IEEE P802.11
Wireless LANs

|  |
| --- |
| 11be D3.0 CR for CID 18265 |
| Date: 2023-06-30 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

18265

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision for the message 3 that also mentions requested link

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 D3.0 Draft. This introduction is not part of the adopted mate

***Editing instructions formatted like this are intended to be copied into the TGbe D3.0 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** |
| 18265 | Yongho Seok | 35.3.6.2.2 | 512.48 | "At the TBTT indicated by the value of the AP Removal Timer subfield in transmitted Reconfiguration Multi-Link elements, an associated non-AP MLD shall consider the link corresponding to the removed AP nonexistent, and the SME of the affiliated non-AP STA associated with the removed affiliated AP shall delete any information maintained for that link."In the 4-way handshake, when rekeying is happened after the AP removal, the non-AP MLD still needs to carry the information of the removed link as specified in the following:"For MLO, when more than one link is requested, an MLO Link KDE for each affiliated STA link containing the affiliated STA MAC address included by the non-AP MLD in the Multi-Link element in the (Re)Association Request frame."To avoid this conflict, there are two options. The first option is that MLO Link KDE should contain the enablied link(s) instead of the request link indicated in the (Re)Association Request frame. Second option is that the non-AP MLD keeps the information of the removed link. But, in such a case, the gain of the ML reconfiguration is reduced. The preferred option is the first. | As in the comment. | Revised – We note that there are difference between initial 4-way and rekey operation. For initial 4-way, there is a need to verify the exact request, so the requested link(s) are verified. For rekey, it is indeed true that maintaining requested link after the initial 4-way is not realistic. We simply clarify the texts that during 4-way for rekey, only the information of the setup link is required. Further, since for rekeying the message can be exchanged in any link rather than same link like initial 4-way. We include information for all the setup link rather than changing content based on the link that is used for exchange. TGbe editor to make the changes shown in 11-23/1123r1 under all headings that include CID 18265 |

**Proposed Texts:**

*TGbe editor: Modify Clause 12.7.2 as follows (track change on): (#18265)*

* + 1. **EAPOL-Key frames**

***Change item g) of the eighth paragraph as follows:***

g) **RSC**. This field contains the current receive sequence counter (RSC) for the GTK being installed. It is used in message 3 of the 4-way handshake and message 1 of the group key handshake, where it is used to synchronize the IEEE 802.11 replay state. It may also be used in the Michael MIC Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure. It shall contain 0 in other messages. If the RSC is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the RSC is in the first octet of the RSC field. The RSC for TKIP is the TKIP sequence number (TSC); for CCMP and GCMP it is the packet number (PN); see Table 12-9 (Key RSC field).

For MLO, the RSC field is set to 0 in all messages.

***Insert the following new rows to*** [***Table 12-10 (KDE selectors)***](#_bookmark13) ***while maintaining the numerical order and updating the reserved range:***

**Table 12-10—KDE selectors**

|  |  |  |
| --- | --- | --- |
| **OUI** | **Data type** | **Meaning** |
| … | … | … |
| 00-0F-AC | 15 | WIGTK KDE |
| 00-0F-AC | 16 | MLO GTK KDE |
| 00-0F-AC | 17 | MLO IGTK KDE |
| 00-0F-AC | 18 | MLO BIGTK KDE |

**Table 12-10—KDE selectors**

|  |  |  |
| --- | --- | --- |
| **OUI** | **Data type** | **Meaning** |
| 00-0F-AC | 19 | MLO Link KDE |
| 00-0F-AC | ~~15~~20–255 | Reserved |

***Change the 28th paragraph as follows (not all items are shown):***

The following EAPOL-Key PDUs are used to implement the handshakes:

* **4-way handshake message 1** is an EAPOL-Key PDU with the Key Type subfield equal to 1. The fields and their values in the EAPOL-Key PDU are described in [12.7.2 (EAPOL-Key frames)](#_bookmark12). Use of the Key Data field to indicate a PMKID when a cached PMKSA is being used in this key derivation is defined in 12.6.8.3 (Cached PMKSAs and RSNA key management).
* **4-way handshake message 2** is an EAPOL-Key PDU with the Key Type subfield equal to 1.

