IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RSNXE interoperability issue | | | | |
| Date: 2020-02-19 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses an interoperability issue with the way RSNXE was added in P802.11-REVmd. This results in FT protocol failing to succeed between an IEEE Std 802.11-2016 based STA and an IEEE P802.11-REVmd/D3.0 based STA. A way to work around this in a backwards compatible manner is also proposed.

r1: fix additional issues with missing RSNXE edits in 13.4.2 and other editorial errors in that subclause

**Discussion**

IEEE P802.11-REVmd introduced a new element RSNXE to allow the RSNE to be extended in a manner that would be less likely to result in interoperability issues due to the design of the RSNE and known issues with deployed devices in parsing this. While this goal is addressed with the design of the RSNXE payload and not needing to modify the RSNE further, the way the RSNXE payload and presence is validated unfortunately results in another interoperability issue.

The RSNXE is added to frames similarly to the RSNE in cases where the transmitting STA has any of the capability bits in the RSNXE set to 1. This includes the cases of validating the RSNE in EAPOL-Key message 2/4 and 3/4 in the 4-way handshake, the FTE MIC calculation for FT protocol, and protection of (Re)Association Request/Response frames when FILS authentication is used. The way these extensions work in EAPOL-Key messages (STAs are expected to ignore unrecognized IEs/KDEs) and FILS authentication (STAs are expected to ignore unrecognized IEs in (Re)Association Request/Response frames) do not have an issue with a STA that is compliant with IEEE Std 802.11-2016. However, the way the FTE MIC calculation is extended is not compatible with IEEE Std 802.11-2016 STAs and this results in not being able to complete FT protocol successfully if one of the STAs (i.e., either the AP or the non-AP STA) is aware of RSNXE and the other one is not. One example of such interoperability issues has come up while testing FT with SAE H2E.

The FTE MIC is calculated on “concatenation of the following data” where the data is explicitly defined to be a set of IEs. The RSNXE was added to that list in P802.11-REVmd, but a STA based on IEEE Std 802.11-2016 would not know to include the RSNXE even if it were included in the Reassociation Request/Response frame. Consequently, the STAs based on different revisions of the standard would derive different MIC values and the reassociation would fail even though both STAs would be compliant with the particular standard revision they implement. Furthermore, the Element Count field of the MIC Control field in the FTE would have a potential interoperability issue if the receiving STA were to verify that it matches the number of protected IEs they consider to be included in the frame (and there is at least one such implementation; and even if this part would not cause a mismatch, the MIC failure will). It should also be noted that this issue with the FTE MIC design is not limited to RSNXE; any other addition of data to include in that calculation would likely result in similar interoperability issues.

It looks like there is no straightforward manner to fix this issue cleanly without opening a possibility of downgrade attack. The simplest approach of not including the RSNXE in the FTE MIC calculation in Reassociation Request frame if the AP did not include the RSNXE in Beacon or Probe Response frame and not including the RSNXE in the FTE MIC calculation in Reassociation Response frame if the RSNXE was not included in Reassociation Request frame would prevent the MIC mismatch issue, but this would result in losing protection for downgrade attacks (e.g., an attacker could send a modified Beacon frame to the non-AP STA to make that non-AP STA consider the RSNXE capabilities not being supported by the AP; this attack would not be detected as part of verifying the FTE MIC under these modified rules).

Luckily there are reserved bits in the FTE (see the Reserved field in Figure 9-357, MIC Control field). Those bits are included in the FTE MIC and as such, are protected as part of the FT protocol reassociation exchange. A STA that is compliant with IEEE Std 802.11-2016 is expected to ignore the actual value of those reserved bits while still including them in the MIC calculation. As such, one of those bits could be defined to indicate that the AP included RSNXE in Beacon and Probe Response frames even in the case where the straightforward changes described in the previous paragraph are used to not include the RSNXE in Reassociation Response frame. This would allow the non-AP STA to detect the downgrade attack (the RSNXE removed from Beacon/Probe Response frame). Similarly, the AP could use this to detect if an attacker has removed the RSNXE from Reassociation Request frame even in case the RSNXE itself could not be included in the FTE MIC calculation without both STAs having indicated support for RSNXE in unprotected frames before this reassociation.

