### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11be D1.0 CR for FT | | | | |
| Date: 2021-07-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel Corporation | 2200 Mission College Blvd, Santa Clara, CA 950542200 |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  |  |
| Daniel F Bravo |  |  |  |
| Michael Montemurro | Huawei |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

5070

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the feedback received offline.
* Rev 2: Revision based on the feedback received after presentation. Mark with green.
* Rev 3: Revision based on the feedback from Dan Harkins to delete non-RSN and use FTR rather than AP or AP MLD. Mark with blue.
* Rev 4: Editorial change. Mark with blue.

Do you support to accept the resolution in 11-21/1121r4 for the following CIDs?

5070, 7452, 6228

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

***Editing instructions formatted like this are intended to be copied into the TGbe D1.0 Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 5070 | Gaurav Patwardhan | 4.5.3.2 | 46.29 | Missing detail for EHT STAs to use Fast BSS Transition. | Include and extend Clause 13  (Fast BSS Transition) from baseline 802.11-2020 spec to include EHT STAs. | Revised –  Agree in principle with the commenter. The first part of the resolution is approved in 11-21/971r3. We propose the remaining change after 13.5 in this document.  TGbe editor to make the changes shown in 11-21/1211r4 under all headings that include CID 5070. |
| 7452 | Thomas Derham | 12 | 0.00 | Use of FT with MLD does not seem to be defined - e.g. must all links of an MLD advertise the same mobility domain etc? | Define FT operation with MLDs | Revised –  Agree in principle with the commenter. The first part of the resolution is approved in 11-21/971r3, where MDE is the same for all links. We propose the remaining change after 13.5 in this document.  TGbe editor to make the changes shown in 11-21/1211r4 under all headings that include CID 5070. |
| 6228 | Ming Gan | 35.x | 0.00 | If MLD participates the fast BSS transition, the security needs update | as in the comment | Revised –  Agree in principle with the commenter. The first part of the resolution is approved in 11-21/971r3, where MDE is the same for all links. We propose the remaining change after 13.5 in this document.  TGbe editor to make the changes shown in 11-21/1211r4 under all headings that include CID 5070. |

