|  |
| --- |
| CR for CIDs relevant to FT |
| Date: 2023-10-26 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Yan Li | ZTE Corporation |  |  | li.yan16@zte.com.cn |
| Jay Yang | ZTE Corporation |  |  |  |
| Yun Li | ZTE Corporation |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

**131,136,274**

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

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **CID** | **Comment** | **Proposed Change** | **Resolution** |
| 131 | IRM is currently only part of 4-way handshake. The MAC address used for next association should be possible to change also in Fast Transition. | Allow STA to use different MAC address in each Fast BSS Transition. Please add possibility to signal the next MAC address in the FT signalign. | Revised.Agree with the commenter in principle.As the FT key hierarchy is established by the fixed mac address of the non-AP STA，we have to consdier a method to guarantee both of AP and non-AP STA can use valid FT key in the case of random mac address.TGbh editor to make the changes under tag 131 in 1123-2050r0 |
| 136 | IRM is currently only part of 4-way handshake. The MAC address used for next association should be possible to change also in PASN setup. | Allow STA to use different MAC address in each Fast BSS Transition. Please add possibility to signal the next MAC address in the FT signaling. | Revised.The comment and proposed change indicate different cases. The PASN case has been resolved in D1.0.If the commenter want to propose the FT case, i agree with the comment in principle.As the FT key hierarchy is established by the fixed mac address of the non-AP STA，we have to consdier a method to guarantee both of AP and non-AP STA can use valid FT key in the case of random mac address.TGbh editor to make the changes under tag 131 in 1123-2050r0 |
| 274 | The draft supports changing the Device ID or IRM MAC address at Reassociation, but does not appear to support such change when using FT (which is the popular way to do Reassociation, now). | Consider a method to support ID/MAC Address changing with FT protocol | Revised.Agree with the commenter in principle.As the FT key hierarchy is established by the fixed mac address of the non-AP STA，we have to consdier a method to guarantee both of AP and non-AP STA can use valid FT key in the case of random mac address.TGbh editor to make the changes under tag 131 in 1123-2050r0 |

Discussion:

According to the 11-23/1852r1, the text for option 2(reuse the PMK-R1s) and the signalings for Device ID/IRM are provided in this document.



*（all of following modification under tag 131）*

13.4 FT initial mobility domain association

13.4.2 FT initial mobility domain association in an RSN

*modify the following text as shown*

The R1KH and S1KH then perform an FT 4-way handshake. The EAPOL-Key PDU notation is

defined in 12.7.4 (EAPOL-Key PDU 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], WIGTK[R], FTE, TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE} or {RSNE[PMKR1Name], MDE, GTK[N], IGTK[M], BIGTK[Q], WIGTK[R], FTE,TIE[ReassociationDeadline], TIE[KeyLifetime], RSNXE, Device ID KDE})

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

13.5 FT protocol

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

*modify the following text as shown*

FTO→Target AP: Authentication-Request (FTAA, 0, RSNE[PMKR0Name], MDE, FTE[SNonce, R0KH-ID], Device ID)

Target AP→FTO: Authentication-Response (FTAA, Status, RSNE[PMKR0Name], MDE, FTE[ANonce, SNonce, R1KH-ID, R0KH-ID])

......

In the Authentication-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’s BSS. The

elements in the frame, and their required contents, shall be as given in 13.8.2 (FT authentication sequence:

contents of first message).

13.5.3 Over-the-DS FT protocol in an RSN

*modify the following text as shown*

To perform an over-the-DS fast BSS transition to a target AP, the FTO and the target AP (through the current AP) shall perform the following exchange:

FTO→Target AP: FT Request (FTO address, TargetAP address, RSNE[PMKR0Name], MDE, FTE[SNonce, R0KH-ID], Device ID)

Target AP→FTO: FT Response (FTO address, TargetAP address, Status, RSNE[PMKR0Name], MDE, FTE[ANonce, SNonce, R1KH-ID, R0KH-ID])

......

The STA Address field of the FT Request frame shall be set to the MAC address of the FTO or, if dot11DeviceIDActivated or dot11IRMActivated is true, set to the FTO’s MAC address to be used for FT reassociation (see 13.7 FT reassociation), and the Target AP Address field of the FT Request frame shall be set to the BSSID of the target AP’s BSS. The elements in the FT Request frame, and their required contents, shall be as given in 13.8.2 (FT authentication sequence: contents of first message).

