthenticity FAIL; from this the plaintext frame body is taken as P, if there was no indication of inauthenticity.”*Error free CCM decryption is defined in the baseline*“CCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as**decrypting the frame body. A MIC check is performed by comparing the received MIC with a MIC calculated**as described in 12.5.2.3 (CCMP cryptographic encapsulation). The plaintext is returned only if the MIC check is successful.**The CCM decryption algorithm is described in IETF RFC 3610. The key, nonce, AAD and encrypted data**described above are passed to the CCM decryption algorithm as K, N, a and c respectively. The CCM decryption algorithm yields a decrypted message m and a value T; from this the plaintext frame body described**below is taken as m, if the MIC described above matches T.**There is one output from error-free CCM recipient processing:”*We revise the sentence and add the reference.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 139 |
| 678 | 124.51 | 12.6.6.1 | "the EDP AP shall reject the association" -- no, here it's the non-AP STA | Change "AP" to "non-AP STA" | Revised – Agree in principle with the commenter.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 678 |
| 680 | 124.58 | 12.6.6.1 | "If FT protocol is not used and the (Re)Association Response frame includes the RSNXE, the EDP non-AP STA shall verify that this element is identical to the RSNXE included in the Beacon and Probe Response frames received from the EDP AP. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP STA shall discard the response." -- what if beacon did include but assocrsp didn't. Also at 126.40 | Change to "If the FT protocol is not used and the (Re)Association Response frame or the Beacon and Probe Response frames received from the EDP AP include the RSNXE, the EDP non-AP STA shall verify that this element is identical in all of these frames. If not all of these frames included the RSNXE or if the RSNXEs are not identical, the EDP non-AP STA shall discard the response." | Revised – Agree in principle with the commenter. We change it to “Beacon or Probe Response frames” to align with the baseline language.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 680 |
| 681 | 125.17 | 12.6.6.1 | "establish EDP non-AP STA to EDP AP mapping to the DS rather than the MAC address of the EDP non-AP STA" not clear and maybe articles missing | As it says in the comment | Revised –Agree in principle with the commenter. We add the article.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 681 |
| 849 | 124.03 | 12.16.6.1 | The text states that a non-AP STA may create a cipher/key relationship with the AP. What is missing is the fact that in order to employ (Re)Association Frame Encryption Support, a non-AP STA must do so. In addition, this text should make reference to clause 12.16.8 that descrbes the key generation process. | Revise text as "In order to employ (Re)association frame encryption, an EDP non-AP STA that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall indicate a pairwise cipher, establish a PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1, following the procedure described in 12.16.8 (Key derivation with Authentication frame exchange)." | Revised – Agree in principle with the commenter. We note that 12.16.8 cover some of the procedures but we also have EDPKE procedures. We change the description to “shall”TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 849 |