**Discussion:** *None.*

**Propose:**

*TGbe editor: Change Table 9-41* *as follows (track change on): (#5070)*

**9.3.3.11 Authentication frame format**

|  |  |  |  |
| --- | --- | --- | --- |
| Table 9-41 - Presence of fields and elements in Authentication frames | | | |
| Authentication algorithm | Authentication transaction sequence number | Status code | Presence of fields and elements  from order 4 onward |
| Open System | 1 | Reserved | Not present |
| Open System | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | Not present |
| Open System | 2 | REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | One or more Neighbor Report element(s) is present |
| Shared Key | 1 | Reserved | Not present |
| Shared Key | 2 | Any | The Challenge Text element is present |
| Shared Key | 3 | Reserved | The Challenge Text element is present |
| Shared Key | 4 | Any | Not present |
| FT | 1 | Reserved | The Mobility Domain element is present.  The Fast BSS Transition element and RSNEs are present if dot11RSNAActivated is true.  The Basic variant Multi-Link element is present  if the STA is affiliated with an MLD and the frame exchange is with a peer STA that is affiliated with an MLD. |
| FT | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | The Mobility Domain element is present if the Status Code field is 0.  The Fast BSS Transition element and RSNEs are present if the Status Code field is 0 and dot11RSNAActivated is true.  The Basic variant Multi-Link element is present  if the STA is affiliated with an MLD and the frame exchange is with a peer STA that is affiliated with an MLD. |
| FT | 2 | REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | One or more Neighbor Report element(s) is present  The Basic variant Multi-Link element is present  if the STA is affiliated with an MLD and the frame exchange is with a peer STA that is affiliated with an MLD. |
| FT | 3 | Reserved | The Mobility Domain element is present.  The Fast BSS Transition element and RSNEs are present if dot11RSNAActivated is true.  The RIC element is optionally present.  The Basic variant Multi-Link element is present  if the STA is affiliated with an MLD and the frame exchange is with a peer STA that is affiliated with an MLD. |
| FT | 4 | Any | The Mobility Domain element is present if the Status Code field is 0.  The Fast BSS Transition element and RSNEs are present if dot11RSNAActivated is true.  The RIC element is optionally present if the Status Code field is 0.  The TIE (reassociation deadline) is present if a RIC element is present.  The Basic variant Multi-Link element is present  if the STA is affiliated with an MLD and the frame exchange is with a peer STA that is affiliated with an MLD. |
| SAE | 1 | Any | The Scalar field is present if the Status Code field is zero or 126.  The FFE field is present if the Status Code field is zero or 126.  When the hunting-and-pecking method is used to drive the PWE, the Anti-Clogging Token field is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED.  The Finite Cyclic Group field is present if the Status Code field is zero, ANTI\_CLOGGING\_TOKEN\_REQUIRED, 77 or 126.  The Password Identifier element is optionally present if the Status Code field is zero, 123 or 126.  The Rejected Groups element is conditionally present if the Status Code field is 126, as described in 12.4.7.4 (Encoding and decoding of SAE Commit messages). When the hash-to-element method is used to derive the PWE, the Anti-Clogging Token Container element is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED. |
| SAE | 2 | Not REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | The Send-Confirm field is present.  The Confirm field is present. |
| SAE | 2 | REJECTED\_WITH\_SUGGESTED\_BSS\_TRANSITION | One or more Neighbor Report element(s) are present |
| FILS Shared Key authentication without PFS | 1 | Reserved | The RSNE is present.  The MDE is present if the FILS authentication is used for FT initial mobility domain association.  The FILS Nonce element is present.  The FILS Session element is present.  The FILS Wrapped Data element is present. |
| FILS Shared Key authentication without PFS | 2 | Status | The RSNE is present.  The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.  The FILS Nonce element is present if the Status Code field is 0.  The FILS Session element is present if the Status Code field is 0.  The FILS Wrapped Data element is present if the Status Code field is 0.  The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| FILS Shared Key authentication with PFS | 1 | Reserved | The Finite Cyclic Group field is present.  The FFE field is present.  The RSNE is present.  The MDE is present if the FILS authentication is used for FT initial mobility domain association.  The FILS Nonce element is present.  The FILS Session element is present.  The FILS Wrapped Data element is present. |
| FILS Shared Key authentication with PFS | 2 | Status | The Finite Cyclic Group is present if the Status Code field is 0.  The FFE field is present if the Status Code field is 0.  The RSNE is present.  The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.  The FILS Nonce element is present if the Status Code field is 0.  The FILS Session element is present if the Status Code field is 0.  The FILS Wrapped Data element is present if the Status Code field is 0.  The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request frame. |
| FILS Public Key authentication | 1 | Reserved | The Finite Cyclic Group field is present.  The FFE field is present.  The RSNE is present.  The MDE is present if the FILS authentication is used for FT initial mobility domain association.  The FILS Nonce element is present.  The FILS Session element is present. |
| FILS Public Key authentication | 2 | Status | The Finite Cyclic Group is present if the Status Code field is 0.  The FFE field is present if the Status Code field is 0.  The RSNE is present.  The MDE and the FTE are present if the Status Code field is 0 and FILS authentication is used for FT initial mobility domain association.  The FILS Nonce element is present if the Status Code field is 0.  The FILS Session element is present if the Status Code field is 0.  The Association Delay Info element is present if the Status Code field is 0 and the AP expects that the (Re)Association Response frame will be transmitted more than 1 TU after the (Re)Association Request  frame. |

*TGbe editor: Modify the following paragraph in 13.1 Overview (track change on): (#5070)*

The FT protocols require information to be exchanged during the initial association (or a later reassociation) between a STA [known as the *FT Originator* (FTO)] and AP [known as the *FT Responder* (FTR)] or between a non-AP MLD [known as the *FT Originator* (FTO)] and AP MLD [known as the *FT Responder* (FTR)]. The initial exchange is referred to as the *FT initial mobility domain association*. Subsequent reassociations to APs within the same mobility domain may make use of the FT protocols.

*TGbe editor: Change 13.5* *as follows (track change on): (#5070)*

* FT protocol
* Overview

STAs and MLDs with dot11FastBSSTransitionActivated equal to true shall support the FT protocol.

The FT protocol supports resource requests as part of the reassociation. The optional FT resource request protocol (see 13.6 (FT resource request protocol)) supports resource requests prior to reassociation.

A FTO shall not use any authentication algorithm except the FT authentication algorithm when using the FT protocol.