The STA Address field of the FT Response frame shall be set to the MAC address of the FTO or, if dot11DeviceIDActivated or dot11IRMActivated is true, set to the FTO’s MAC address to be used for FT reassociation (see 13.7 FT reassociation), and the Target AP Address field of the FT Response frame shall be set to the BSSID of the target AP’s BSS. The elements in the FT Response frame, and their required contents, shall be as given in 13.8.3 (FT authentication sequence: contents of second message). The Status Code field shall be a value from the options listed in 9.4.1.9 (Status Code field).

13.6 FT resource request protocol

13.6.3 Over-the-DS fast BSS transition with resource request

*modify the following text as shown*

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

Target AP→FTO: FT Ack (FTO, TargetAP, Status, RSNE[PMKR1Name], MDE, FTE[MIC,

ANonce, SNonce, R1KH-ID, R0KH-ID], TIE[ReassociationDeadline], RIC-Response)

The STA Address field of the FT Confirm frame shall be set to the MAC address of the FTO or, if dot11DeviceIDActivated or dot11IRMActivated is true, set to the FTO’s MAC address to be used for FT reassociation (see 13.7 FT reassociation), and the Target AP Address field of the FT Confirm frame shall be set to the BSSID of the target AP’s BSS. The elements in the FT Confirm frame, the element contents, and the MIC calculation shall be as given in 13.8.4 (FT authentication sequence: contents of third message). In a non-RSN, the FTE and RSNE shall not be present.

......

The STA Address field of the FT Ack frame shall be set to the MAC address of the FTO or, if dot11DeviceIDActivated or dot11IRMActivated is true, set to the FTO’s MAC address to be used for FT reassociation (see 13.7 FT reassociation), and the Target AP Address field of the FT Ack frame shall be set to the BSSID of the target AP’s BSS. The elements in the FT Ack frame, the element contents, and the MIC calculation shall be as given in 13.8.5 (FT authentication sequence: contents of fourth message). In a non-RSN, the FTE and RSNE shall not be present. The Status Code field value shall be a value from the options listed in 9.4.1.9 (Status Code field), and a TIE may appear.

13.7 FT reassociation

13.7.1 FT reassociation in an RSN

*modify the following text as shown*

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, IRM], 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], WIGTK[R], Device ID], RIC-Response, RSNXE)

13.8 FT authentication sequence

13.8.2 FT authentication sequence: contents of first message

*modify the following text as shown*

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.

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

— If dot11DeviceIDActivated is true, the FTO shall include Device ID element (see 9.4.2.307a Device ID element).

— All other fields shall be set to 0.

13.8.4 FT authentication sequence: contents of third message

*modify the following text as shown*

If present, the FTE shall be set as follows:

......

—When this message of the authentication sequence appears in a Reassociation Request frame, if dot11IRMActivated is true, the Optional Parameter(s) field in the FTE may include the IRM subelements. If an IRM is included, the Key field of the subelement shall be wrapped using PTK-KEK or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-11 (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 IRM subelement.

— All other fields shall be set to 0.

13.8.5 FT authentication sequence: contents of fourth message

*modify the following text as shown*

If present, the FTE shall be set as follows:

......

— 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, BIGTK, WIGTK, and, if dot11DeviceIDActivated is true, Device ID subelements. If a GTK, an IGTK, a BIGTK, WIGTK or a Device ID is included, the Key field of the subelement shall be wrapped using PTK-KEK or KEK2 and the appropriate key wrap algorithm, as specified in Table 12-11 (Integrity and key wrap algorithms(#3244)) 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, WIGTK, or Device ID subelement.

9.4.2.46 FTE

The fast BSS transition element (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 9-412 (FTE format).

.....

The Subelement ID field is defined in Table 9-219 (Subelement IDs):

*please insert the follow item into Table 9-219 in appropriate place.*

Table 9-219—Subelement IDs

|  |  |
| --- | --- |
| Value | Contents of Data field |
| ... | ... |
| 7 | WIGTK |
| <ANA> | Device ID |
| <ANA> | IRM |

*please add the following at the end of clause 9.4.2.46 FTE*

The Device ID subelement contains the device ID, used for identifying the FTO. The Device ID subelement format is shown in Figure xxx1(Device ID subelement format)

|  |  |  |  |
| --- | --- | --- | --- |
| Subelement ID | Length | Key Length |  Wrapped Key |

Octets: 1 1 1 variable

Figure xxx1 - Device ID subelement format

The Key Length field is the length of the Device ID in octets, not including any padding (see 13.8.5 (FT

authentication sequence: contents of fourth message)).

The Wrapped Key field contains the wrapped Device ID.

