IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bi D0.4 CR for 12.14.5 | | | | |
| Date: 2024-07-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

1488, 1442, 1125, 1127, 1443, 1444, 1445, 1446, 1447, 1448,

1449, 1450, 1451, 1452, 1126, 1128, 1453, 1454, 1455, 1456,

1457, 1458, 1459, 1460, 1461, 1463, 1464, 1512, 1067, 1131,

1234, 1508, 1509, 1510, 1143, 1144, 1462, 1511, 1035

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the offline discussion
* Rev 2: Further revision for 1512

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D0.5 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.5 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1488 | Mark RISON | C.3 | 0.00 | "dot11EDPEncryptionOfTheFrameBodyFieldOfTheReAssociationRequestResponseFrameSupportActivated" -- such a long MIB attribute name is a violation of the Geneva convention | As it says in the comment | Revised –  Agree in principle with the commenter.  We change the MIB to dot11EDPReAssociationFrameEncryptionSupportActivated agreed in CID 1042. We also change the field name correspondingly.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1488 |
| 1442 | Mark RISON | 12.14.5 | 75.65 | "nd include DS MAC Address element in the encrypted (Re)Association Request frame." -- this is not where this should be defined. Frame contents are defined in the tables in Clause 9. Ditto stuff like "The EDP non-AP STA shall include the DS MAC Address element in the (Re)Association Request frame" | As it says in the comment | Rejected –  We note that per baseline, there are “shall” statement for inclusion of the elements.  *When dot11OperatingClassesRequired and dot11ExtendedChannelSwitchActivated are true and a*  *STA is capable of operating as specified in more than one operating class, the STA shall include the*  *Supported Operating Classes element in (Re)Association Request and Response frames.* |
| 1125 | Po-Kai Huang | 12.14.5.1 | 77.11 | "established PTKSA" should be "the established PTKSA" | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1125 |
| 1127 | Po-Kai Huang | 12.14.5.1 | 76.61 | Move second and fifth bullet before the first bullet because operation of key should be before transiton to state 4 | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1127 |
| 1443 | Mark RISON | 12.14.5.1 | 76.06 | "Encryption of the Frame Body Field of the (Re)Association Request/ Response Frame Support subfield" is probably the worst field name ever, but at least all words should start with an uppercase letter and it should be field not subfield | As it says in the comment | Revised –  Agree in principle with the commenter.  We change the MIB to dot11EDPReAssociationFrameEncryptionSupportActivated and change the name correspondingly as done in CID 1488.  We change subfield to field across the spec based on CID 1242.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1488 |
| 1444 | Mark RISON |  | 0.00 | Articles missing in many places (e.g. "establish PTKSA") | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1444 |
| 1445 | Mark RISON | 12.14.5.1 | 76.18 | "then the EDP" should be "the EDP" | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1445 |
| 1446 | Mark RISON | 12.14.5.1 | 76.20 | "the indicated pairwise cipher" should be "the pairwise cipher indicated". Ditto below (multiple) | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1446 |
| 1447 | Mark RISON | 12.14.5.1 | 0.00 | "Key delivery element " bad case (multiple) | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1447 |
| 1448 | Mark RISON | 12.14.5.1 | 0.00 | "with WIGTK KDE" missing article | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1448 |
| 1449 | Mark RISON | 12.14.5.1 | 76.59 | "to enable Data frame transmission" -- you transition to State 4 full stop, not restricted to any specific behaviour. Also in other subclauses | Delete the cited text | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1449 |
| 1450 | Mark RISON | 12.14.5.1 | 0.00 | Sentences should start with uppercase letters | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1450 |
| 1451 | Mark RISON | 12.14.5.1 | 76.64 | "the EDP non-AP STA to EDP AP mapping to the DS" not clear | Clarify | Rejected –  This follows the same writing style of baseline for DS mapping. See the following.  *“For a non-GLK STA, the act of becoming associated invokes the association service, which provides the STA to AP mapping to the DS.”* |
| 1452 | Mark RISON | 12.14.5.1 | 77.05 | " The EDP non-AP STA installs" -- why is this not a shall like the others? | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1452 |