To prevent key reinstallation attacks, the non-AP STA shall maintain a copy of the most recent GTK, IGTK, and BIGTK when present installed as part of the FT protocol as if they were installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation considerations)) and shall refuse to update a GTK, IGTK, or a BIGTK when the key to be set matches any one of these keys (see 6.3.19 (SetKeys)).

* Over-the-air FT protocol authentication in an RSN

The over-the-air FT protocol in an RSN is shown in Figure 13-5 (Over-the-air FT protocol in an RSN).



Figure 13-5 – Over-the-air FT protocol in an RSN

The FTO and FTR use the FT authentication sequence to specify the PMK-R1 security association and to provide values of SNonce and ANonce that enable a liveness proof, replay protection, and PTK separation. This exchange enables a fresh PTK to be computed in advance of reassociation. The PTKSA is used to protect the subsequent reassociation transaction, including the optional RIC-Request.

To perform an over-the-air fast BSS transition to a target FTR, the FTO and target FTR shall perform the following exchange:

FTOTarget FTR: Authentication-Request (FTAA, 0, RSNE[PMKR0Name], MDE, FTE[SNonce, R0KH-ID], Basic variant Multi-Link element)

Target FTRFTO: Authentication-Response (FTAA, Status, RSNE[PMKR0Name], MDE, FTE[ANonce, SNonce, R1KH-ID, R0KH-ID] , Basic variant Multi-link element)

where the Basic variant Multi-Link element is included when the target FTR is an AP MLD.

The SME of the FTO initiates the authentication exchange, through the use of the MLME‑AUTHENTICATE.request primitive, and the SME of the FTR responds with an MLME-AUTHENTICATE.response primitive. See 11.3.4 (Authentication and deauthentication). The MLME primitives for Authentication when the FT authentication algorithm is selected use only authentication transaction sequence number values 1 and 2.

In the Authentication-Request frame that does not include the Basic variant Multi-Link element, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS. In the Authentication-Request frame that includes the Basic variant Multi-Link element, the Address 1 (RA) field and the Address 2 (TA) field of the message header shall be set as defined in 35.3.3 (Multi-link device addressing).

The elements in the frame, and their required contents, shall be as given in 13.8.2 (FT authentication sequence: contents of first message).

If the contents of the MDE received by the FTR do not match the contents advertised in the Beacon and Probe Response frames if the FTR is an AP or in the Beacon and Probe Response frames of any AP affiliated with the FTR if the FTR is an AP MLD, the FTR shall reject the authentication request with status code STATUS\_INVALID\_MDE. If the Authentication-Request frame contains an authentication algorithm equal to FT authentication and the contents of the RSNE do not indicate a negotiated AKM for which the Authentication type column indicates FT authentication (see Table 9-151 (AKM suite selectors)), the FTR shall reject the authentication request with status code STATUS\_INVALID\_AKMP. If the FTE in the FT Request frame contains an invalid R0KH-ID, the FTR shall reject the FT Request frame with status code STATUS\_INVALID\_FTE. If the RSNE in the Authentication-Request frame contains an invalid PMKR0Name and the FTR has determined that it is an invalid PMKR0Name, the FTR shall reject the authentication request with status code STATUS\_INVALID\_PMKID. If the requested R0KH is not reachable, the FTR shall respond to the authentication request with status code R0KH\_UNREACHABLE. If the FTO selects a pairwise cipher suite in the RSNE that is different from the ones used in the Initial mobility domain association, then the FTR shall reject the authentication request with status code STATUS\_INVALID\_PAIRWISE\_CIPHER. Subsequent to a rejection of an authentication request, the FTO may retry the authentication request.

In the Authentication-Response frame that does not include the Basic variant Multi-Link element, the SA field of the message header shall be set to the BSSID of the target AP’s BSS, and the DA field of the message header shall be set to the MAC address of the FTO. In the Authentication-Response frame that includes the Basic variant Multi-Link element, the Address 1 (RA) field and the Address 2 (TA) field of the message header shall be set as defined in 35.3.3 (Multi-link device addressing).

The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field). The elements in the frame, and their required contents, shall be as given in 13.8.3 (FT authentication sequence: contents of second message).