| 850 | 125.31 | 12.6.6.2 | The text states that a non-AP STA may create a cipher/key relationship with the AP. What is missing is the fact that in order to employ (Re)Association Frame Encryption Support, a non-AP STA must do so. In addition, this text should make reference to clause 12.16.8 that descrbes the key generation process. | Revise text to: "In order to employ (Re)association frame encryption, an EDP non-AP MLD that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall indicate a pairwise cipher, establish a PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP MLD if APs affiliated with the EDP AP MLD set the (Re)Association Frame Encryption Support field in the RSNXE to 1, following the procedure described in 12.16.8 (Key derivation with Authentication frame exchange)." | Revised – Agree in principle with the commenter. We note that 12.16.8 cover some of the procedures but we also have EDPKE procedures. We change the description to “shall”TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 850 |
| 945 | 124.01 | 12.6.6.1 | Non-MLO is a terrible clause title | Modify the title of the clause title, maybe something like "EDP STA requirements". Note that this clause title is used for multiple sub-clauses of the draft. | Revised – Agree in principle with the commenter. We add procedure to the title.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 945 |
| 4 | 127.08 | 12.16.6.2 | add some texts to say "the supplicant MAC address is the DS MAC address if present", also, the "DS MAC address is passed to construct the AAD (see 12.5.4.3.3 (Construct AAD)) and nonce (see 12.5.4.3.4 (Construct GCM nonce)) values". | as the comments | Rejected –The proposal does not change the AAD construction procedure and supplicant address.  |
| 266 | 126.25 | 12.16.6.2 | A non-AP MLD should be identified by PMKID (or PMKR0Name in FT) only. This allows a non-AP MLD to change its all addresses (link and MLD) freely. The MLD address may remain the same in roaming and FT to keep the same IP addresses. Thus the MLD address has the same operation as the DS address and the DS address is not needed. | Do not allow non-AP MLDs to have a DS address. Allow a non-AP MLD to be identified only by PMKID or PMKR0Name, so that MLD address of the non-AP MLD may change. | Rejected –MLD address in on the clear in authentication frame. Hence, MLD address can not be the same.  |
| 978 | 126.25 | 12.16.6.2 | A non-AP MLD should be identified solely by the PMKID.Thus, a non-AP MLD can change its addresses whenever it wants without any performance loss. | As in comment. | Rejected –PMKID can not be use for the mapping in the DS. MLD MAC address and the link address can be changed during the initial connection or roaming.  |
| 683 | 125.55 | 12.6.6.2 | "to establish a PTKSA" -- not any old PTKSA, the specific PTKSA for this link. Also at line 58 | Change to "to establish the PTKSA" | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 683 |
| 684 | 126.12 | 12.6.6.2 | "the transmitted (Re)Association Response frame transmitted to the EDP non-AP MLD in response to the (Re)Association Request frame" -- too many transmitteds, and obviously the response is in response to the request | Change to "the (Re)Association Response frame" | Accepted - |
| 685 | 126.24 | 12.6.6.2 | "if EDP epoch is supported" -- not clear. Also 97.50, 126.54, 135.27 | Delete "epoch " | Revised -PGTK is specifically for EDP epoch. We refer to the RSNXE bit setting. TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 685 |
| 915 | 60.24 | 9.4.2.240 | Currently key delivery in (re)Assoc Respons is doubly encrypted, by KEK and by the regular mgmt frame encryption | Fix the issues. Will follow up with a contribution. | Revised –Agree in principle with the commenter. After discussing with the commenter, the proposed resolution is not to do KEK encryption and additional MIC calculation.TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 915 |
| 176 | 123.61 | 12.16.6 | Need to handle FT initial domain connection with relevant rules for MDE, FTE and RSNE/RSNXE verification. | The commenter will submit a contribution to resolve the issue. | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in the latest version of 11-25/0554 under all headings that include CID 176 |