An ESS Supplicant’s SME shall insert the RSNE it sent in its (Re)Association Request frame, and shall insert the RSNXE it sent in its (Re)Association Request frame if the RSNXE is present in the (Re)Association Request frame it sent. The RSNE and the RSNXE are included as transmitted in the Management frame. For MLO when more than one link is requested by the non-AP MLD in the (Re)Association Request frame, and the message 2 is used for the initial 4-way handshake, it shall include an MLO Link KDE containing the LinkID field and affiliated STA MAC address corresponding to each link included in the Basic Multi-Link element. For MLO, if the message 2 is used for the rekeying, it shall include an MLO Link KDE containing the LinkID field and affiliated STA MAC address corresponding to each setup link.

On receipt of message 2, the Authenticator’s SME shall validate the selected security configuration against the RSNE received in the (Re)Association Request frame, and shall validate the RSNXE included in message 2 against the RSNXE received in the (Re)Association Request frame from the Supplicant. An IBSS Supplicant’s SME shall insert an RSNE containing a selected pairwise cipher suite. The Authenticator’s SME shall validate that the pairwise cipher suite selected is one of its configured cipher suites and that the group cipher suite and AKM are consistent.

(…existing texts…)

*TGbe editor: Modify Clause 12.7.6.1 as follows (track change on): (#18265)*

* + 1. **4-way handshake**
			1. **General**

***Change the first paragraph as follows:***

RSNA defines a protocol using EAPOL-Key PDUs called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator  Supplicant: EAPOL-Key(0 or 1,0,1,0,P,0,0,ANonce,0,{} or

{PMKID} or {MAC Address})

Message 2: Supplicant  Authenticator: EAPOL-Key(0 or 1,1,0,0,P,0,0,SNonce,MIC,{RSNE} or

{RSNE, OCI KDE} or {RSNE, RSNXE} or {RSNE, OCI KDE, RSNXE} or {RSNE, MAC Address} or {RSNE, RSNXE, MAC Address} or {RSNE, OCI KDE, RSNXE,

MAC Address} or {RSNE, MAC Address, MLO Linkn} or {RSNE, RSNXE, MAC Address, MLO Linkn}or {RSNE, OCI KDE, RSNXE, MAC Address, MLO Linkn})

Message 3: AuthenticatorSupplicant: EAPOL-

Key(1,1,1,1,P,0,RSC,ANonce,MIC,{RSNE,GTK[N]} or {RSNE, GTK[N], OCI KDE} or {RSNE, GTK[N], RSNXE} or {RSNE, GTK[N], OCI KDE, RSNXE} or {MAC Address, MLO Linkm, MLO GTKn, MLO IGTKn, MLO BIGTKn} or {OCI KDE, MAC Address, MLO Linkm, MLO GTKn, MLO IGTKn, MLO BIGTKn})

Message 4: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{} or {MAC Address}).

***Change the third paragraph as follows:***

The following apply:

* EAPOL-Key() denotes an EAPOL-Key PDU conveying the specified argument list, using the notation introduced in [12.7.4 (EAPOL-Key PDU notation)](#_bookmark19).
* ANonce is a nonce that the Authenticator contributes for PTK generation. ANonce has the same value in message 1 and message 3.
* SNonce is a nonce from the Supplicant for PTK generation.
* P means the pairwise bit is set.
* The MIC is computed over the body of the EAPOL-Key PDU (with the Key MIC field first zeroed before the computation) using the PTK-KCK defined in 12.7.1.3 (Pairwise key hierarchy) for PTK generation.
* RSNE represents the appropriate RSNEs. For AP MLD, the RSNE is present in the MLO Link KDE.
* GTK[N] represents the GTK with its key OD.
* OCI KDE contains the current operating channel information for the operating channel in which the EAPOL-Key PDU is sent. OCI KDE is present when dot11RSNAOperatingChannelValidationActivated is true on the Supplicant in Message 2 and Authenticator in Message 3. Otherwise it is absent.
* RSNXE, when included in message 2, contains the RSNXE that the Supplicant sent in its (Re)Association Request frame, and when included in message 3, contains the RSNXE that the Authenticator sent in its Beacon or Probe Response frame. RSNXE is present in message 2 if this element is present in the (Re)Association Request frame that the Supplicant sent, and is present in message 3 if this element is present in the Beacon or Probe Response frame that the Authenticator sent. For AP MLD, the RSNXE is present in the MLO Link KDE.
* The Key Data descriptions specify what shall or may be included; nothing else shall be included except that one or more vendor specific KDEs and/or Vendor Specific elements may be included.
* For MLO, each message of the 4-way handshake contains (#16332)a MAC Address KDE containing the MLD MAC address of the Authenticator or Supplicant that is sending the message.
* For MLO, an MLO Link KDE is included for a STA affiliated with an MLD as follows. When more than one link is requested and included in message 2 for the initial 4-way handshake, an MLO Link KDE is included for each link and contains the LinkId field and corresponding affiliated STA MAC address received in the Basic Multi-Link element by the AP MLD in the (Re)Association Request frame. When included in message 2 for rekeying, an MLO Link KDE is included for each setup link and contains the LinkId field and corresponding affiliated STA MAC address. When included in message 3, an MLO Link KDE is included for each affiliated AP and contains the LinkId field, corresponding affiliated AP MAC address, RSNE, and RSNXE (if present) for each affiliated AP that was sent by the Authenticator.