The R1KH of the target FTR uses the value of PMKR0Name and other information in the frame to calculate PMKR1Name. If the target FTR does not have the key identified by PMKR1Name, it may retrieve that key from the R0KH identified by the FTO. See 13.2 (Key holders). Upon receiving a new PMK-R1 for a FTO, the target FTR shall delete the prior PMK-R1 security association and PTKSAs derived from the prior PMK-R1.

The FTO and the target FTR compute the PTK and PTKName using the PMK-R1, PMKR1Name, ANonce, and SNonce, as specified in 12.7.1.6.5 (PTK). The PTKSA shall be deleted by the target FTR if it does not receive a Reassociation Request frame from the FTO within the reassociation deadline timeout value.

If the FTO does not receive a response to the Authentication-Request frame, it may reissue the request following the restrictions given for Authentication frames in 11.3 (STA authentication and association). If the Status Code field value returned by the target FTR is SUCCESS, the FTO and target FTR transition to State 2 (as defined in 11.3 (STA authentication and association)); the FTO may continue with reassociation (13.7.1 (FT reassociation in an RSN)). Handling of errors returned in the Status Code field shall be as specified in 11.3 (STA authentication and association).

*TGbe editor: Change 13.7* *as follows (track change on): (#5070):*

* FT reassociation
* FT reassociation in an RSN

If the FTO does not send a Reassociation Request frame to the target FTR within the reassociation deadline interval received during the FT initial mobility domain association, the target FTR may delete the PTKSA, and the FTO shall abandon this transition attempt.

The FTO shall perform a reassociation directly with the target FTR via the following exchange:

FTOTarget FTR: Reassociation Request(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request, RSNXE, Basic variant Multi-Link element)

Target FTRFTO: Reassociation Response(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N], IGTK[M], BIGTK[Q], MLO GTKn, MLO IGTKn, MLO BIGTKn], RIC‑Response, RSNXE, Basic variant Multi-Link element)

, where

* MLO GTKn is MLO GTK subelement for link n, MLO IGTKn is MLO IGTK subelement for link n, and MLO BIGTKn is MLO BIGTK subelement for link n.
* The GTK[N], IGTK[M], BIGTK[Q] is present when the FTR is an AP.

The MLO GTKn, MLO IGTKn, MLO BIGTKn, and the Basic variant Multi-Link element is present when the FTR is an AP MLD.

The SME of the FTO initiates the reassociation through the use of the MLME-REASSOCIATE.request primitive. The SME of the FTR responds to the indication with MLME-REASSOCIATE.response primitive. See 11.3.5 (Association, reassociation, and disassociation).

In the Reassociation Request frame that does not include the Basic variant Multi-Link element, the SA field of the message header shall be set to the MAC address of the FTO, and the DA field of the message header shall be set to the BSSID of the target AP’s BSS. In the Reassociation Request frame that includes the Basic variant Multi-Link element, the Address 1 (RA) field and the Address 2 (TA) field of the message header shall be set as defined in 35.3.3 (Multi-link device addressing).

The elements in the frame, the element contents, and the MIC calculation shall be as given in 13.8.4 (FT authentication sequence: contents of third message).

The R1KH of the target FTR verifies the MIC in the FTE in the Reassociation Request frame and shall discard the request if the MIC is incorrect.

If the target FTR is an AP that includes an RSNXE in its Beacon and Probe Response frames and the RSNXE Used subfield of the MIC Control field of the FTE is set to 1 or if the target FTR is an AP MLD and any AP affiliated with the AP MLD includes an RSNXE in its Beacon and Probe Response frames and the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, but the Reassociation Request frame does not include an RSNXE, the R1KH of the target FTR shall discard the request.

If dot11RSNAOperatingChannelValidationActivated is true and the FTO indicates OCVC capability, the target AP shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true:

* OCI subelement is present
* Channel information in the OCI matches current operating channel parameters (see 12.2.9 (Requirements for Operating Channel Validation))

Otherwise, the AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE.

If the contents of the MDE received by the target FTR do not match the contents advertised in the Beacon and Probe Response frames if the FTR is an AP or in the Beacon and Probe Response frames of any APs affiliated with the FTR if the FTR is an AP MLD, the target FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDEIf the FTE in the Reassociation Request frame contains a different R0KH-ID, R1KH-ID, ANonce, or SNonce, the FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE. If the RSNE in the Reassociation Request frame contains an invalid PMKR1Name, the FTR shall reject the Reassociation Request frame with status code STATUS\_INVALID\_PMKID.

