IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 CR for editorial CIDs related to PGTK |
| Date: 2025-07-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Julien Sevin | Canon  |  |  | julien.sevin@crf.canon.fr |
| Stéphane Baron |  |  | stephane.baron@crf.canon.fr |
| Patrice Nezou |  |  | patrice.nezou@crf.canon.fr |

Abstract

This submission proposes resolutions for the following CIDs:

17, 39, 320, 367, 368, 398, 462, 463, 464, 489, 490,

642, 646, 654, 656, 658, 659, 662, 663, 767, 990

Revisions:

* R0. Initial version of the document
* R1. New resolution of CID #398 and #462

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 17 | 6.5.14.1.14 | "When the Key Type parameter is PGTK, the MAC installs the key such that the successive start times of the EDP Epochs are processed using that key." Don't like "such that". Replace with "and" | Replace cited sentence with "When the Key Type parameter is PGTK, the MAC installs the key and the successive start times of the EDP Epochs are processed using that key." | ACCEPTED |
| 398 | 6.5.14.1.4 | " the MAC installs the key such that the successive start times of the EDP Epochs are pro-cessed using that key" -- it is not clear what these are successive to, or how you process start times using a key |   | REVISED. Agree in principle with the commenter.TGBI Editor, please make the changes as shown in the latest version of 25/1078 and identified with tag #398.  |
| 462 | 9.4.2.46 | "all STAs of the EDP epoch" is not clear, since epochs are not STAs | As it says in the comment | REVISEDAgree in principle with the commenter.TGBI Editor, please make the changes as shown in the latest version of 25/1078 and identified with tag #462.  |
| 463 | 9.4.2.46 | "The PGTK Switch Time Indication field" -- no such field | Delete "Indication" | ACCEPTED |
| 39 | 9.4.2.46 | Missing parenthesis | Add ")" at end of sentence. | ACCEPTED |
| 464 | 9.4.2.46 | Missing closing paren | As it says in the comment | ACCEPTED |
| 489 | 9.6.13.20 | "The PGTK subelement contains" -- that's not the PGTK subelement | Change to "The WNM Sleep Mode PGTK subelement contains" | ACCEPTED |
| 490 | 9.6.13.20 | "The PGTK Switch Time Indication field is as defined in Figure 12-50i (PGTK KDE format)." -- the figure does not define the field, only its size | Refer to the subclause in which the field is defined | REVISEDAgree in principle with the commenter.TGBI Editor, please make the changes as shown in the latest version of 25/1078 and identified with tag #490.  |
| 367 | 11.2.3.15.2 | Missing word: "If EDP epoch is supported" | Change to:"If EDP epoch operation is supported" | REVISEDThe resolution of CID#685 (25/0554r5) has modified the sentence : “For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that set the Group EDP Epoch Supported field in the RSNXE to 1.”Instructions to the editor: no change needed.  |
| 642 | 11.2.3.15.3 | "by both AP MLD and non-AP MLD" missing articles | As it says in the comment | REVISED according to the CID#685 (25/0554r5). TGBI Editor, please make the changes as shown in the latest version of 25/1078 and identified with tag #642.  |
| 646 | 11.3.5.3 | Numbering of this and similar subbullets below is wrong | As it says in the comment | REJECTED. The numbering of sub bullets is right. |
| 654 | 12.6.16 | "PGTKSA (s)" spurious space | As it says in the comment | ACCEPTED |
| 656 | 12.6.19 | "updates PGTK" missing article | As it says in the comment | ACCEPTED |
| 658 | 12.7.2 | "The 8 octet PGTK Switch Time Indication" -- size is already shown in figure, but "field" is missing | Delete "8 octet" and append " field" | ACCEPTED |
| 659 | 12.7.2 | "contained in the PGTK field" -- this is specified in the next para | Delete the cited text | ACCEPTED |
| 662 | 12.7.7.2 | "PGTK, PGTK Switch Time Indication" should be just "PGTK and its switch time" | As it says in the comment | ACCEPTED |
| 663 | 12.7.7.2 | "the time indicating by the PGTK Switch Time Indication" should be ujst "at the switch time" | As it says in the comment | ACCEPTED |
| 320 | 13.2.2 | Close bullet points with "." | add "." at end of the sentence | REVISEDThe resolution of CID#685 (25/0554r5) has modified the sentence : “For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that set the Group EDP Epoch Supported field in the RSNXE to 1.”Instructions to the editor: no change needed.  |
| 767 | 13.2.2 | A period is missing at the end of this sentence. | Please add a period at the end of this sentence. | REVISEDThe resolution of CID#685 (25/0554r5) has modified the sentence : “For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that set the Group EDP Epoch Supported field in the RSNXE to 1.”Instructions to the editor: no change needed.  |
| 368 | 13.2.2 | Missing word: "if EDP epoch is supported" | Change to:"if EDP epoch operation is supported" | REVISEDThe resolution of CID#685 (25/0554r5) has modified the sentence : “For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that set the Group EDP Epoch Supported field in the RSNXE to 1.”Instructions to the editor: no change needed.  |
| 990 | 3.2 | The term "fields" is a bit ambiguous here. | Replace "fields" with "...fields common to the non access point (non-AP MLDs) associated to a AP MLD with BSS privacy enhancements enabled ." | REVISEDAgree in principle with the commenter.TGBI Editor, please make the changes as shown in the latest version of 25/1078 and identified with tag #990.  |