NOTE 1— A non-AP MLD obtains the Link ID, AP MAC address, RSNE, and RSNXE (if present) for an AP affiliated with the AP MLD when it receives a Beacon or Probe Response frame from that AP or when it receives a multi-link probe response transmitted by another AP affiliated with the same AP MLD carrying a Basic Multi-Link element containing a complete profile of that AP (see 35.3.4 (Discovery of an AP MLD)).

* For MLO, if RSNA has not been established, each message of the 4-way handshake shall be sent on the same link used by the latest exchange of successful (Re)Association Request/Response frames.

*TGbe editor: Modify Clause 12.7.6.3 as follows (track change on): (#18265)*

* + - 1. **4-way handshake message 2**

***Change the first paragraph as follows:***

Message 2 uses the following values for each of the EAPOL-Key PDU fields: Descriptor Type **=** N – see [12.7.2 (EAPOL-Key frames)](#_bookmark12)

Key Information:

Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

Key Type = 1 (Pairwise) – same as message 1 Reserved = 0

Install = 0 Key Ack = 0

Key MIC Present = 0 when using an AEAD cipher or 1 otherwise

Secure = 0 in initial 4-way handshake, or 1 when PTK rekeying (but see [12.7.2 (EAPOL-Key](#_bookmark12) [frames)](#_bookmark12))

Error = 0 – same as message 1 Request = 0 – same as message 1

Encrypted Key Data = 1 when using an AEAD cipher or 0 otherwise Reserved = 0 – unused by this protocol version

Key Length = 0

Key Replay Counter = *n* – to let the Authenticator or initiator STA know to which message 1 this corresponds

Key Nonce = SNonce EAPOL-Key IV = 0 RSC = 0

Key MIC = MIC(PTK-KCK, EAPOL); or not present when using an AEAD cipher; Key Data Length = length of Key Data field in octets

Key Data =

* included RSNE – the sending STA’s RSNE for PTK generation or peer RSNE for the current operating band, and when this message 2 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated by the S1KH according to the procedures of 12.7.1.6.4 (PMK- R1) is included in the PMKID List field of the RSNE and the FTE and MDE are also included, or;
* The sending STA’s Multi-band element for PTK generation for a supported band other than the current operating band if dot11MultibandImplemented is true, or;
* The sending STA’s RSNE and Multi-band element(s) for generating a single PTK for all involved bands, if dot11MultibandImplemented is true and both the Authenticator and the Supplicant use the same MAC address in the current operating band and the other supported band(s); or;
* The sending STA’s RSNE and Multi-band element(s) for generating a different PTK for each involved band, if dot11MultibandImplemented is true and the Joint Multi-band RSNA subfield of the RSN capabilities field is 1 for both the Authenticator and the Supplicant, and either the Authenticator or the Supplicant uses different MAC addresses for different bands.
* Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Supplicant.
* The RSNXE that the Supplicant sent in its (Re)Association Request frame, if this element is present in the (Re)Association Request frame that the Supplicant sent.
* For MLO, a MAC Address KDE containing the MLD MAC address of the Supplicant.
* For MLO, when more than one link is requested and the message 2 is used for the initial 4-way handshake, an MLO Link KDE for each affiliated STA link containing the affiliated STA MAC address included by the non-AP MLD in the Multi-Link element in the (Re)Association Request frame. For MLO, when the message 2 is used for the rekeying, an MLO Link KDE for each affiliated STA of the setup link containing the affiliated STA MAC address

***Change the last paragraph as follows:***

Otherwise, the Authenticator:

* + - * 1. Derives PTK.
				2. Verifies the message 2 MIC or AEAD decryption operation result.

If the calculated MIC does not match the MIC that the Supplicant included in the EAPOL-Key PDU or the AEAD decryption operation returns failure, the Authenticator shall silently discard message 2.