In the Reassociation Response frame that does not include the Basic variant Multi-Link element, the SA field of the message header shall be set to the BSSID of the target AP’s BSS, and the DA field of the message header shall be set to the MAC address of the FTO. In the Reassociation Response frame that includes the Basic variant Multi-Link element, the Address 1 (RA) field and the Address 2 (TA) field of the message header shall be set as defined in 35.3.3 (Multi-link device addressing).

The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field). The elements in the frame, the element contents, and the MIC calculation shall be as given in 13.8.5 (FT authentication sequence: contents of fourth message).

The S1KH of the FTO verifies the MIC in the FTE in the Reassociation Response frame and shall discard the response if the MIC is incorrect.

If in the Reassociation Response frame the RSNE fields other than the PMKID Count field and the PMKID List field are not identical to the corresponding RSNE fields in the Beacon and Probe Response frames received from the target FTR if the FTR is an AP or if in the Reassociation Response frame the RSNE fields other than the PMKID Count field and the PMKID List field of each link are not identical to the corresponding RSNE fields of the link in the Beacon and Probe Response frames received from any AP affiliated with the FTR if the FTR is an AP MLD, the S1KH of the FTO shall discard the response. If the PMKID List field does not include the correct PMKR1Name value, the S1KH of the FTO shall discard the response.

If the Beacon and Probe Response frames received from the target FTR if the FTR is an AP or the Beacon and Probe Response frames received from an AP affiliated with the target FTR if the FTR is an AP MLD did not include an RSNXE, but the RSNXE Used subfield of the MIC Control field of the FTE is set to 1, the S1KH of the FTO shall discard the response.

If the Reassociation Response frame includes the RSNXE, the S1KH of the FTO shall verify that this element matches information included in the Beacon and Probe Response frames received from the target FTR if the FTR is an AP or in the Beacon and Probe Response frames received from any AP affiliated with the target FTR if the FTR is an AP MLD. If those frames did not include the RSNXE or if the contents of the RSNXE are not identical, the S1KH of the FTO shall discard the response.

If dot11RSNAOperatingChannelValidationActivated is true and the target AP indicates OCVC capability, FTO shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true

* OCI subelement is present
* Channel information in the OCI matches current operating channel parameters (see 12.2.9 (Requirements for Operating Channel Validation))

Otherwise, the FTO rejects the Reassociation Response frame by discarding the frame.

If an FTO is performing a reassociation exchange as part of the FT resource request protocol, then the FTO shall not include the RIC-Request in the Reassociation Request frame, and the AP shall not include the RIC-Response in the Reassociation Response frame. If the reassociation exchange is part of the FT resource request protocol and the AP is unable to honor the resources that have been placed in the accepted state for that FTO, then the AP shall reject the Reassociation Request frame and may use status code DENIED\_INSUFFICIENT\_BANDWIDTH.

If the FTO did not utilize the FT resource request protocol, the FTO may make a request for resources by including a RIC-Request (see 13.11 (Resource request procedures)) in the Reassociation Request frame. The RIC-Request is generated by the procedures of 13.11.3.1 (FTO procedures), and the RIC-Response is generated by the procedures of 13.11.3.2 (AP procedures).

If the Status Code field value returned by the target FTR in the response is REFUSED\_REASON\_UNSPECIFIED, TRANSACTION\_SEQUENCE\_ERROR, or REJECTED\_SEQUENCE\_TIMEOUT, then the FTO shall abandon this transition attempt. Handling of other errors returned in the Status Code field shall be as specified in 11.3 (STA authentication and association).

Upon a successful reassociation, the PTKSA has been established and proven live. The SME of the FTR shall open the IEEE 802.1X Controlled Port. The FTO shall transition to State 4 (as defined in 11.3 (STA authentication and association)). If the target FTR is distinct from the previous FTR the FTO shall enter State 1 with respect to the previous FTR.

Upon a successful reassociation, the FTO shall delete any corresponding PTKSA with its previous FTR. The SME of the FTO shall issue an MLME-DELETEKEYS.request primitive to delete the pairwise keys with the previous FTR, and the FTO and the FTR shall issue an MLME-SETKEYS.request primitive and MLME-SETPROTECTION.request primitive to install the pairwise keys. The PTK lifetime timer shall be initialized with the value calculated as the difference between the TIE[KeyLifetime] sent in message 3 of the FT initial mobility domain association and the time since the completion of the FT 4-way handshake during the FT initial mobility domain association.