In addition to addressing the new interoperability issue, the proposed changes cover couple of editorial fixes (“field” to “subfield” to be consistent with the FTE format definition) and various issues in 13.4.2. Furthermore, an explicit verification step for comparing the RSNE in FT protocol Reassocation Response frame against the RSNE in the Beacon/Probe Response frame is added to clarify protection against potential downgrade attacks (i.e., perform a similar check that is done during 4-way handshake EAPOL-Key msg 3/4 processing). This detail seemed to have been missing in the description of FT reassociation in an RSN (see 13.7.1), but this is implied in the description of the contents of the fourth message in the FT authentication sequence (see 13.8.5).

**Proposed Changes**

**9.3.3.7 Reassociation Request frame format**

*Change Table 9-38 (page 870 lines 11-13) as shown:*

**Table 9-38—Reassociation Request frame body**

|  |  |  |
| --- | --- | --- |
| 47 | RSN Extension | The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield and the rules for FT reassociation in Table 13-1 (FT authentication elements) do not omit the RSNXE from the third message. |

**9.3.3.8 Reassociation Response frame format**

*Change Table 9-39 (page 873 lines 53-55) as shown:*

**Table 9-39—Reassociation Response frame body**

|  |  |  |
| --- | --- | --- |
| 59 | RSN Extension | The RSNXE is present if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield and the rules for FT reassociation in Table 13-1 (FT authentication elements) do not omit the RSNXE from the fourth message. |

**9.4.2.47 Fast BSS Transition element (FTE)**

*Change 9.4.2.47 (page 1164 lines 6-15) as shown:*

The FTE includes information needed to perform the FT authentication sequence or FILS authentication during a fast BSS transition in an RSN. This element is shown in Figure 9-356 (FTE format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Element ID | Length | MIC Control | MIC | ANonce | SNonce | Optional Parameter(s) |
| Octets: | 1 | 1 | 2 | variable | 32 | 32 | Variable |

**Figure 9-356—FTE format**

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

The MIC Control field is 2 octets and is defined in Figure 9-357 (MIC Control field format).

|  |  |  |  |
| --- | --- | --- | --- |
|  | B0 | B1 B7 | B8 B15 |
|  | RSNXE Used | Reserved | Element Count |
| Bits: | 1 | 7 | 8 |

**Figure 9-357—MIC Control field format**

The RSNXE Used subfield of the MIC Control field indicates whether the STA transmitting the frame includes RSNXE in other frames.

The Element Count subfield of the MIC Control field contains the number of elements that are included in the message integrity code (MIC) calculation.

When the Element Count subfield has a value greater than 0, the MIC field contains a MIC that is calculated using the algorithm specified in 13.8.4 (FT authentication sequence: contents of third message) and 13.8.5 (FT authentication sequence: contents of fourth message). Otherwise, the MIC field is set to 0.

The length of the MIC field depends on the negotiated AKM selector and is specific in Table 12-10 (Integrity and key-wrap algorithms).

**13.4 FT initial mobility domain association**

**13.4.2 FT initial mobility domain association in an RSN**

*Change 13.4.2 as shown:*

A STA indicates its support for the FT procedures by including the MDE in the (Re)Association Request frame and indicates its support of security by including the RSNE. The AP responds by including the FTE, MDE, and RSNE in the (Re)Association Response frame. After a successful IEEE 802.1X authentication (if needed) or SAE authentication, the STA and AP perform an FT 4-way handshake. At the end of the sequence, the IEEE 802.1X Controlled Port is opened, and the FT key hierarchy has been established. The message flow is shown in Figure 13-2 (FT initial mobility domain association in an RSN).

A non-DMG STA initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the Open System authentication algorithm.

STA→AP: Authentication-Request (Open System authentication algorithm)

AP→STA: Authentication-Response (Open System authentication algorithm, Status)

A DMG STA initiates the FT initial mobility domain association procedures by performing an IEEE 802.11 authentication using the SAE algorithm.

STA→AP: Authentication-Request (SAE algorithm)

AP→STA: Authentication-Response (SAE algorithm, Status)

The SME of the STA initiates the authentication exchange, through the use of the MLME-AUTHENTICATE.request primitive, and the SME of the AP responds with MLME-AUTHENTICATE.response primitive. See 11.3.4 (Authentication and deauthentication).