* **Definitions, acronyms, and abbreviations**
* **Definitions specific to IEEE 802.11**

**privacy group temporal key (PGTK):** [PGTK] A random value, assigned by an access point (AP) multi-link device (MLD) with privacy enhancements enabled, shared to all non-access point (non-AP) multi-link devices (MLDs) associated to the AP MLD, for frame anonymization purpose (#990) .

* **Effect of receipt**

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

When the Key Type is Group, IGTK, BIGTK, ~~or~~ WIGTK, or PGTK and the key matches the GTK, IGTK, BIGTK, or WIGTK, or PGTK, if any, installed as a result of EAPOL-Key PDUs (see 12.7.7.4 (Group key handshake implementation considerations)) or exiting WNM sleep mode (see 11.2.3.15.1 (WNM sleep mode capability)) receipt of this primitive shall have no effect except updating the RSC(s) when they are greater than those currently stored. Otherwise, irrespective of the Key Type parameter, when the Key parameter is the same as a key installed as a result of EAPOL-Key PDUs or exiting WNM sleep mode, receipt of this primitive shall have no effect. Otherwise, receipt of this primitive causes the MAC to apply the keys as follows, subject to the MLME-SETPROTECTION.request primitive:

* The MAC uses the key and key ID for the transmission of subsequent frames to which the key and key ID apply (as defined by the Key Type and Address parameters).
* When the Key Type parameter is not PGTK, t~~T~~he MAC installs the key with the associated key ID such that received frames for that cipher, of the appropriate type, and containing the matching key ID are processed using that key and its associated state information. When the Key Type parameter is PGTK, the MAC installs the key, and (#17) the start times of an EDP epoch sequence (#398) are processed using that key.
* When the Key Type parameter is Pairwise or PeerKey, and the Key, Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize the transmitter TSC/PN counter and the receiver replay counter(s) to 0. When the Key Type parameter is not Pairwise, PeerKey, ~~or~~ BIGTK, or PGTK, and the Key, Key ID, and Address (where valid) parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the traffic, the transmitter TSC/PN/IPN/WIPN counter to 0 or 1 (see Clause 12 (Security) and Clause 29 (Wake-Up Radio (WUR) MAC specification(11ba))) or the receiver replay counter(s) to the value in the Receive Sequence Count parameter. When the Key Type parameter is BIGTK, and the Key and Key ID parameters identify a new key to be set, the MAC shall initialize, depending on the direction of the traffic, the transmitter BIPN counter as specified in 12.5.3.4 (BIP replay counters and packet numbers) or the receiver replay counter to the value in the Receive Sequence Count parameter. When the Key Type, Key, Key ID, and Address (where valid) parameters identify an existing key, the MAC shall not change the transmitter TSC/PN/IPN/BIPN/WIPN counter or the receiver replay counter(s) associated with that key.