When the IEEE 802.1X Controlled Port is opened, the EAPOL-Key frame replay counter shall be initialized to 0. The R1KH shall increment the key replay counter on each successive EAPOL-Key frame that it transmits.

*TGbe editor: Change 13.8* *as follows (track change on): (#5070)*

* FT authentication sequence
* Overview

The FT authentication sequence comprises four sets of FT elements. Each set of FT elements is referred to in 13.8 (FT authentication sequence) as a *message*. These messages are included in the FT Protocol frames or FT Resource Request Protocol frames to initiate a fast BSS transition. The FT authentication sequence is always initiated by the FTO and responded to by the target FTR.

In an RSN, the first two messages in the sequence allow the FTO and target FTR to provide association instance identifiers, SNonce and ANonce, respectively. SNonce and ANonce are chosen randomly or pseudorandomly and are used to generate a fresh PTK. The first two messages also enable the target FTR to provision the PMK-R1 and the FTO and target FTR to compute the PTK. The third and fourth messages demonstrate liveness of the peer, authenticate the elements, and enable an authenticated resource request.

When an FTO invokes the FT protocol, then the first two messages of the sequence are both carried in Authentication frames or both carried in Action frames, and these messages are described in 13.8.2 (FT authentication sequence: contents of first message) and 13.8.3 (FT authentication sequence: contents of second message). The third and fourth messages in the sequence are carried in the Reassociation Request and Reassociation Response frames and are described in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message).

When the FTO invokes the FT resource request protocol, then the first four messages of the sequence are all carried in Authentication frames or all carried in Action frames, and these messages are described in 13.8.2 (FT authentication sequence: contents of first message) to 13.8.5 (FT authentication sequence: contents of fourth message). The fifth and sixth frames of the FT resource request protocol are carried in the Reassociation Request frame and Reassociation Response frame and are described in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message).

Regardless of the transport mechanism, the information contained in the FT authentication sequence consists of the set of elements shown in Table 13-1 (FT authentication elements).

|  |  |  |
| --- | --- | --- |
| * FT authentication elements | | |
| Information | Presence in Authentication Sequence messages | Description |
| RSN | The RSNE is present if dot11RSNAActivated is true. | 9.4.2.24 (RSNE) |
| Mobility Domain | The Mobility Domain element is present. | 9.4.2.46 (Mobility Domain element (MDE)) |
| Fast BSS Transition | The Fast BSS Transition element is present if dot11RSNAActivated is true. | 9.4.2.47 (Fast BSS Transition element (FTE)) |
| Timeout Interval (reassociation deadline) | The Timeout Interval element is optionally present in the fourth message of the sequence if dot11RSNAActivated is not true. | 9.4.2.48 (Timeout Interval element (TIE)) |
| RIC | The RIC Data element is optionally present in the third and fourth messages. | 9.4.2.49 (RIC Data element (RDE)) |
| RSNXE | The RSNXE is present in the third message if an RSNXE is present in a Beacon or Probe Response frame that the FTO has received from the target AP or an AP affiliated with the target AP MLD and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element, and is present in the fourth message if an RSNXE was present in the third message and the target AP or an AP affiliated with the target AP MLD set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element. | 9.4.2.241 (RSN Extension element (RSNXE)) |

The first message is used by the FTO to initiate a fast BSS transition. When RSNA is enabled, the FTO shall include the R0KH-ID and the SNonce in the FTE and the PMKR0Name in the RSNE. The target FTR can use the PMKR0Name to derive the PMKR1Name, and if the target FTR does not have the PMK-R1 identified by PMKR1Name, it may attempt to retrieve that key from the R0KH identified by R0KH-ID. See 13.2 (Key holders). The FTO includes a fresh SNonce as its contribution to the association instance identifier and to provide key separation of the derived PTK; it is selected randomly to serve as a challenge that demonstrates the liveness of the peer in the fourth message.

The second message is used by the target FTR to respond to the requesting FTO. The target FTR provides the key holder identifiers and key names used to generate the PTK. The target FTR also includes a fresh ANonce as its contribution to the association instance identifier and to provide key separation of the derived PTK. The response includes a status code.