**Figure 13-2—FT initial mobility domain association in an RSN**

*Change Figure 13-2 EAPOL-Key message texts (page 2726 lines 14-20) as shown:*

EAPOL-Key (0, 0, 1, 0, P, 0, 0, ANonce, 0, {})

EAPOL-Key (0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE[PMKR1Name], MDE, FTE, RSNXE})

EAPOL-Key (1, 1, 1, 1, P, 0, 0, ANonce, MIC, {RSNE[PMKR1Name], MDE, GTK[N],

IGTK[M], BIGTK[Q], FTE, TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE})

EAPOL-Key (1, 1, 0, 0, P, 0, 0, 0, MIC, {})

*Continue changing 13.4.2 as shown:*

Upon successful IEEE 802.11 Open System or SAE authentication, if using a suite type for which the Authentication type column indicates FT authentication (see Table 9-151 (AKM suite selectors)), the STA shall send a (Re)Association Request frame to the AP that includes the MDE. The contents of the MDE shall be the values advertised by the AP in its Beacon or Probe Response frames. Additionally, the STA includes its security capabilities in the RSNE.

STA→AP: (Re)Association Request (MDE, RSNE)

AP→STA: (Re)Association Response (MDE, FTE[R1KH-ID, R0KH-ID])

The SME of the STA initiates the (re)association through the use of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive. The SME of the AP responds to the indication with MLME-ASSOCIATE.response or MLME-REASSOCIATE.response primitive. See 11.3.5 (Association, reassociation, and disassociation).

If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_MDE. If an MDE is present in the (Re)Association Request frame 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 AP shall reject the (Re)Association Request frame with status code STATUS\_INVALID\_AKMP.

The (Re)Association Response frame from the AP shall contain an MDE, with contents as presented in Beacon and Probe Response frames. The FTE shall include the key holder identities of the AP, 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.

On successful (re)association, the S0KH on the STA and the R0KH on the AP then proceed with an IEEE 802.1X authentication using EAPOL frames carried in IEEE 802.11 Data frames if SAE authentication was not performed (i.e., if the suite type is not 00-0F-AC:9). The S0KH shall use the value of R0KH-ID as the endpoint identifier of the NAS Client (NAS-Identifier if RADIUS is used) in the exchange as defined in IETF RFC 3748 [B37].

If IEEE 802.1X authentication was performed, then upon successful completion of authentication, the R0KH receives the MSK and authorization attributes. If SAE authentication was performed, the R0KH receives the PMK, resulting in the successful completion of SAE. If a key hierarchy already exists for this STA 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 of the AP with which the STA is associated.

If the SME of the STA cannot authenticate the AS, then it shall disassociate with an MLME-DISASSOCIATE.request primitive. If the AS signals the Authenticator that the STA cannot be authenticated, then the SME of the AP shall disassociate with an MLME-DISASSOCIATE.request primitive.

If the MSK lifetime attribute is provided by the AS, the lifetime of the PMK-R0 shall not be more than the lifetime of the MSK. If the MSK lifetime attribute is not provided, the PMK-R0 lifetime shall be dot11FTR0KeyLifetime. For PSK, the PMK-R0 lifetime shall be dot11FTR0KeyLifetime. The lifetime of the PMK-R1s and PTK shall be the same as the lifetime of PMK-R0. When the key lifetime expires, each key holder shall delete its respective PMK-R0, PMK-R1, and PTK SAs.

The R1KH and S1KH then perform an FT 4-way handshake. The EAPOL-Key frame notation is defined in 12.7.4 (EAPOL-Key frame notation).

R1KH→S1KH: EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0, {})

S1KH→R1KH: EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE[PMKR1Name], MDE,

FTE,

RSNXE})

R1KH→S1KH: EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, {RSNE[PMKR1Name], MDE,

GTK[N], IGTK[M], BIGTK[Q], FTE,

TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE})

S1KH→R1KH: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {})

The message sequence is described in 12.7.6 (4-way handshake).

It is assumed by this standard that the reassociation deadline is administered consistently across the mobility domain. The mechanism for such consistent administration is outside the scope of this standard.

The PTK shall be calculated by the R1KH and S1KH according to the procedures given in 12.7.1.6.5 (PTK).

Upon completion of a successful FT 4-way handshake, the IEEE 802.1X Controlled Port shall be opened on both the non-AP STA and the AP. Subsequent EAPOL-Key frames shall use the key replay counter to detect replayed messages.

