IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D1.0 CR for technical 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:

185, 260, 396, 397, 643, 645, 657, 660, 661, 733, 1008

Revisions:

R0. Initial version of the document

Revisions:

* R0. Initial version of the document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 185 | 6.5.14.1.2 | The PGTK should have Key ID that enables the AP to change the key. This is needed especially for BPE AP MLDs that operate only a single epoch. | Please assign at least 2 Key IDs for the PGTK and describe how the PGTK can be changed while AP MLD has associated STAs. | REJECTEDThe Key ID is used to identify which key to be used when rekey (between the current and new). It is not necessary for PGTK because a PGTK Switch Time Indication has been introduced indicating the time at which the delivered PGTK shall be applied by the EDP AP MLD and the EDP non-AP MLDs. |
| 396 | 6.5.14.1.2 | The key ID for PGTK is not specified | The pattern suggests it should be 10-11 for PGTK (also in 6.5.15.1.3) | REJECTEDThe Key ID is used to identify which key to be used when rekey (between the current and new). It is not necessary for PGTK because a PGTK Switch Time Indication because it has been introduced indicating the time at which the delivered PGTK shall be applied by the EDP AP MLD and the EDP non-AP MLDs. |
| 397 | 6.5.14.1.2 | If the PGTK is a group-like key an RSC is needed (though hm the last bullet of 6.5.14.1.4 does not cover PGTKs so not sure now) | Change ", or WIGTK" to ", WIGTK, or PGTK" | REJECTEDNo Packet Number (so no RSC) is needed for PGTK  |
| 1008 | 9.6.13.20 | 16 Octets are allocated for the "Key" field. Should this subelement support larger key sizes? | If larger key sizes should be supported, then update the number of octets for the "Key" field to support those sizes. | REJECTEDA fixed length of PGTK allows not to use a length field in the format of the WNM Sleep Mode PGTK subelement and the relevance of using larger key size for privacy purpose (and not security purposes) is not really identified. For reminder, it is used as input parameter of a KDF-Hash-Length to generate random EDP Epoch Start Times and random offsets for BPE frame anonymization parameter sets)  |
| 260 | 11.2.3.15.2 | PGTKSA deletion in the WNM Sleep mode may require the STA to reassociate with the AP, because a CPE STA cannot know the excat epoch start time and a BPE STA cannot know the AP BSSID. The spec should define how a non-AP STA wakes up from the WNM Sleep mode without reassocaition. | Please clarify how a WNM STA wakes up from the sleep if it has deleted the PGTK. If this is not possible, please add a note to instruct that reassociation is required. | REJECTEDThe start time could be computed from the (current/new) PGTK contained in the WNM Sleep Mode PGTK subelement of the WNM Sleep Mode Response frame and the EDP Epoch setting negotiated before entering in sleep mode (always valid). If the BPE AP has changed its BSSID when the BPE non-AP STA was in sleep mode, it will ignore the WNM-Sleep Request from the non-AP STA indicating that the non-AP STA is exiting sleep mode. So no specific process is required. |
| 643 | 11.2.3.15.3 | "If EDP epoch operation is supported by both AP MLD and non-AP MLD, 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." means that if a PGTK update is in process, both the current and the pending PGTK are included. I suspect that's not the intent | As it says in the comment | REVISED. Agree in principle with the commenter. The WNM Sleep Mode Response frame can’t contain both the current key and the pending key.TGBI Editor, please make the changes as shown in the latest version of 25/1079 and identified with tag #643.  |
| 645 | 11.3.5.3 | "the SME pro-grams the PGTK into the MAC for anonymization of individually addressed frames. " -- I struggled to find a clear statement of what the PGTK is used for, but isn't it also used for group frames? I note it is updated in the group key handshake | As it says in the comment | REVISEDAgree in principle with the commenter. It is no aligned with the PGTK usage specified in the definition of the PGTK : privacy group temporal key is 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. TGBI Editor, please make the changes as shown in the latest version of 25/1079 and identified with tag #645.  |
| 657 | 12.7.1.1 | "fields that are common for all STAsof the EDP epoch" -- fields and STAs can't be compared | As it says in the comment | REVISED. Agree in principle with the commenter. To be aligned with the definition of the PGTK, “frame anonymization” is added and “anonymize fields that are common for all STAs of the EDP epoch” is deleted. TGBI Editor, please make the changes as shown in the latest version of 25/1079 and identified with tag #657.  |
| 660 | 12.7.4 | "is the PGTK KDE" -- it's the PGTK, as provided by the PGTK KDE, together with the start time | Match the baseline formulation | REVISED. Agree in principle with the commenter. The PGTK Switch Time Indication has been included.TGBI Editor, please make the changes as shown in the latest version of 25/1079 and identified with tag #660.  |
| 661 | 12.7.7.1 | "PGTK Switch Time (ST)" should be just "switch time" | As it says in the comment | ACCEPTED |
| 733 | 13.2.2 | "-- For MLO, if EDP epoch is supported by both the AP MLD and the non-AP MLDs, the R1KH shallderive and distribute the PGTK to all connected non-AP MLDs" -- not clear what happens if some but not all non-AP MLDs support | Change to "-- For MLO, if <EDP epoch> is supported by both the AP MLD and at least one non-AP MLD, the R1KH shall derive and distribute the PGTK to all connected non-AP MLDs that support <EDP epoch>"" | REVISEDThe resolution of CID#685 (25/0554r5) has already clarified 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.  |

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

***Editing instructions formatted like this are intended to be copied*** ***into the TGbi D1.0 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

**Discussion:**

This submission proposes spec text for TGbi draft D1.0 for the generation and the distribution of the Privacy Management Group Temporal Keys (PMGTK) corresponding to the cryptographic keys that are used by BPE APs affiliated with a BPE AP MLD to encrypt the Frame Body field of the Privacy Beacon.