In an RSN, the third message is used by the FTO to assert to the target FTR that it has a valid PTK. If no resources are required, then the FTO omits inclusion of the RIC.

The fourth message is used by the target FTR to respond to the requesting FTO. This message serves as final confirmation of the transition, establishes that the FTR possesses the PMK-R1 and is participating in this association instance, and protects against downgrade attacks. Note, however, that the RIC is absent if no resources were requested in the third message. This also includes a status code and may include a reassociation deadline.

* FT authentication sequence: contents of first message

If present, the RSNE shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR0Name.
* All other fields shall be as specified in 9.4.2.24 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).

The MDE shall contain the MDID field and the FT Capability and Policy field settings obtained from the target AP or any AP affiliated with the target AP MLD, as advertised by the target AP or any AP affiliated with the target AP MLD in Beacon and Probe Response frames. The MDID shall be identical to that obtained during the FT initial mobility domain association exchange.

If present, the FTE shall be set as follows:

* R0KH-ID shall be the value of R0KH-ID obtained by the FTO during its FT initial mobility domain association exchange.
* SNonce shall be set to a value chosen randomly by the FTO, see 12.7.5 (Nonce generation) for a recommended procedure.
* All other fields shall be set to 0.
* FT authentication sequence: contents of second message

If the status code is SUCCESS, then the following rules apply.

If present, the RSNE(s) shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall be set to the value contained in the first message of this sequence.
* All other fields shall be identical to the contents of the RSNE advertised by the AP or the AP affiliated with the AP MLD in Beacon and Probe Response frames.

The MDE shall contain the MDID and FT Capability and Policy fields. This element shall be the same as the MDE advertised by the target AP or any AP affiliated with the AP MLD in Beacon and Probe Response frames.

If present, the FTE shall be set as follows:

* R0KH-ID shall be identical to the R0KH-ID provided by the FTO in the first message.
* R1KH-ID shall be set to the R1KH-ID of the target FTR, from dot11FTR1KeyHolderID.
* ANonce shall be set to a value chosen randomly by the target FTR, see 12.7.5 (Nonce generation) for a recommended procedure.
* SNonce shall be set to the value contained in the first message of this sequence.
* All other fields shall be set to 0.
* FT authentication sequence: contents of third message

If present, the RSNE shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR1Name.
* All other fields shall be as specified in 9.4.2.24 (RSNE) and 12.6.3 (RSNA policy selection in an infrastructure BSS).

The MDE shall contain the MDID and FT Capability and Policy fields. This element shall be identical to the MDE contained in the first message of this sequence.

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).
* The RSNXE Used subfield of the MIC Control field shall be set to 1 if the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in the RSNXE; otherwise this subfield shall be set to 0.
* When the negotiated AKM is 00-0F-AC:3, 00-0F-AC:4, or 00-0F-AC:9, the MIC shall be calculated using the KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:13, the MIC shall be calculated using the KCK and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* When the negotiated AKM is 00-0F-AC:16, the MIC shall be calculated using the KCK2 and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:17, the MIC shall be calculated using the KCK2 and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* If dot11RSNAOperatingChannelValidationActivated is true and Authenticator indicates OCVC capability, the supplicant shall include FT OCI subelement in FTE.
* The MIC shall be calculated on the concatenation of the following data, in the order given here:
* FTO’s MAC address (6 octets)
* Target FTR’s MAC address (6 octets)
* Transaction sequence number (1 octet), which shall be set to the value 5 if this is a Reassociation Request frame and, otherwise, set to the value 3
* RSNE
* MDE
* FTE, with the MIC field of the FTE set to 0
* Contents of the RIC-Request (if present)
* RSNXE (if present)
* Non-AP STA MAC address corresponding to all the requested links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassocaition Request frame
* All other fields shall be set to 0.

If resources are being requested by the FTO, then a sequence of elements forming the RIC‑Request shall be included.

The RSNXE shall be present if an RSNXE was present in a Beacon or Probe Response frame that the FTO has received from the target FTR if the FTR is an AP or an AP affiliated with the target FTR if the FTR is an AP MLD and the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

* FT authentication sequence: contents of fourth message

If the status code is SUCCESS, then the following rules apply.