Upon completion of a successful FT 4-way handshake, the PTK lifetime timer is initiated. The operation of this timer prevents the PTKSA being used for longer than the value provided in the TIE[KeyLifetime] sent in message 3.

Once the PTKSA key lifetime expires, as indicated by the TIE[KeyLifetime], to continue its association in the mobility domain the STA shall perform the FT initial mobility domain association procedures. If the AP sends a Deauthentication or Disassociation frame to the STA with reason code INVALID\_AUTHENTICATION, then to continue its association in the mobility domain, the STA shall perform the FT initial mobility domain association procedures with any AP in the mobility domain. If the Supplicant EAPOL state machines are triggered to send an EAPOL-Start frame after a successful initial mobility domain association, the STA shall perform the FT initial mobility domain association procedures.

**13.7 FT reassociation**

**13.7.1 FT reassociation in an RSN**

*Change 13.7.1 as shown:*

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

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

FTO→Target AP: Reassociation Request(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request, RSNXE)

Target AP→FTO: Reassociation Response(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N], IGTK[M], BIGTK[Q]], RICResponse, RSNXE)

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

In the Reassociation Request frame, 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. 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 AP verifies the MIC in the FTE in the Reassociation Request frame and shall discard the request if the MIC is incorrect.

If the target AP includes 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 does not include the RSNXE, the R1KH of the target AP 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 AP do not match the contents advertised in the Beacon and Probe Response frames, the target AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_MDE. If the FTE in the Reassociation Request frame contains a different R0KH-ID, R1KH-ID, ANonce, or SNonce, the AP 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 AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_PMKID.

In the Reassociation Response frame, the SA field of the message header shall be set to the BSSID of the target AP, and the DA field of the message header shall be set to the MAC address of the FTO. 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 the RSNE fields other than the PMKID Count field and the PMKID List field in the Reassociation Response frame are not identical to the RSNE fields in the Beacon and Probe Response frames received from the target AP, 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 AP did not include the 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 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 reject 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 RICResponse 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 AP 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 AP 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 AP is distinct from the previous AP, the FTO shall enter State 1 with respect to the previous AP.

Upon a successful reassociation, the FTO shall delete any corresponding PTKSA with its previous AP. The SME of the FTO shall issue an MLME-DELETEKEYS.request primitive to delete the pairwise keys with the previous AP, and the FTO and the AP 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.

**13.8 FT authentication sequence**

**13.8.1 Overview**

*Change Table 13-1 (page 2746 lines 22-27) as shown:*

**Table 13-1—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 the RSNXE is present in a Beacon or Probe Response frame that the FTO has received from the target AP and the FTO set any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element to 1, and is present in the fourth message if the RSNXE was present in the third message and the target AP set any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element to 1. | 9.4.2.241 (RSN  Extension element  (RSNXE) |

**13.8.4 FT authentication sequence: contents of third message**

*Change 13.8.4 as shown:*

The RSNE shall be present only if dot11RSNAActivated is true. 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.

The FTE shall be present only if dot11RSNAActivated is true. 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 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 AP’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)

— 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 the RSNXE is present in a Beacon or Probe Response frame that the FTO has received from the target AP and the FTO set any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element to 1.

**13.8.5 FT authentication sequence: contents of fourth message**

*Change 13.8.5 as shown:*

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

The RSNE shall be present only if dot11RSNAActivated is true. 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 identical to the contents of the RSNE advertised by the target AP 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.

The FTE shall be present only if dot11RSNAActivated is true. 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 includes 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. If a GTK, an IGTK or a BIGTK are included, the Key field of the subelement shall be encrypted using KEK (when the negotiated AKM is 00-0F-AC:3, 00-0F-AC:4, 00-0F-AC:9, or 00-0F-AC:13) or KEK2 (when the negotiated AKM is 00-0F-AC:16 or 00-0F-AC:17) and the NIST AES key wrap algorithm. The Key field shall be padded before encrypting if the key length is less than 16 octets or if it is not a multiple of 8. 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 or 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 AP’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

— MDE

— FTE, with the MIC field of the FTE set to 0

— Contents of the RIC-Response (if present)

—RSNXE (if present)

— 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 the RSNXE was present in the third message and the target AP set any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in this element to 1.