If the MIC or AEAD decryption is valid and this message 2 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the Authenticator checks that all fields of the RSNE other than the PMKID List field and, if present, the RSNXE bitwise matches the fields from the (Re)Association Request frame and that the FTE and MDE are the same as those provided in the AP’s (Re)Association Response frame. If the MIC or AEAD decryption is valid and this message 2 is not part of a fast BSS transition initial mobility domain association and this message 2 is not part of an association started through the FT protocol, the Authenticator checks that the RSNE and, if present, the RSNXE bitwise matches that from the (Re)Association Request frame. For MLO, if the non- AP MLD includes requested link(s) in the Basic Multi-Link element in the (Re)Association Request frame and the message 2 is used for the initial 4-way handshake, validates that the affiliated STA MAC addresses are the same for each link included in the Multi-Link element in the (Re)Association Request frame.

For MLO, if the message 2 is used for rekeying, validates that the affiliated STA MAC addresses are the same for each setup link.

If these are not exactly the same, the Authenticator uses MLME-DEAUTHENTI- CATE.request primitive to terminate the association.

If they do match bitwise, the Authenticator constructs message 3.

* + - * 1. If management frame protection is being negotiated, the AP initializes the SA Query Transaction Identifier to an implementation-specific non-negative integer value, valid for the current pairwise security association.

*TGbe editor: Modify Clause 12.7.6.4 as follows (track change on): (#18265)*

* + - 1. **4-way handshake message 3**

(…existing texts…)

***Change the last paragraph as follows:***

The Supplicant shall also:

* + - * 1. Verify the RSNE and, if present, the RSNXE. If this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the Supplicant verifies that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and verifies that all other fields of the RSNE are identical to the fields in the RSNE present in the Beacon or Probe Response frames and verifies that the FTE and MDE are the same as in the (Re)Association Response frame. Otherwise, the Supplicant verifies that the RSNE is identical to that the STA received in the Beacon or Probe Response frame. If the RSNXE is present, the Supplicant verifies that the RSNXE is identical to that the STA received in the Beacon or Probe Response frame. If any of these verification steps indicates a mismatch, the STA shall disassociate or deauthenticate. If a second RSNE is provided in the message, the Supplicant uses the pairwise cipher suite specified in the second RSNE or deauthenticates.

a1) For MLO, verify the following:

* If the message 3 is used for the initial 4-way handshake, the affiliated AP MAC address and all fields in the RSNE, and the RSNXE (if present), for each requested link are identical to those received for the corresponding affiliated APs of the AP MLD.
* If the message 3 is used for the rekeying, the affiliated AP MAC address and all fields in the RSNE, and the RSNXE (if present), for each setup link are identical to those received for the corresponding affiliated APs of the AP MLD.
* The affiliated AP MAC address and all fields in the RSNE and the RSNXE (if present), of other discovered links, if information is available are identical to those received for the affiliated APs of the AP MLD.

NOTE 3—A non-AP MLD obtains the Link ID, AP MAC address, RSNE, and RSNXE (if present) for an AP affiliated with the AP MLD when it receives a Beacon or Probe Response frame from that AP or when it receives a multi-link probe response transmitted by another AP affiliated with the same AP MLD carrying a Basic Multi-Link element containing a complete profile of that AP (see 35.3.4 (Discovery of an AP MLD)).

If any of these verification steps indicates a mismatch, the supplicant shall disassociate or deauthen- ticate. If a second RSNE is provided for any link in the message, the supplicant shall dis- associate or deauthenticate.

* + - * 1. Verify the message 3 MIC or AEAD decryption operation result. If the calculated MIC does not match the MIC that the Authenticator included in the EAPOL-Key PDU or AEAD decryption operation returns failure, the Supplicant silently discards message 3.
				2. Update the last-seen value of the Key Replay Counter field.
				3. If the Extended Key ID for Individually Addressed Frames subfield of the RSN Capabilities field is 1 for both the Authenticator and Supplicant: Uses the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to receive individually addressed MPDUs protected by the PTK with the assigned Key ID.
				4. Construct message 4.
				5. Send message 4 to the Authenticator.
				6. Use the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to send and, if the receive key has not yet been installed, to receive individually addressed MPDUs protected by the PTK. The GTK is also configured by MLME-SETKEYS primitive. If WUR frame protection is negotiated, the WTK, and if applicable the WIGTK, is also configured by using the MLME- SETKEYS primitive.