If present, the RSNE(s) shall be set as follows:

* Version field shall be set to 1.
* PMKID Count field shall be set to 1.
* PMKID List field shall contain the PMKR1Name
* All other fields shall be identical to the contents of the RSNE advertised by the target FTR if the FTR is an AP or the AP affiliated with the target FTR if the FTR is an AP MLD in Beacon and Probe Response frames.

The MDE shall contain the MDID and FT Capability and Policy fields. This element shall be identical to the MDE contained in the second message of this sequence.

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
* The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).The RSNXE Used subfield of the MIC Control field shall be set to 1 if the target AP or an AP affiliated with the target AP MLD includes an RSNXE in its Beacon and Probe Response frames; otherwise this subfield shall be set to 0.
* If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC capability, the Authenticator shall include FT OCI subelement in FTE.
* When this message of the authentication sequence appears in a Reassociation Response frame, the Optional Parameter(s) field in the FTE may include the GTK, IGTK and BIGTK subelements or MLO GTK, MLO IGTK, and MLO BIGTK subelements. If a GTK, an IGTK, a BIGTK, an MLO GTK, an MLO IGTK, or an MLO BIGTK are included, the Key field of the subelement shall be wrapped using KEK or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-10 (Integrity and key wrap algorithms) and 12.7.2 (EAPOL-Key frames). The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received message, the receiver shall ignore this trailing padding. Addition of padding does not change the value of the Key Length field. Note that the length of the encrypted Key field can be determined from the length of the GTK, IGTK, BIGTK, MLO GTK, MLO IGTK, or MLO BIGTK subelement.
* When the negotiated AKM is 00-0F-AC:3, 00-0F-AC:4, or 00-0F-AC:9, the MIC shall be calculated using the KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC algorithm shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:13, the MIC shall be calculated using the KCK and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* When the negotiated AKM is 00-0F-AC:16, the MIC shall be calculated using the KCK2 and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.
* When the negotiated AKM is 00-0F-AC:17, the MIC shall be calculated using the KCK2 and the HMAC-SHA-384 algorithm. The output of the HMAC-SHA-384 shall be truncated to 192 bits.
* The MIC shall be calculated on the concatenation of the following data, in the order given here:
* FTO’s MAC address (6 octets)
* Target FTR’s MAC address (6 octets)
* Transaction sequence number (1 octet), which shall be set to the value 6 if this is a Reassociation Response frame or, otherwise, set to the value 4
* RSNE if Basic variant Multi-Link element is not included in the Reassocaition Response frame
* RSNEs corresponding to all accepted links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassociation Response frameMDEFTE, with the MIC field of the FTE set to 0
* Contents of the RIC-Response (if present)
* RSNXE (if present) if Basic variant Multi-Link element is not included in the Reassocaition Response frame
* RSNXEs (if present) corresponding to all accepted links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassocaition Response frame
* AP MAC address corresponding to all the accepted links in increasing order of link ID if Basic variant Multi-Link element is included in the Reassocaition Response frame
* All other fields shall be set to 0.

If this message is other than a Reassociation Response frame and dot11RSNAActivated is false, a TIE may appear. If this message is other than a Reassociation Response frame, includes a RIC-Response, and dot11RSNAActivated is false, then a timeout interval shall appear. If it appears, it shall be set as follows:

* Timeout Interval Type field shall be set to 1 (reassociation deadline).
* Timeout Interval Value field shall be set to the reassociation deadline time.

If resources were requested by the FTO, then a RIC-Response shall be included.

The RSNXE shall be present if an RSNXE was present in the third message and the target FTR if the FTR is an AP or an AP affiliated with the target FTR if the FTR is an AP MLD set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element.

* FT security architecture state machines
* Introduction

*TGbe editor: Change the fifth paragraph as follows (track change on):*

The interactions between the R0KH and IEEE Std 802.1X, between the R1KH and IEEE Std 802.1X, and between the S1KH and IEEE Std 802.1X occur within the SME. At both the target FTR and at the FTO, the R1KH and S1KH initialize the IEEE 802.1X EAPOL state machines in the respective SMEs. The Controlled Port is opened without an EAP exchange when the reassociation completes.

* S1KH state machine
* S1KH state machine variables

*TGbe editor: Change the third bullet of the first paragraph as follows (track change on):*

The following list summarizes the variables used by the S1KH state machine:

* *Init.* This variable is set to true to initialize the S1KH state machine. In addition, this variable is used to restart the state machine when transitioning to a new FTR.