| 1126 | Po-Kai Huang | 12.14.5.2 | 78.31 | "established PTKSA" should be "the established PTKSA" | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1125 |
| 1128 | Po-Kai Huang | 12.14.5.2 | 78.17 | Move second and fifth bullet before the first bullet because operation of key should be before transiton to state 4 | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1127 |
| 1453 | Mark RISON | 12.14.5.2 | 0.00 | "establish PTKSA" missing article | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1444 |
| 1454 | Mark RISON | 12.14.5.2 | 77.17 | "drive a temporal key (TK)" -- what does it mean to drive a key? Ah, maybe "derive"? | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1454 |
| 1455 | Mark RISON | 12.14.5.2 | 0.00 | "uses encrypted (Re)Association Request frame" missing article. Also "If FILS authentication and FT protocol are not used" | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1455 |
| 1456 | Mark RISON | 12.14.5.2 | 77.34 | "the indicated pairwise cipher in the Authentication frame exchange" -- order of words is wrong. More below | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1446 |
| 1457 | Mark RISON | 12.14.5.2 | 77.39 | "the value of the Address 1 field" -- these can all have the "the value of"s deleted | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1457 |
| 1458 | Mark RISON | 12.14.5.2 | 77.64 | "include a Key Delivery element into the (Re)Association Response frame. " should be in not into | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1458 |
| 1459 | Mark RISON |  | 0.00 | "Key delivery element" should be "Key Delivery element" | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1447 |
| 1460 | Mark RISON | 12.14.5.2 | 78.03 | ", with the MLO BIGTK KDE for each setup link if beacon protection is enabled." should be "and with the..." | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1460 |
| 1461 | Mark RISON | 12.14 | 0.00 | What is an "association exchange"? | Delete "exchange" | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1463 |
| 1463 | Mark RISON | 12.14.5.2 | 77.55 | "the association exchange fails and the EDP AP MLD shall reject the association" -- what is the difference? Also previous subclause | Delete from "and" onwards | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1463 |
| 1464 | Mark RISON | 12.14.5.2 | 0.00 | There seems to be a lot of duplication between 12.14.5.1 and .2 | Have a subclause with all the common stuff, and reduce the existing subclauses to the diffs only | Rejected –  Separate clauses are written since the entity under description are different (non-AP STA vs non-AP MLD). Mixing into one sentence will have a lot of “respectively” description and that seems to confuse reader based on the experience in 11be. |
| 1512 | Jarkko Kneckt | 12.14.5.2 | 76.63 | When DS addresses are in use, what is the Transmitter address of a group addressed data frames transmitted by a STA? Is this address set to DS address? | Please clarify whether group addressed frames created by the associated STAs use DS address. | Revised –  For a client, the STA does not transmit group addressed data frame. After talking with the commenter, understand that the fundamental question is whether SA will be the DS MAC address. We clarify that SA has to be equal to the DS MAC address.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1512 |
| 1067 | Antonio DeLaOlivaDelgado | 12.14.5.2 | 77.27 | The phrase "An EDP non-AP MLD shall randomize over-the-air MAC address (including STA MAC address and MLD MAC address) during BSS transition if the BSS transition procedure uses encrypted" may imply you change the MLD MAC address while not all the affiliated STAs have finished the handover, may it brake something? | Just think if this may brake something, imho it may happen you change the MLD MAC Address while the handover has not been complited for all affilaited STAs and may create a mess | Rejected –  For MLD, the transition is per MLD, and there is no per affiliated STA transition. |
| 1131 | Po-Kai Huang | 9.4.2.1 | 36.21 | Missing extensible and fragmentable description for DS MAC address element. Likely NO for fragmentable and discuss whether we need the element to be extensible | As in comment | Revised –  Agree in principle with the commenter. For extensible, we make this element not extensible because it is hard to know if the peer can parse the added information in the future anyway.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1131 |
| 1234 | Mark RISON |  | 0.00 | The term "DS MAC address" is used but not defined | As it says in the comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1234 |