9.4.2.46 **FTE**

The PGTK subelement contains the PGTK, used to anonymize fields that are common for all STAs assigned to an EDP group (#462). The PGTK subelement format is shown in Figure 9-442d (PGTK subelement format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | PGTK Switch Time | Key Length  | Wrapped Key |
| Octets: | 1 | 1 | 8 | 1 | variable(#Ed related to #915) |
| * **PGTK subelement format**
 |

The PGTK Switch Time (#463) field is as defined in Figure 12-50i (PGTK KDE format).

The Key Length field is the length of the PGTK in octets, not including any padding (see 13.8.5 (FT authentication sequence: contents of fourth message)) (#39,#464) .

The Wrapped Key field contains the wrapped PGTK being distributed if the frame contains the FTE is not encrypted and contains the PGTK being distributed if the frame contains the FTE is encrypted.(#Ed related to #915)

* **WNM Sleep Mode Response frame format**

***Change the sixth paragraph as follows:***

* ***revme D7.0 up to Figure 9-1290, 11be D7.0 up to Figure 9-1290c***

The Key Data field contains zero or more subelements that provide the current GTK, IGTK, BIGTK to the STA and the current PGTK to the non-AP MLD. The format of these subelements is shown in Figure 9-1288 (WNM Sleep Mode GTK subelement format), Figure 9-1289 (WNM Sleep Mode IGTK subelement format), Figure 9-1290 (WNM Sleep Mode BIGTK subelement format), Figure 9-1290a (WNM Sleep Mode MLO GTK subelement format), Figure 9-1290b (WNM Sleep Mode MLO IGTK subelement format), and Figure 9-1290c (WNM Sleep Mode MLO BIGTK subelement format), and Figure 9-1290d (WNM Sleep Mode PGTK subelement format). The subelement IDs for these subelements are defined in Table 9- 540 (Optional subelement IDs for WNM Sleep Mode parameters). When management frame protection is not used, the Key Data field is not present.

***change Table 9-540 as follows:***

* **Optional subelement IDs for WNM Sleep Mode parameters**

|  |  |
| --- | --- |
| **Value** | **Meaning** |
| ... |  |
| 5 | MLO BIGTK |
| 6 | PGTK |
| ~~6~~7-255 | Reserved |

***Insert the following at the end of this subclause:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Subelement ID | Length | PGTK Switch Time Indication | Key |
| Octets: | 1 | 1 | 8 | 16 |

* **WNM Sleep Mode PGTK subelement format**

The WNM Sleep Mode (#489) PGTK subelement contains the PGTK of the EDP AP MLD as shown in Figure 9-1290d (WNM Sleep Mode PGTK subelement format).

The Subelement ID field is defined in 9.6.13.20 (WNM Sleep Mode Response frame format).

The Length field is defined in 9.4.3 (Subelements).

The PGTK Switch Time Indication field is defined in 12.7.2 EAPOL-Key frames (#490).

 The Key field is the PGTK being distributed.