**Proposed spec text:**

The baseline for this text is 802.11 REVme D7.0, and 802.11 TGbe draft D7.0.

* **SetKeys**
* **MLME-SETKEYS.request**
* **Semantics of the service primitive**

***Modify the table at the end as follows:***

Each SetKeyDescriptor consists of the following parameters:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| Key | Bit string | N/A | The temporal key value |
| Length | Integer | N/A | The number of bits in the Key to be used. |
| Key ID | Integer | 0–3 shall be used with TKIP, CCMP, and GCMP; 4–5 with BIP for IGTK; 6-7 with BIP for BIGTK; 8–9 with BIP for WIGTK; and 10–4095 are reserved | Key identifier |
| Key Type | Enumeration | Group, Pairwise, PeerKey, IGTK, BIGTK, WIGTK, PGTK | Defines whether this key is a GTK, TK, TPK-TK, IGTK, BIGTK, ~~or~~ WIGTK or PGTK respectively. |
| Address | MAC address | Any valid -individual address | This parameter is valid only when the Key Type value is one of:* Pairwise,
* Group and the STA is in an IBSS or PBSS (but not an MBSS),
* PeerKey.
 |
| Receive Sequence Counter | 8 octets | N/A | Initialization value of the replay counter(s).This parameter is valid only when the Key Type is Group, IGTK, BIGTK, or WIGTK. |

* **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 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 as defined in Figure 12-50i (PGTK KDE format).

 The Key field is the PGTK being distributed.

* **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 EDP epoch operation is supported by both AP MLD and non-AP MLD, 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 sent to the non-AP MLD using another group key handshake immediately after the current PGTK has been sent (#643).
* **Security**
* **Framework**
* **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 frame anonymization (#645).
* 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 frame anonymization(#645).
* 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 frame anonymization (#645).
* If an RSNA uses PASN authentication, an RSNA capable the STA establishes an RSNA asdescribed 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).
* **Keys and key distribution**
* **Key hierarchy**
* **General**

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

RSNA defines the following key hierarchies:

* WIGTK, a hierarchy consisting of a single key to provide integrity protection for broadcast and group addressed WUR Wake-up frames
* PGTK, a hierarchy consisting of a single key used to frame anonymization (#657)
* **EAPOL-Key PDU notation**

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

The following notation is used throughout the remainder of 12.7 (Keys and key distribution) and 13.4 (FT initial mobility domain association) to represent EAPOL-Key PDUs:

EAPOL-Key(S, M, A, I, K, Reserved, RSC, ANonce/SNonce, MIC, {Key Data})

where

 .... .....

 WIPN is the last WIPN, as provided by the WIGTK KDE

 PGTK[ST] is the PGTK KDE, with the PGTK Switch Time Indication field set to ST (#660)

* **Group key handshake**
* **General**

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

The Authenticator uses the Group key handshake to send a new GTK and, if management frame protection is negotiated, a new IGTK, and if beacon protection is enabled, a new BIGTK, and if WUR frame protection is negotiated, a new WIGTK, to the Supplicant. When the Authenticator is an AP MLD and the Supplicant is a non-AP MLD, the Authenticator may also use the Group key handshake to send new GTK(s) for any of the setup links and, if management frame protection is negotiated, new IGTK(s) for any of the setup links, and if beacon protection is enabled, new BIGTK(s) for any of the setup links to the Supplicant and if EDP epoch operation is supported by both the AP MLD and the non-AP MLD, a new PGTK.

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

The Authenticator may initiate the exchange at any time when a Supplicant is disassociated or deauthenticated.

 Message 1: Authenticator®Supplicant:

EAPOL-Key(1,1,1,0,G,0,RSC,0, MIC, {[GTK(N)] [, OCI} [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, MLO GTKn] [, MLO IGTKn] [, MLO BIGTKn] [, PGTK (ST)]})

 Message 2: Supplican®Authenticator: EAPOL-Key(1,1,0,0,G,0,0,0,MIC,{ [OCI]})

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

The following apply:

* WIGTK[R], when present, denotes the WIGTK with its key ID as encapsulated using the KDE as defined in 12.7.2 (EAPOL-Key frames) using the PTK-KEK defined in 12.7.1.3 (Pairwise key hierarchy) and associated IV.
* PGTK, when present, denotes the PGTK with its switch time (#661) as encapsulated using the KDE as defined in 12.7.2 (EAPOL-Key frames).
* **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.