| 1508 | Jarkko Kneckt | 12.14.5 | 75.63 | Is there requirements for the DS MAC address selection? How the 48 bits of the DS address may be configured? | Please clarify how the 48 bits of address are set for the DS address. | Revised –  DS MAC address is a MAC address used for DS mapping purpose. We clarify this through definition.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1234 |
| 1509 | Jarkko Kneckt | 12.14.5 | 75.63 | Can the proxy ARP use DS address? What are the procedures for proxy arp to use DS address? | Please clarify how the DS address is used by the proxy ARP. | Revised –  Agree in principle with the commenter. We follow similar modification in ARP clause for MLD MAC address.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1509 |
| 1510 | Jarkko Kneckt | 12.14.5 | 75.63 | The DS address use in FT should describe the AP operations needed to use the DS address as STA's MAC address where the IP addresses are bind. | Please add details how DS address is used in the FT or roaming procedures. For instance, how gracious ARP signaling and IP addressed data delivery to the new AP are handled. | Revised –  Agree in principle with the commenter. We follow similar modification in ARP clause for MLD MAC address.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1509 |
| 1143 | Po-Kai Huang | 12.14.5.1 | 76.55 | Verification of RSNE and RSNXE compared with the ones observed during discovery is likely needed. Note that the flow is very similar to the FT flow, where there is no additonal 4-way handshake after. Hence, similar verification rules defined in clause 13 can be used. For example, verify the AKM indicated in (re)association request indicates corresponding AKM. verify pairwise cipher same as indicated in authentication frame (P84 L5 tries to do similar things). Verify RSNE of AP in (re)association resposne same (other than the PMKID Count field and the PMKID List field) as the ones discovered in Beacon and Probe Response. Verify RSNXE of AP in (re)association resposne same as the ones discovered in Beacon and Probe Response. Obviously, under FT, we already have rules, so we do not need further rules. | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1143 |
| 1144 | Po-Kai Huang | 12.14.5.2 | 78.11 | Verification of RSNE and RSNXE compared with the ones observed during discovery is likely needed. Note that the flow is very similar to the FT flow, where there is no additonal 4-way handshake after. Hence, similar verification rules defined in clause 13 can be used. For example, verify the AKM indicated in (re)association request indicates corresponding AKM. verify pairwise cipher same as indicated in authentication frame (P84 L5 tries to do similar things). Verify RSNE of AP in (re)association resposne same (other than the PMKID Count field and the PMKID List field) as the ones discovered in Beacon and Probe Response. Verify RSNXE of AP in (re)association resposne same as the ones discovered in Beacon and Probe Response. Consider using similar language used in 11be. Obviously, under FT, we already have rules, so we do not need further rules. | As in comment | Revised –  Agree in principle with the commenter.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1144 |
| 1462 | Mark RISON | 12.14.5.1 | 76.27 | "The EDP non-AP STA may randomize the DS MAC address." not clear. When may it randomise it? At any time? Ditto next subclause | As it says in the comment | Revised –  Agree in principle with the commenter. We follow the 11aq rule to clarify the selection and no change of DS MAC address during the connection of ESS.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1462 |
| 1511 | Jarkko Kneckt | 12.14.5.2 | 77.49 | The DS MAC address randomization is allowed for the non-AP STA. The procedures in the non-AP STA and AP to randomize this address should be described in details. | Please describe the procedures to randomize DS MAC address. Please explain the operation steps needed by the STA and the AP | Revised –  Agree in principle with the commenter. We follow the 11aq rule to clarify the selection and no change of DS MAC address during the connection of ESS.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1462 |
| 1035 | Chaoming Luo | 11.3.2 | 0.00 | 11.3.2 (State transition diagram for nonmesh STAs) needs to be updated since there is no 4-way handshake after Associated in the case of 802.1X authentication. | As in comment. | Revised –  Agree that the state transition diagrame needs to be changed. No 4-way only happens when encrypted (Re)Association frame exchange is successful.  TGbi editor to make the changes shown in 11-24/1128r2 under all headings that include CID 1035 |