* **MLME**
* **Power management**
* **Power management in a non-DMG infrastructure network**
* **General**
* **WNM sleep mode non-AP STA operation**

***Change the fifth paragraph as follows:***

The receipt of an MLME-SLEEPMODE.confirm primitive with a valid SleepMode parameter indicates to the STA's SME that the AP has processed the corresponding WNM Sleep Mode Request frame. The content of the WNM sleep mode parameter in the WNM Sleep Mode Response frame provides the status of WNM Sleep Mode elements processed by the AP. The non-AP STA shall delete the GTKSA if the response indicates success. If RSN is used with management frame protection, the non-AP STA shall delete the IGTKSA if the response indicates success, If RSN is used with beacon frame protection, the non-AP STA shall delete the BIGTKSA if the response indicates success. If the Group EDP Epoch Supported field in the RSNXE is set to 1 by both the APs affiliated with the AP MLD and the non-AP MLD, the non-AP MLD shall delete the PGTKSA if the response indicates success.(#685)

* **WNM sleep mode AP operation**

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

For MLO, with RSN and a valid PTK is configured for the non-AP MLD:

* If management frame protection is negotiated for the MLDs, the current GTK, IGTK when management frame protection is negotiated, and BIGTK when beacon protection is negotiated for each setup link shall be included in the WNM Sleep Mode Response frame using the WNM Sleep Mode MLO GTK/IGTK/BIGTK subelement (see 9.6.13.20 (WNM Sleep Mode Response frame format)). If a GTK/IGTK/BIGTK update is in progress for one or more links, the pending GTK, IGTK when management frame protection is negotiated, and BIGTK when beacon protection is negotiated for each of the affected AP(s) shall be included in the WNM Sleep Mode Response frame using the WNM Sleep Mode MLO GTK/IGTK/BIGTK subelement (see 9.6.13.20 (WNM Sleep Mode Response frame format)). A non-AP MLD identifies the corresponding link to which the GTK/IGTK/BIGTK belongs based on the value of the Link ID subfield included in the subelement of the Key Data field.
* If management frame protection is not negotiated for the MLDs, the current GTK for each setup link shall be sent to the non-AP MLD using a group key handshake (see 12.7.7 (Group key handshake)) immediately following the WNM Sleep Mode Response frame. If a GTK update is in progress for a setup link, the pending GTK for the setup link shall be sent to the STA using another group key handshake immediately after the current GTK of the setup link has been sent.
* If the Group EDP Epoch Supported field in the RSNXE is set to 1 by both the APs affiliated with the AP MLD and the non-AP MLD (#642), the current PGTK shall be included in the WNM Sleep Mode Response frame. If a PGTK update is in progress, the pending PGTK shall be included in the WNM Sleep Mode Response frame.
* **AP, AP MLD or PCP association receipt procedures**

***Change the first paragraph as follows (not all lines shown):***

The following procedure shall be used by an AP or PCP upon receipt of an Association Request frame from a STA or by an AP MLD after an AP affiliated with the AP MLD receives an Association Request frame with Basic Multi-Link element from a non-AP STA affiliated with a non-AP MLD:

* If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA, and TPKSA (including temporal keys) held for communication with the STA or non-AP MLD by using the MLME-DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)).
* **RSNA establishment**

***Change the first bullet, the second bullet, the fifth bullet, and add a new bullet of the first paragraph as follows (not all lines are shown):***

An SME establishes an RSNA in one of seven ways:

* If an RSNA uses authentication negotiated over IEEE Std 802.1X or FILS authentication in an infrastructure BSS, an SME establishes an RSNA as follows:
* It identifies the AP as an RSNA AP from the AP’s Beacon, DMG Beacon, Announce, Information Response, FILS Discovery, or Probe Response frames.
* It shall invoke Open System, IEEE 802.1X authentication, or FILS authentication if the STA is a non-DMG STA.
* It negotiates cipher suites during the association process, as described in 12.6.2 (RSNA selection) and 12.6.3 (RSNA policy selection in an infrastructure BSS).
* It uses IEEE Std 802.1X-2020 to authenticate if IEEE 802.1X authentication is not performed before association, as described in 12.6.8 (RSNA establishment in an infrastructure BSS) and 12.6.9 (RSNA authentication in an IBSS), FT protocol to authenticate as described in 13.5 (FT protocol) or uses FILS authentication to authenticate as described in 12.11 (Authentication for FILS).
* If EDP epoch operation is supported by both the AP MLD and the non-AP MLD, the SME programs the PGTK into the MAC for anonymization of individually addressed frames.
* If an RSNA is based on a PSK or password in an infrastructure BSS, an SME establishes an RSNA as follows:
* If EDP epoch operation is supported by both the AP MLD and the non-AP MLD, the SME programs the PGTK into the MAC for anonymization of individually addressed frames.
* If an RSNA allows for confidentiality only (no authentication) in an infrastructure BSS, an SME establishes an RSNA as follows:
* If EDP epoch operation is supported by both the AP MLD and the non-AP MLD, the SME programs the PGTK into the MAC for anonymization of individually addressed frames.
* If an RSNA uses PASN authentication, an RSNA capable the STA establishes an RSNA as described in 12.13 (Preassociation security negotiation(11az)).
* If an RSNA uses EDPKE authentication, an RSNA capable STA establishes an RSNA as described in 12.16.9 (Enhanced Data Privacy Key Exchange).
* **RSNA security association termination**

***Change the second paragraph as follows:***

it deletes some security associations. In the case of an ESS, the non-AP STA's SME shall delete any PTKSA(s), GTKSA(s), IGTKSA(s), BIGTKSA(s), WIGTKSA(s), WTKSA(s), TPKSA(s), the non-AP MLD's SME shall delete any PGTKSA(s) (#654) and the AP's SME shall delete the PTKSA. In the case of an IBSS, the SME shall delete the PTKSA(s) and the GTKSA(s) and any IGTKSA(s). Once the security associations have been deleted, the SME then invokes the MLME-DELETEKEYS.request primitive to delete all temporal keys associated with the deleted security associations.

* **RSNA rekeying**

***Change the fifth paragraph as follows:***

For MLO, the AP MLD's Authenticator manages packet number assignment for the PTKSA with a non-AP MLD. For a given link, the affiliated AP's Authenticator manages packet number assignment for the IGTKSA, GTKSA, or BIGTKSA. If an IGTKSA, GTKSA, or BIGTKSA update is triggered, the affiliated AP updates group keys for the given link through a group key handshake between the AP MLD and non-AP MLD. If a PGTKSA update is triggered, the AP MLD updates the (#656) PGTK through a group key handshake between the AP MLD and non-AP MLD.

* **EAPOL-Key frames**

***Modify Table 12-10 (KDE selectors) (not all lines shown) as follows:***

* **KDE selectors**

|  |  |  |
| --- | --- | --- |
| **OUI** | **Data type** | **Meaning** |
| 00-0F-AC | 23 | PGTK KDE |

***Insert the following at the end of 12.7.2 (EAPOL-Key frames):***

* ***Revme D7.0 up to Figure 12-50, 11be D7.0 up to Figure 12-50h***

The format of the PGTK KDE is shown in Figure 12-50i (PGTK KDE format).

|  |  |  |
| --- | --- | --- |
|  | PGTK Switch Time Indication | PGTK |
| Octets: | 8 | 32 |
| * **PGTK KDE format**
 |

The PGTK Switch Time Indication field indicates the time at which the PGTK indicated in the Key field shall be applied to replace the PGTK in use by the EDP AP MLD and EDP non-AP MLDs. The PGTK Switch Time Indication field (#658) is set to the time at which the PGTK (#659) shall be applied by the EDP AP MLD and the EDP non-AP MLDs using, as a time-base, the value of the TSF corresponding to the BSS identified by the BSSID of the frame containing the PGTK KDE.

The PGTK field contains the PGTK.