***Discussion:***

***Proposal:***

***TGbi Editor: Modify 12.16.9.1 as shown below***

***12.16.9 Enhanced Data Privacy Key Exchange***

***12.16.9.1 General***

If dot11EDPKEActivated is true, then dot11EDPReAssociationFrameEncryptionSupportActivated and dot11KEKPASNActivated are set to true.

Enhanced Data Privacy Key Exchange (EDPKE) is an RSNA authentication protocol that uses the PASN procedures (see 12.12 (Preassociation security negotiation)) with the following differences:

* SAE AKMP 00-0F-AC:8, 00-0F-AC:9, 00-0F-AC:24, or 00-0F-AC:25 can be used as the Base AKMP.(#176)
* When there is no Base AKMP, EDKPE is not used.
* The three Authentication frames have the Authentication Algorithm Number field set to 9 (EDPKE Authentication).
* The generated PTK is used as the initial PTK once associated.

***TGbi Editor: Modify 12.16.9.3.3 as shown below***

**12.16.9.3.3 EDPKE authentication with SAE**

The same procedures as specified in 12.13.5 (PASN authentication with SAE) are used.

If the Base AKMP is 00-0F-AC:9 or 00-0F-AC:25, the rules defined in 12.16.8.1a FT initial mobility domain association is followed.(#176)

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

**9.3.3.11 Authentication frame format**

***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) |
| .... |  |  |  |
| IEEE 802.1X authentication | 1 | Reserved  | The Encapsulation Length field is present.The Encapsulation field is present only when the Encapsulation Length field is nonzero.The AKM Suite Selector element is optionally present as defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames).The RSNE is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The RSNXE is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Nonce element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Diffie-Hellman Parameter element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).MDE is optionally present as defined in 12.16.8.1a (FT initial mobility domain association).(#176) |
| IEEE 802.1X authentication | 2 | SUCCESS | The Encapsulation Length field is present.The Encapsulation field is present only when the Encapsulation Length field is nonzero.The AKM Suite Selector element is optionally present as defined in 12.16.5 (IEEE 802.1X authentication utilizing Authentication frames).The RSNE is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Nonce element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).The Diffie-Hellman Parameter element is optionally present as defined in 12.16.8.2 (IEEE 802.1X).MDE is optionally present as defined in 12.16.8.1a (FT initial mobility domain association). (#176)FTE is optionally present as defined in 12.16.8.1a (FT initial mobility domain association). (#176) |
| .... |  |  |  |
| 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.MDE is present if the Base AKMP is 00-0F-AC:9 or 00-0F-AC:25.(#176)PASN Parameters element is present.Timeout Interval element may be present.Wrapped Data element is present if the wrapped data format in 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.MDE and FTE are present if the Base AKMP is 00-0F-AC:9 or 00-0F-AC:25.(#176)Timeout Interval element may be present.Wrapped data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved and Status Code field is 0.MIC element is present. |
| 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 PASN Parameters element is nonzero and not reserved; and Status Code field is 0.MIC element is present. |

***TGbi Editor: Modify Table 9-64—Association Request frame body as shown below***

* Association Request frame body

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| … |  |  |
| 12 | Mobility domain | An MDE is present in an Association Request frame ifdot11FastBSSTransitionActivated is true, encryption of the Association Request frame is used, and if the frame is beingsent to an AP that advertised its FT capability in the MDE in itsBeacon or Probe Response frame (i.e., AP also hasdot11FastBSSTransitionActivated equal to true). (#176) |
| 13 | Fast BSS Transition | An FTE is present in an Association Request frame ifdot11FastBSSTransitionActivated is true, encryption of the Association Request frame is used, anddot11RSNAAuthenticationSuiteSelected is equal to an AKM suiteselector value for which the Authentication type column indicatesFT authentication. See Table 9-190 (AKM suite selectors) (i.e.,part of a fast BSS transition in an RSN). (#176) |

***TGbi Editor: modify the title of 12.16.8.1***

**12.16.8 Key derivation with Authentication frame exchange**

(…existing texts….)

**12.16.8.1 FT protocol**(#176)

(…existing texts….)

***TGbi Editor: add another subclause 12.16.8.1a*** (#176)

**12.16.8.1a FT initial mobility domain association**

If an FTO and an FTR (see 13 (Fast BSS transition)) set the (Re)Association Frame Encryption Support field in the RSNXE to 1, then the FTO and the FTR support the additional rules defined in this subclause to initiate FT initial mobility domain association.

For the FTO, the first Authentication frame carries an MDE. The contents of the MDE shall be the values advertised by the AP that receives the first Authentication frame in its Beacon or Probe Response frames.

For the FTR, if the contents of the MDE received in the first Authentication frame do not match the contents advertised in the Beacon or Probe Response frames, the processing status is set to STATUS\_INVALID\_MDE. If an MDE is present in the first Authentication frame and the base AKMP does not indicate the single FT AKMP, the processing status is set to STATUS\_INVALID\_AKMP.

For the FTR, the second Authentication frame carries an MDE and an FTE. The MDE has contents as presented in Beacon and Probe Response frames. The FTE shall include the key holder identities, the R0KH-ID and R1KH-ID, set to the values of dot11FTR0KeyHolderID and dot11FTR1KeyHolderID, respectively. The FTE shall have a MIC element count of zero (i.e., no MIC present) and have ANonce, SNonce, and MIC fields set to 0. When the

negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.