The IRM subelement contains the IRM, used for identifying the FTO. The IRM subelement format is shown in Figure xxx2(IRM subelement format)

|  |  |  |  |
| --- | --- | --- | --- |
| Subelement ID | Length | Key Length | Wrapped Key |

Octets: 1 1 1 6

Figure xxx2 - IRM subelement format

The Key Length field is the length of the IRM in octets, not including any padding (see 13.8.4 (FT

authentication sequence: contents of third message)).

The Wrapped Key field contains the wrapped IRM.

12.7.1.6 FT key hierarchy

12.7.1.6.4 PMK-R1

The second-level key in the FT key hierarchy, PMK-R1, is a key used to derive the PTK. The PMK-R1 is

derived using the KDF defined in 12.7.1.6.2 (Key derivation function (KDF)):

PMK-R1 = KDF-Hash-Length(PMK-R0, “FT-R1”, R1KH-ID || S1KH-ID)

where

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

Hash is the hash algorithm specific to the negotiated AKM (see Table 9-188 (AKM suite selectors))

Length is the length of the hash algorithm’s digest

PMK-R0 is the first level key in the FT key hierarchy

R1KH-ID is a MAC address of the holder of the PMK-R1 in the Authenticator of the AP

S1KH-ID is the SPA or, if dot11DeviceIDActivated or dot11IRMActivated is true, is the SPA used in the FT initial mobility domain association

The PMK-R1 is referenced and named as follows:

PMKR1Name = Truncate-128(Hash(“FT-R1N” || PMKR0Name || R1KH-ID || S1KH-ID))

where

Hash is the hash algorithm specific to the negotiated AKM (see Table 9-188 (AKM suite selectors))

“FT-R1N” is treated as an ASCII string

S1KH-ID is the SPA or, if dot11DeviceIDActivated or dot11IRMActivated is true, is the SPA used in the FT initial mobility domain association

PMKR1Name is used to identify the PMK-R1.

12. Security

12.2.11 Changing MAC Address

12.2.11.1 Device ID mechanism

*modify the following text as shown*

A non-AP STA shall provide a device ID when required by the procedures described below: :

1) When using PASN authentication, in the Device ID element in the first PASN frame.

2) When using FILS authentication, in the Device ID element in the (Re)Association Request frame.

3) When using FT protocol, in the Device ID element in the Authentication Request frame.

4) When not using PASN or FILS authentication, in the Device ID KDE in message 2 of the 4 way handshake.

An AP shall provide a device ID when required by the procedures described below:

1) When using PASN authentication, in the Device ID element in the second PASN frame.

2) When using FILS authentication, in the Device ID element in the (Re)Association Response frame.

3) When using FT protocol, in the Device ID subelement in the Optional Parameter(s) field of FTE in Reassociation respone frame.

4) When not using PASN or FILS authentication, in the Device ID KDE in message 3 of the 4 way handshake.

*add the following paragraph above the text (Figure 12-0a (Example of device ID exchange in PASN) shows an example of a device ID exchange in PASN...)*

When in FT protocol a non-AP STA sends an Authentication Request with an Device ID element, which is provided by the associated AP before, to the target AP, the target AP can identify the non-AP STA and map the Device ID to the original MAC address of the non-AP STA used in the FT initial mobility domain association.Then the R1KH of the target AP uses the value of PMKR0Name, the original MAC address of the non-AP STA and other information in the frame to calculate PMKR1Name. If the Device ID is not recognized or the calculated PMKR1Name does not match with any stored PMKR1Name, the target AP shall reject the authentication request with status code STATUS\_INVALID\_PMKID.

12.2.11.2 Identifiable Random MAC address (IRM) operation

*modify the following text as shown and add a new paragraph*

When associating to an AP that advertises support for IRM, the non-AP STA may allocate a new IRM MAC address to the AP by including an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication, including the IRM element in the Association Response frame. When using PASN, the non-AP STA may allocate a new IRM MAC address to the AP by including the IRM element in the third PASN frame.When using FT protocol in an RSN,the non-AP STA may provide a new IRM to the AP by including an IRM subelement in the Optional Parameter(s) field in FTE in Reassociation request frame.

When in FT protocol a non-AP STA sends an Authentication Request using an IRM as the TA to the target AP that was provided that address, the target AP can identify the non-AP STA and map the IRM to the original MAC address of the non-AP STA used in the FT initial mobility domain association.Then the R1KH of the target AP uses the value of PMKR0Name, the original MAC address of the non-AP STA and other information in the frame to calculate PMKR1Name. If the IRM is not recognized or the calculated PMKR1Name does not match with any stored PMKR1Name, the target AP shall reject the authentication request with status code STATUS\_INVALID\_PMKID.

The IRM Status field in the IRM KDE or IRM element is reserved when transmitted by the non-AP STA.