**Discussion:**

**Proposal:**

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

* RSNXE

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

* Extended RSN Capabilities field

|  |  |  |
| --- | --- | --- |
| Bit | Information | Notes |
| … |  |  |
| <ANA>(#1160r4) | (Re)Association Frame Encryption Support(#1488) | A EDP STA sets the (Re)Association Frame Encryption Support subfield to 1 if dot11EDPReAssociationFrameEncryptionSupportActivated is true. Otherwise, this subfield is set to 0. See 12.14.5 (Encryption of the Frame Body Field of the (Re)Association Request/Response Frame).(#1488) |

*TGbi editor: Modify Clause 12.14.8 as follows (track change on):*

**12.14.8 Enhanced Data Privacy Key Exchange**

**12.14.8.1 General**

If dot11EDPKEActivated is true, then dot11EDPEncryptionOfTheReAssociation

FrameSupportActivated is true.(#1433)

(…existing texts…)

*TGbi editor: Modify Clause 12.14.5 as follows (track change on):*

* (Re)Association Request/Response Frame(#1160r4) Encryption (#1488)

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

* non-MLO

An EDP non-AP STA that sets the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1 may indicate a pairwise cipher, establish a(#1444) PTKSA, and derive a temporal key (TK) through Authentication frame exchange with an EDP AP that sets the (Re)Association Frame Encryption Support subfield in the RSNXE to 1.(#1488)

An EDP non-AP STA shall randomize over-the-air MAC address during BSS transition if the BSS transition procedure uses an(#1455) 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, (#1445)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(#1446) in the Authentication frame exchange.

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. The EDP non-AP STA shall use the same DS MAC address for the duration of its connection across an ESS.(#Ed)(#1462)

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(#1446) in the Authentication frame exchange. If the decryption fails, then the EDP AP shall reject the association(#1463).

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(#1446) in the Authentication frame exchange.

If the FILS authentication and the(#1455) FT protocol are not used, the EDP AP shall include a(#Ed) Key Delivery(#1447) element in the (Re)Association Response frame.

If a(#Ed) Key Delivery(#1447) element is included in the (Re)Association Response frame, the EDP AP shall construct the(#Ed) 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(#1460) with the(#1448) 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(#1446) in the Authentication frame exchange. If the decryption fails, then the EDP AP shall reject the association(#1463).

If FT protocol is not used and in the (Re)Association Response frame the RSNE fields are not identical to the corresponding RSNE fields in the Beacon and Probe Response frames received from the EDP AP, the EDP non-AP STA shall discard the response.(#1143)

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 identifical 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.(#1143)

On successful (re)association,

* T(#1450)(#1127)
* The EDP non-AP STA shall install(#1452) 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. (#1127)
* The(#1450) EDP AP and the EDP non-AP STA shall transition to State 4 (as defined in 11.3 (STA authentication and association)). (#1449)
* (#1127)
* The EDP non-AP STA shall use the indicated DS MAC address for the EDP non-AP STA to EDP AP mapping to the DS rather than the MAC address of the EDP non-AP STA.
* The EDP AP shall process the DS MAC Address element and use the indicated DS MAC address to establish EDP non-AP STA to EDP AP mapping to the DS rather than the MAC address of the EDP non-AP STA

(#1127)

NOTE - 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 MLD known by the DS.(#1512)

On failed (re)association, the(#1125) established PTKSA shall be irretrievably deleted.

* MLO

A non-AP MLD that sets the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1 may indicate a pairwise cipher, establish a(#1444) PTKSA, and derive(#1454) 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(#1488) Support subfield in the RSNXE to 1.

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

An EDP non-AP MLD shall randomize over-the-air MAC address (including STA MAC address and MLD MAC address) during BSS transition if the BSS transition procedure uses an(#1455) 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, then 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(#1446) in the Authentication frame exchange.

The (Re)Association Request frame shall:

* Have (#1457)the Address 1 field equal to (#1457)the Address 1 field of the Authentication frame used by the non-AP MLD to establish a(#1444) PTKSA
* Have (#1457)the Address 2 field equal to (#1457)the Address 2 field of the Authentication frame used by the non-AP MLD to establish a(#1444) 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.

The EDP non-AP MLD may randomize the 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.The EDP non-AP MLD shall use the same DS MAC address for the duration of its connection across an ESS.(#1462)

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(#1446) in the Authentication frame exchange. If the decryption fails, then (#1463)the EDP AP MLD shall reject the association.

The EDP AP MLD shall encrypt the transmitted (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(#1446) in the Authentication frame exchange.

If the FILS authentication and the(#1455) FT protocol are not used, the EDP AP MLD shall include a(#Ed) Key Delivery element in(#1458) the (Re)Association Response frame.

If a(#Ed) Key Delivery(#1447) element is included in the (Re)Association Response frame, the EDP AP MLD shall construct the(#Ed) 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, and(#1460) with the MLO BIGTK KDE for each setup link if beacon protection is enabled.