Upon successful completion Authentication frame processing to establish PMKSA, the R0KH establishes key hierarchy. If a key hierarchy already exists for the FTO belonging to the same mobility domain (i.e., having the same MDID), the R0KH shall delete the existing PMK-R0 security association and PMK-R1 security associations. It then calculates the PMK-R0, PMKR0Name, and PMK-R1 and makes the PMK-R1 available to the R1KH.

**TGbi Editor: *Instruction: Modify 12.2.7 as follows***

12.2.7 Requirements for management frame protection

The robust Management frames are Disassociation, Deauthentication, robust Action, robust Action No Ack frames, and if encryption of (Re)Association Request/Response frames is used (see 12.16.6), Association Request frame, Association Response frame, Reassociation Request frame, and Reassociation Response frame.(#167)

Action and Action No Ack frames specified with No in the Robust column of Table 9-81 (Category values) are not robust Management frames and shall not be protected.

When management frame protection is negotiated, individually addressed robust Management frames shall be encapsulated using the pairwise cipher suite (see 12.6.17 (Protection of robust Management frames.)) and group addressed robust Management frames shall be encapsulated using the procedures defined in 11.12 (Group addressed management frame protection procedures).

**TGbi Editor: *Instruction: Modify 12.6.17 as follows***

**12.6.17 Protection of robust Management frames**

(…existing texts…)

If management frame protection is negotiated for the link, a STA shall not transmit any of the following, and shall discard all of the following:

— An unprotected individually addressed Deauthentication or Disassociation frame.

(#2128)NOTE 5—The STA might invoke the SA Query procedures (see 11.13 (SA Query procedures)) if received with a reason code of INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME.

— An unprotected individually addressed robust Action or robust Action No Ack frame(#7078)

(#2128)NOTE 6—The STA is not(M118) sent any protected individually addressed robust Management frames before the PTKSA has been established.

— An unprotected group addressed robust Management frame.

If management frame protection is negotiated for the link and encryption of (Re)Association Request/Response frames is used, a STA shall not transmit any of the following, and shall discard all of the following:

- An unprotected individually addressed Association Request frame or Association Response frame or Reassociation Request frame or Reassociation Response frame.(#167)

(…existing texts…)

**TGbi Editor: *Instruction: Modify 12.16.6 as follows***

* (Re)Association Request/Response Frame Encryption

This subclause defines rules to encrypt the Frame Body field of the (Re)Association Request/Response frame and to include a DS MAC Address element in the encrypted (Re)Association Request frame.

An EDP STA that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall set the MFPC subfield in the RSN Capabilities field in the RSNE to 1.(#167)

* Non-MLO procedure(#945)

An EDP non-AP STA that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall indicate a pairwise cipher, establish a PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 (see 12.16.8 (Key derivation with Authentication frame exchange) and 12.16.9 (Enhanced Data Privacy Key Exchange)). (#849)

An EDP non-AP STA shall randomize its STA MAC address during a BSS transition if the BSS transition procedure uses an encrypted (Re)Association Request frame to carry the DS MAC Address element.

After a pairwise cipher is indicated by the EDP non-AP STA and a temporal key (TK) is derived during Authentication frame exchange between the EDP non-AP STA and an EDP AP, the EDP non-AP STA shall encrypt the (Re)Association Request frame transmitted to the EDP AP using the TK and the pairwise cipher indicated in the Authentication frame exchange.

If the FT initial mobility domain association is used, then the EDP non-AP STA shall include MDE and FTE in the (Re)Association Request frame. MDE and FTE shall be the same as the ones in the second Authentication frame as described in 12.16.8.1a (FT initial mobility domain association). (#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Request frame. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK-R1). (#176)

For the RSNE included in the (Re)Association Request frame, other than the Length field, the PMKID Count field and the PMKID list field, shall be identical to those in the RSNE present in the first Authentication frame. (#176)

If the FT protocol is used, then the EDP non-AP STA shall not calculate the MIC for the MIC field of the FTE in the Reassociation Request frame. The size of the MIC field of the FTE in the Reassociation Request frame is as defined in 13.8.4 (FT authentication sequence: contents of third message). The MIC field of the FTE and the Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

If dot11DSMACAddressActivated is true and the EDP AP sets the DS MAC Address Support field in the RSNXE to 1, the EDP non-AP STA shall include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP for the mapping to the DS.