* **Group key handshake message 1**

***Change the first paragraph by inserting a sub-bullet at the end of Key Data as follows (not all lines shown):***

Message 1 uses the following values for each of the EAPOL-Key PDU fields:

Key Data =

* For MLO, when present, PGTK and its switch time (#662) (see 12.7.2 (EAPOL-Key frames))

***Change the third paragraph as follows (not all lines shown):***

On reception of message 1, the Supplicant:

* When the Supplicant is not an MLD, uses the MLME-SETKEYS.request primitive to configure the GTK and, the IGTK when present, and the BIGTK if beacon protection is enabled at the non-AP STA, and the WIGTK if WUR frame protection is negotiated, into the MAC. When the Supplicant is a non-AP MLD, uses the MLME-SETKEYS.request primitive to configure the GTK(s) when present and, the IGTK(s) when present, and the BIGTK(s) when present for the indicated link(s) into the MAC of the affiliated non-AP STA(s) operating on the indicated link(s). When the Supplicant is a non-AP MLD, uses the MLME-SETKEYS.request primitive to configure the PGTK when present, into the MAC at the switch time . (#663)
* **Fast BSS transition**
* **Key holders**
* **Authenticator key holders**

***Change the seventh paragraph as follows***

The R1KH shall meet the following requirements:

* The R1KH-ID shall be set to a MAC address of the physical entity that stores the PMK-R1 and uses it to generate the PTK. That same MAC address shall be used to advertise the PMK-R1 identity to the STA or non-AP MLD and the R0KH.
* For non-MLO, the R1KH shall derive and distribute the GTK and IGTK to all connected STAs. For MLO, the R1KH shall distribute the GTKs and IGTKs for setup links to all connected non-AP MLDs.
* If WUR frame protection is enabled, the R1KH shall derive and distribute the IWGTK and WIPN to all WUR non-AP STAs with which the R1KH has negotiated WUR frame protection.
* For non-MLO, if beacon protection is enabled, the R1KH shall derive and distribute the BIGTK and BIPN to all connected STAs. For MLO, the R1KH shall derive and distribute the BIGTKs and BIPNs for setup links to all connected non-AP MLDs.
* For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated

with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that set the

Group EDP Epoch Supported field in the RSNXE to 1.(#685)

* When the PMK-R1 lifetime expires, the R1KH shall delete the PMK-R1 PMKSA and shall revoke all PTKSAs derived from the PMK-R1 using the MLME-DELETEKEYS primitive.
* The R1KH shall not expose the PMK-R1 to other parties.
* **Fast BSS transition**
* **Key holders**
* **Authenticator key holders**

***Change the seventh paragraph as follows***

The R1KH shall meet the following requirements:

* The R1KH-ID shall be set to a MAC address of the physical entity that stores the PMK-R1 and uses it to generate the PTK. That same MAC address shall be used to advertise the PMK-R1 identity to the STA or non-AP MLD and the R0KH.
* For non-MLO, the R1KH shall derive and distribute the GTK and IGTK to all connected STAs. For MLO, the R1KH shall distribute the GTKs and IGTKs for setup links to all connected non-AP MLDs.
* If WUR frame protection is enabled, the R1KH shall derive and distribute the IWGTK and WIPN to all WUR non-AP STAs with which the R1KH has negotiated WUR frame protection.
* For non-MLO, if beacon protection is enabled, the R1KH shall derive and distribute the BIGTK and BIPN to all connected STAs. For MLO, the R1KH shall derive and distribute the BIGTKs and BIPNs for setup links to all connected non-AP MLDs.
* For MLO, if the Group EDP Epoch Supported field in the RSNXE is set to 1 by the APs affiliated with the AP MLD, the R1KH shall derive and distribute the PGTK to the non-AP MLDs that set the Group EDP Epoch Supported field in the RSNXE to 1.(#685)
* When the PMK-R1 lifetime expires, the R1KH shall delete the PMK-R1 PMKSA and shall revoke all PTKSAs derived from the PMK-R1 using the MLME-DELETEKEYS primitive.
* The R1KH shall not expose the PMK-R1 to other parties.