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(#1446) in the Authentication frame exchange. If the decryption fails, the EDP AP MLD shall reject the association(#1463).

If FT protocol is not used 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 and 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.(#1144)

If FT protocol is not used and the (Re)Association Response frame includes the RSNXE, the EDP non-AP MLD shall verify that the RSNXE corresponding to each link is identical to the corresponding RSNXE of the link in the Beacon and 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.(#1144)

On successful (re)association,

* The(#1450) EDP non-AP MLD shall process the Key Delivery element in the (Re)Association Response frame if present. (#1127)
* T(#1450)shall (#1452) (#1127)
* The(#1450) EDP AP MLD and the EDP non-AP MLD shall transition to State 4 (as defined in 11.3 (STA authentication and association)).(#1449)
* (#1127)The(#1450) EDP non-AP MLD shall use the indicated DS MAC address for the EDP non-AP MLD to EDP AP MLD mapping to the DS rather than the MLD MAC address of the non-AP MLD.
* The(#1450) EDP AP MLD shall process the DS MAC Address element and use the indicated DS MAC address to establish EDP non-AP MLD to EDP AP MLD mapping to the DS rather than the MLD MAC address of the EDP non-AP MLD.
* (#1127)

NOTE - 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.(#1512)

On failed (re)association, the(#1125) established PTKSA shall be irretrievably deleted.

*TGbi editor: Modify Clause 12.14.6 as follows (track change on):*

* PMKSA caching privacy(#1664r7)

This subclause defines rules to have PMKSA caching privacy such that the identifier related to PMKSA caching can be recomputed after using the identifier to establish a(#1444) PTKSA, thus, cannot be used for tracking.

A STA that sets the PMKSA Caching Privacy Support subfield in the RSNXE to 1 shall set the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1.

*TGbi editor: Modify Clause 12.14.7 as follows (track change on):*

* Key derivation with Authentication frame exchange(#150r5)

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(#150r5)

If an FTO or FTR (see 13 (Fast BSS transition)) sets the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1, then FTO or FTR supports the additional rules defined in this subclause.

An FTO that sets the Encryption of the (Re)Association Frame Support subfield in the RSNXE to 1 and sees the (Re)Association Frame Encryption Support subfield in the RSNXE of the FTR set to 1 shall: (#1488)

(…existing textrs…)

An FTR that sets the Encryption of the (Re)Association Frame Support subfield in the RSNXE to 1 and receives the first message with the (Re)Association Frame Encryption Support(#1488) subfield in the RSNXE set to 1 shall:

(…existing textrs…)

* 802.1X(#762r2)

If an authentication originator or an authentication responder defined in 12.14.4 (IEEE 802.1X authentication utilizing Authentication frames) sets the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1, then the authentication originator or the authentication responder supports the additional rules defined in this subclause when performing 802.1X Authentication frame exchange.

An authentication originator that sets the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1, has the corresponding SME to act as the Supplicant, sees the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE of the authentication responder set to 1, and intends to continue association after authentication shall:

(…existing texts…)

An authentication responder that sets the (Re)Association Frame Encryption(#1488) Support subfield in the RSNXE to 1, has the corresponding 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:

(…existing texts…)

*TGbi editor: Modify Clause 9.4.2.1 as follows (track change on):*

* General

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element | Element ID | Element ID Extension | Extensible | Fragmentable |
| ...... |  |  |  |  |
| ~~FILS~~ Nonce (see 9.4.2.188 (FILS Nonce element))(#762r2) | 255 | 13 | No | No |
| ..... |  |  |  |  |
| DS MAC Address (see 9.4.2.336 (DS MAC Address element))(#Ed) | 255 | <ANA> | No(#1131) | No(#1131) |
| Enhanced Data Privacy (EDP) element(#Ed) | 255 | <ANA> |  |  |
| Minimum Epoch Pacing element(#Ed) | 255 | <ANA> |  |  |
| Enhanced Group Privacy Availability (EGPA) element(#Ed) | 255 | <ANA> |  |  |
| otaMAC Collision Warning element(#Ed) | 255 | <ANA> |  |  |
| EDP Epoch Setting element(#Ed) | 255 | <ANA> |  |  |
| ... |  |  |  |  |
| NOTE—See 10.28.6 (Element parsing) on the parsing of elements. | | | | |