The EDP non-AP STA may randomize the DS MAC address. To construct a random DS MAC address, the EDP non-AP STA shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EDP non-AP STA shall use the same DS MAC address for the duration of its connection across an ESS.

The EDP AP shall decrypt the (Re)Association Request frame received from the EDP non-AP STA using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), then the EDP AP shall discard the frame and terminate further protocol processing(#139).

If the FT initial mobility domain association is used, then the FTE and MDE in the (Re)Association Request frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.1a (FT initial mobility domain association). If the MDE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_MDE. If the FTE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_FTE. (#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Request frame is checked to be included and calculated according to the procedures of 12.7.1.6.4 (PMK-R1). If the check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_PMKID. (#176)

The EDP AP shall verify that the RSNE fields other than the Length field, the PMKID Count field and the PMKID list field in the (Re)Association Request frame is identical to the RSNE fields included in the first Authentication frame. The EDP AP shall also verify that the RSNXE in the (Re)Association Request frame is identical to the RSNXE included in the first Authentication frame. If the validation fails, the EDP AP shall reject the association. (#176)

If the FT initial mobility domain association is used, then EDP AP shall include MDE, FTE, TIE[ReassociationDeadline], and TIE[KeyLifetime] in the (Re)Association Response frame. MDE and FTE shall be the same as the ones in the second Authentication frame as described in 12.16.8.1a (FT initial mobility domain association). The reassociation deadline timeout is set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime].(#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Response frame. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 12.7.1.6.4 (PMK-R1). (#176)

If the FT protocol is used, then the EDP AP shall not wrap the Key field of the subelements in the FTE in the Reassociation Response frame and shall not calculate the MIC for the MIC field of the FTE in the Reassociation Response frame. The size of the MIC field of the FTE in the Reassociation Response frame is as defined in 13.8.5 (FT authentication sequence: contents of fourth message). The MIC field of the FTE and the Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

The EDP AP shall encrypt the (Re)Association Response frame transmitted to the EDP non-AP STA in response to the (Re)Association Request frame using the TK and the pairwise cipher indicated in the Authentication frame exchange.

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

If a Key Delivery element is included in the (Re)Association Response frame, the EDP AP shall construct the Key Delivery element indicating the current GTK PN in the RSC subfield, with the GTK KDE, with the IGTK KDE if management frame protection is enabled, with the BIGTK KDE if beacon protection is enabled, and with the WIGTK KDE if WUR frame protection is enabled.

The EDP non-AP STA shall decrypt the (Re)Association Response frame received from the EDP AP using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), then the EDP non-AP STA(#678) shall discard the frame and terminate further protocol processing. (#139)

If the FT protocol is not used, the FT initial mobility domain association is not used, (#176) and in the (Re)Association Response frame the RSNE fields are not identical to the corresponding RSNE fields in the Beacon or(#680) Probe Response frames received from the EDP AP, the EDP non-AP STA shall discard the response.(#679)

If the FT protocol is not used(#176), the EDP non-AP STA shall verify that the RSNXE included in the (Re)Association Response frame (#176)is identical to the RSNXE included in the Beacon or(#680) Probe Response frames received from the EDP AP. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP STA shall discard the response.(#679)

If the FT initial mobility domain association is used, then the FTE and MDE in the (Re)Association Response frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.1a (FT initial mobility domain association). If the check fails, the EDP non-AP STA shall discard the response. (#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Response frame is checked to be included and identical to the value that is sent in the Association Request frame. If the check fails, the EDP non-AP STA shall discard the response. (#176)

If the FT initial mobility domain association is used and in the (Re)Association Response frame the RSNE fields other than the Length field, the PMKID Count field and the PMKID list field are not identical to the corresponding RSNE fields in the Beacon or Probe Response frames received from the EDP AP, the EDP non-AP STA shall discard the response. (#176)

If IEEE 802.1X Authentication utilizing Authentication frame is used, and the RSN capabilities fields of the RSNE received in the (Re)Association Response frame is not identical to the RSN capabilities fields of the RSNE received in the second Authentication frame, the EDP non-AP STA shall discard the response.(#176)

On a successful (re)association,

* The EDP non-AP STA shall process the Key Delivery element in the (Re)Association Response frame if present.
* The EDP non-AP STA shall install the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true.
* The EDP AP and the EDP non-AP STA shall transition to State 4 (as defined in 11.3 (STA authentication and association)).
* If the DS MAC Address element is included in the (Re)Association Request frame, the EDP non-AP STA shall use the indicated DS MAC address rather than the MAC address of the EDP non-AP STA for the EDP non-AP STA to the EDP AP mapping to the DS(#681).
* If the DS MAC Address element is included in the (Re)Association Request frame, the EDP AP shall process the DS MAC Address element and use the indicated DS MAC address to establish the EDP non-AP STA to the EDP AP(#681) mapping to the DS rather than the MAC address of the EDP non-AP STA.

NOTE 1—If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EDP non-AP STA are set to the DS MAC address, which is the identity of the non-AP STA known by the DS.

On a failed (re)association, the established PTKSA shall be irretrievably deleted.

* MLO procedure(#945)

A non-AP MLD that sets the (Re)Association Frame Encryption Support field in the RSNXE to 1 shall indicate a pairwise cipher, establish a PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP MLD if APs affiliated with the EDP AP MLD set the (Re)Association Frame Encryption Support field in the RSNXE to 1 (see 12.16.8 (Key derivation with Authentication frame exchange) and 12.16.9 (Enhanced Data Privacy Key Exchange))(#850).

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

An EDP non-AP MLD shall randomize the STA MAC addresses of its affiliated STAs and its MLD MAC address during a BSS transition if the BSS transition procedure uses an encrypted (Re)Association Request frame to carry the DS MAC Address element.

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, 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.(#682)

If the FT initial mobility domain association is used, then the EDP non-AP MLD shall include MDE and FTE in the (Re)Association Request frame. MDE and FTE shall be the same as the ones in the second Authentication frame as defined in 12.16.8.1a (FT initial mobility domain association).(#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Request frame. The PMKR1Name shall be as calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK-R1). (#176)

For the RSNE included in the (Re)Association Request frame, other than the Length field, the PMKID Count field and the PMKID list field, shall be identical to the RSNE fields in the first Authentication frame. (#176)

The (Re)Association Request frame shall:

* Have the Address 1 field equal to the Address 1 field of the Authentication frame used by the non-AP MLD to establish the(#683) PTKSA
* Have the Address 2 field equal to the Address 2 field of the Authentication frame used by the non-AP MLD to establish the(#683) PTKSA
* Include the DS MAC Address element in the (Re)Association Request frame to indicate the DS MAC address to be used by the EDP AP MLD for the mapping to the DS if dot11DSMACAddressActivated is true and the APs affiliated with the EDP AP MLD set the DS MAC Address Support field in the RSNXE to 1.

If the FT protocol is used, then the EDP non-AP MLD shall not calculate the MIC for the MIC field of the FTE in the Reassociation Request frame. The size of the MIC field of the FTE in the Reassociation Request frame is as defined in 13.8.4 (FT authentication sequence: contents of third message). The MIC field of the FTE and the Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

An EDP non-AP MLD may randomize its DS MAC address. To construct a random DS MAC address, the EDP non-AP MLD shall select the randomized DS MAC address according to IEEE Std 802-2014 and IEEE Std 802c-2017. If dot11DSMACAddressActivated is true, the EDP non-AP MLD shall use the same DS MAC address for the duration of its connection across an ESS.