*TGbi editor: Modify Clause 3.2 as follows (track change on):*

* Definitions specific to IEEE 802.11

***Insert the following definitions (maintaining alphabetical order):***

distribution system (DS) medium access control (MAC) address: [DS MAC adress] A MAC address indicated by an enhanced data privacy (EDP) non–access point (non-AP) station (STA) to an EDP AP or an EDP non-AP multi-link device (MLD) to an EDP AP MLD and used by the EDP AP or the EDP AP MLD as the address to notify the DS and establish the destination mapping for the EDP non-AP STA or the EDP non-AP MLD after (re)association.(#1234)

*TGbi editor: Modify Clause 11.21.14 as follows (track change on):*

* + 1. **Proxy ARP service**

## *Change the second to 11th paragraphs as follows:*

When the AP sets the Proxy ARP field to 1 in the Extended Capabilities element, the AP shall maintain a Hardware Address or a DS MAC address (if present)(#1509) to Internet Address mapping for each associated STA and for each IPv4 and IPv6 address of the STA, and shall update the mapping when one of the addresses of the associated STA changes. When an AP MLD supports proxy ARP (see 35.3.22 (Proxy ARP service in AP MLDs)), the AP MLD shall maintain an MLD MAC address or a DS MAC address (if present)(#1509) to Internet address mapping for each associated non-AP MLD and for each IPv4 and IPv6 address of the non-AP MLD, and shall update the mapping when one of the addresses of the associated non-AP MLD changes. A Proxy ARP service receives and processes three types of messages: IPv4 ARP requests, IPv6 ND address lookups, and IPv6 ND duplicate address detection (DAD) messages. These messages are all received as group addressed. If the target address is not known, the Proxy ARP service does not forward the request to the BSS. If the target address is known, the Proxy ARP service can either respond directly on behalf of a STA or forward the request as an individually addressed frame to the intended STA. For fixed devices in the doze state, a direct response is preferable. Otherwise, forwarding as an individually addressed frame is recommended, to avoid responding with misleading information.

(…existing texts…)

When an AP receives an IPv4 ARP request from one associated STA or from the DS with a target IPv4 address that corresponds to a second associated STA, the AP that decides to form a proxy ARP response frame shall insert the second STA’s MAC address or the second STA’s DS MAC address (if present) (#1509) as the sender’s MAC address in the ARP response. When an AP affiliated with an AP MLD receives an IPv4 ARP request from one associated STA, or from a non-AP STA affiliated with a non-AP MLD that is associated with the AP MLD, or from the DS, with a target IPv4 address that corresponds to a second associated STA, the AP shall insert the second STA’s MAC address or the second STA’s DS MAC address (if present) (#1509) as the Sender’s MAC Address in the ARP response packet. When an AP MLD receives an IPv4 ARP request from a STA associated with an affiliated AP, or from one associated non-AP MLD via any affiliated AP, or from the DS, with a target IPv4 address that corresponds to a second associated non-AP MLD, the AP MLD that decides to form a proxy ARP response shall insert the MLD MAC address or the DS MAC address (if present) (#1509) of the second non-AP MLD as the Sender’s MAC Address in the ARP response packet.

(…existing texts…)

With the IPv6 ND proxy operation defined in IETF RFC 8929, the backbone router function at the AP typically operates as a bridging proxy though operation as a routing proxy is also possible. As a bridging proxy, the NS lookups are replied with the MAC address or the DS MAC address (if present) (#1509) of the STA (or the non-AP MLD), and the packets to the STA (or the non-AP MLD) are bridged normally; as a routing proxy, the backbone router function replies to lookups from the wired backbone with its own MAC address and then routes to the STA (or the non-AP MLD) at the IP layer. The routing proxy isolates the layer-2 domains and hides the MAC address or the DS MAC address (if present) (#1509) of the STA (or the non-AP MLD) in the wired backbone, for a better stability and scalability of the bridged domain. The Proxy ARP function shall support the bridging proxy and may support the routing proxy operation.

(…existing texts…)

*TGbi editor: Modify Clause 11.3.2 as follows (track change on):*

* State transition diagram for nonmesh STAs

(…existing texts.)

(#1035)