The EDP AP MLD shall decrypt the (Re)Association Request frame received from the EDP non-AP MLD using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing)), then the EDP AP MLD shall discard the frame and terminate further protocol processing.(#139)

If the FT initial mobility domain association is used, then the FTE and MDE in the (Re)Association Request frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.1a (FT initial mobility domain association). If the MDE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_MDE. If the FTE check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_FTE. (#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Request frame is checked to be included and calculated according to the procedures of 12.7.1.6.4 (PMK-R1). If the check fails, the (Re)Association Request frame is rejected with status code STATUS\_INVALID\_PMKID. (#176)

The EDP AP MLD shall verify that the RSNE fields other than the Length field, the PMKID Count field and the PMKID list field in the (Re)Association Request frame is identical to the RSNE fields included in the first Authentication frame. The EDP AP MLD shall also verify that the RSNXE in the (Re)Association Request frame is identical to the RSNXE included in the first Authentication frame. If the validation fails, the EDP AP MLD shall reject the association. (#176)

If the FT initial mobility domain association is used, then EDP AP MLD shall include MDE, FTE, TIE[ReassociationDeadline], and TIE[KeyLifetime] in the (Re)Association Response frame. MDE and FTE shall be the same as the ones in the second Authentication frame as described in 12.16.8.1a (FT initial mobility domain association). The reassociation deadline timeout is set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime].(#176)

If the FT initial mobility domain association is used, then the PMKR1Name shall be included in the RSNE in the (Re)Association Response frame. The PMKR1Name shall be as calculated by the R1KH according to the procedures of 12.7.1.6.4 (PMK-R1). (#176)

If the FT protocol is used, then the EDP AP MLD shall not wrap the Key field of the subelements in the FTE in the Reassociation Response frame and shall not calculate the MIC for the MIC field of the FTE. The size of the MIC field of the FTE in the Reassociation Response frame is as defined in 13.8.5 (FT authentication sequence: contents of fourth message). The MIC field of the FTE and the Element Count subfield of the MIC Control field of the FTE shall be set to 0.(#915)

The EDP AP MLD shall encrypt the (#684)(Re)Association Response frame transmitted to the EDP non-AP MLD in response to the (Re)Association Request frame using the TK and the pairwise cipher indicated in the Authentication frame exchange.

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

If a Key Delivery element is included in the (Re)Association Response frame, the EDP AP MLD shall construct the Key Delivery element with the RSC field set to 0, with the MLO GTK KDE for each setup link, with the MLO IGTK KDE for each setup link if management frame protection is negotiated, with the MLO BIGTK KDE for each setup link if beacon protection is enabled, and with the PGTK KDE if the Group EDP Epoch Supported field in the RSNXE is set to 1by the APs affiliated with the AP MLD and the non-AP MLD (#685).

The EDP non-AP MLD shall decrypt the (Re)Association Response frame received from the EDP AP MLD using the TK and the pairwise cipher indicated in the Authentication frame exchange. If there is no output from the decryption algorithm because of unsuccessful MIC check (see 12.5.2.4.2 (CCM recipient processing) and 12.5.4.4.2 (GCM recipient processing))(#139), the EDP non-AP(#678) MLD shall discard the frame and terminate further protocol processing(#139).

If the FT protocol is not used, the FT initial mobility domain association is not used, (#176) and in the (Re)Association Response frame the RSNE fields corresponding to each link are not identical to the corresponding RSNE fields of the link in the Beacon or(#680) Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD, the EDP non-AP MLD shall discard the response.(#679)

If the FT protocol is not used(#176), the EDP non-AP MLD shall verify that the RSNXE corresponding to each link in the (Re)Association Response frame(#176) is identical to the corresponding RSNXE of the link in the Beacon or(#680) Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD. If those frames did not include the RSNXE or if the RSNXEs are not identical, the EDP non-AP MLD shall discard the response.(#679)

If the FT initial mobility domain association is used, then the FTE and MDE in the (Re)Association Response frame are checked to be the same as those provided in the second Authentication frame as defined in 12.16.8.1a (FT initial mobility domain association). If the check fails, the EDP non-AP MLD shall discard the response. (#176)

If the FT initial mobility domain association is used, then the PMKR1Name in the RSNE in the (Re)Association Response frame is checked to be included and identical to the value that is sent in the (Re)Association Request frame. If the check fails, the EDP non-AP MLD shall discard the response. (#176)

If the FT initial mobility domain association is used and in the (Re)Association Response frame the RSNE fields other than the Length field, the PMKID Count field and the PMKID list field corresponding to each link are not identical to the corresponding RSNE fields of the link in the Beacon or Probe Response frames received from the corresponding AP affiliated with the EDP AP MLD or in the multi-link probe response received from the EDP AP MLD, the EDP non-AP MLD shall discard the response. (#176)

If IEEE 802.1X Authentication utilizing Authentication frame is used, and the RSN capabilities fields of the RSNE received in the (Re)Association Response frame is not identical to the RSN capabilities fields of the RSNE received in the second Authentication frame, the EDP non-AP MLD shall discard the response. (#176)

On successful (re)association,

* The EDP non-AP MLD shall process the Key Delivery element in the (Re)Association Response frame if present.
* The EDP non-AP MLD shall install the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and PGTK if the Group EDP Epoch Supported field in the RSNXE is set to 1by the APs affiliated with the AP MLD and the non-AP MLD(#685).
* The EDP AP MLD and the EDP non-AP MLD shall transition to State 4 (as defined in 11.3 (STA authentication and association)).
* If the DS MAC Address element is included in the (Re)Association Request frame, the EDP non-AP MLD shall use the indicated DS MAC address for the EDP non-AP MLD to the(#681) EDP AP MLD mapping to the DS rather than the MLD MAC address of the non-AP MLD.
* If the DS MAC Address element is included in the (Re)Association Request frame, the EDP AP MLD shall process the DS MAC Address element and use the indicated DS MAC address to establish the EDP non-AP MLD to the(#681) EDP AP MLD mapping to the DS rather than the MLD MAC address of the EDP non-AP MLD.

NOTE 2—If the DS MAC Address element is included in the (Re)Association Request frame, the source address or destination address parameters of the MAC service tuples (see 5.2.4.2 (Semantics of the service primitive)) for the EDP non-AP MLD are set to the DS MAC address, which is the identity of the non-AP MLD known by the DS.

On failed (re)association, the established PTKSA shall be irretrievably deleted.

***TGbi Editor: modify 12.16.8.2 as follows***

**12.16.8.2 IEEE 802.1X**

(…existing texts…)

 (#176)

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

**12.16.4 EDP capabilities and operation parameters request and response procedure**

**12.16.4.1 Non-MLO procedure(#945)**

**12.16.4.2 MLO procedure(#945)**

**TGbi Editor: *Instruction: Modify 11.2.3.15.2 as follows***

**11.2.3.15.2 WNM sleep mode non-AP STA operation**

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

The receipt of an MLME-SLEEPMODE.confirm primitive with a valid SleepMode parameter indicates to

the STA's SME that the AP has processed the corresponding WNM Sleep Mode Request frame. The content

of the WNM sleep mode parameter in the WNM Sleep Mode Response frame provides the status of WNM

Sleep Mode elements processed by the AP. The non-AP STA shall delete the GTKSA if the response indicates

success. If RSN is used with management frame protection, the non-AP STA shall delete the IGTKSA

if the response indicates success, If RSN is used with beacon frame protection, the non-AP STA shall delete

the BIGTKSA if the response indicates success. If the Group EDP Epoch Supported field in the RSNXE is set to 1by the APs affiliated with the AP MLD and the

non-AP MLD, the non-AP MLD shall delete the PGTKSA if the response indicates success.(#685)

**TGbi Editor: *Instruction: Modify 13.2 as follows***

**13.2 Key holders**

**13.2.2 Authenticator key holders**

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

The R1KH shall meet the following requirements:

…..

— For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that sets the Group EDP Epoch Supported field in the RSNXE to 1.(#685)

…..