IEEE P802.11
Wireless LANs

|  |
| --- |
| Proposed spec texts for Privacy GTK |
| Date: 2024-09-06 |
| 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 |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This submission proposes resolutions and discussions for CID1001, CID1085 and CID1086 on 802.11bi D0.4:

Revisions:

* R0. Initial version of the document

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 1001 | 42 | 7 | The generation and distribution of the PGTK is not defined | Please define. | Revised.As per discussion below |
| 1085 | 42 | 7 | “How the PGTK is generated by the EDP AP MLD ?” | Specify how the PGTK is assigned by the EDP AP | Revised.As per discussion below |
| 1086 | 42 | 7 | “How the PGTK is distributed by the EDP AP MLD to the EDP non-AP MLDs?” | “Specify how the PGTK is distributed by the EDP AP MLD to the EDP non-AP MLDs” | RevisedAs per discussion below |

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 D0.4 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied*** ***into the TGbi D0.4 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 D0.4 for the generation and the distribution of the Privacy GTK (PGTK) corresponding to the cryptographic key assigned by an EDP AP MLD that is used to manage the group EDP epoch and distributed to the EDP non-AP MLDs associated with the EDP AP MLD.

As the Privacy GTK (PGTK) is a group key, like the existing keys GTK, IGTK and BIGTK, a framework similar to the one used for managing these keys may be used to manage the PGTK meaning, in particular, that the PGTK is generated by the EDP AP MLD and distributed to its EDP non-AP MLDs in the Key Delivery element included in the (Re)Association Response frame and may be updated and distributed later during a Group Key Handshake. However, it is worthwhile to note that the PGTK operates at MLD level contrary to the other group keys operating at link level allowing to have an alignment of the group EDP epochs across the links (if necessary, the term “PGTK” could be replaced by “MLO PGTK” to be clearer).

As a Group Key Handshake shall be done separately for each station during a GTK rekeying (used here to deliver the PGTK), the EDP non-AP MLDs don’t receive the PGTK at the same time whereas all the EDP non-AP MLDs of an EDP group shall use the same PGTK in order to compute the same start time of a group EDP Epoch. To address this temporal issue, a PGTK Switch Time Indication is delivered in companion with the PGTK to indicate the time at which the delivered PGTK shall be applied by the EDP AP MLD and EDP non-AP MLDs.

**Proposed spec text:**

The baseline for this text is 802.11 REVme D5.0, and 802.11 TGbe draft D6.0.

1. Definitions, acronyms, and abbreviations
	1. Definitions specific to IEEE 802.11

***TGbi editor: Add the following definition***

**privacy group temporal key:** [PGTK] A random value, assigned by the access point (AP) MLD, that is used to manage group EDP epoch.

***TGbi editor: Change the following definition:***

wireless network management (WNM) sleep mode: [WNM sleep mode] An extended power save mode for non-access point (non-AP) stations (STAs) and non-AP multi-link devices (non-AP MLDs) whereby a non-AP STA or non-AP STAs affiliated with a non-AP MLD need not listen for every delivery traffic indication map (DTIM) beacon and do not perform group temporal key/integrity group temporal key/beacon integrity group temporal key (GTK/IGTK/BIGTK) updates, the non-AP MLD need not perform privacy group temporal key (PGTK) updates.

9.4.2.46 **FTE**

***TGbi editor: Change Table 9-221 (Subelement IDs) (not all lines shown) as follows:***

The Subelement ID field is defined in Table 9-221 (Subelement IDs):

|  |
| --- |
| * Subelement IDs
 |
| Value | Subelement Name |
| 10 | MLO BIGTK |
| 11 | PGTK |
| ~~11~~12–255 | Reserved |

***TGbi editor: Add the following paragraph at the end of the section as follows:***

The PGTK subelement contains the PGTK, used for providing anonymization for individually addressed frames. The PGTK subelement format is shown in Figure 9-442a (PGTK subelement format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | PGTK Switch Time Indication | Key Length | Wrapped Key |
| Octets: | 1 | 1 | 8 | 1 | 24-40 |

**Figure 9-442a – PGTK subelement format**

The PGTK Switch Time Indication field is as defined in Figure 12-49a (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)).

The Wrapped Key field contains the wrapped PGTK being distributed.

* WNM Sleep Mode element

***TGbi editor: Change the row corresponding to value 1 in Table 9-266 Table 9-266—WNM Sleep Mode Response Status definition as follows:***

|  |
| --- |
| * WNM Sleep Mode Response Status definition
 |
| Value | Description |
| 0 | Enter/Exit WNM sleep mode Accept. |
| 1 | Exit WNM sleep mode Accept, GTK/IGTK/BIGTK/PGTK update required. |

* WNM Sleep Mode Response frame format

***TGbi editor: Change the paragraph related to Key Data field as follows:***

The Key Data field contains zero or more subelements that provide the current GTK, IGTK, BIGTK to the STA and current PGTK to the non-AP MLD. The format of these subelements is shown in Figure 9-1286 (WNM Sleep Mode GTK subelement format), Figure 9-1287 (WNM Sleep Mode IGTK subelement format), Figure 9-1288 (WNM Sleep Mode BIGTK subelement format), Figure 9-1288a (WNM Sleep Mode MLO GTK subelement format), Figure 9-1288b (WNM Sleep Mode MLO IGTK subelement format), ~~and~~ Figure 9-1288c (WNM Sleep Mode MLO BIGTK subelement format), and Figure 9-1288d (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.

***TGbi editor: Insert a new row after value 5 in Table 9-540—Optional subelement IDs for WNM Sleep Mode parameters and change corresponding reserved value as follows:***

|  |
| --- |
| * Optional subelement IDs for WNM Sleep Mode parameters
 |
| Value | Contents of subelement |
| … | … |
| 5 | MLO BIGTK |
| 6 | PGTK |
| ~~6~~7–255 | Reserved |

***Add the following paragraph at the end of the section as follows:***

The PGTK subelement contains the PGTK of the EDP AP MLD as shown in Figure 9-1288a (WNM Sleep Mode PGTK subelement format).

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

**Figure 9-1288d—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 12-49a (PGTK KDE Format).

 The Key field is the PGTK being distributed.

* MLME
* Power management
* Power management in a non-DMG infrastructure network
* General

***TGbi editor: Change the eighth paragraph as follows:***

WNM sleep mode enables an extended power save mode in which a non-AP STA need not listen for every DTIM beacon, and need not perform GTK/IGTK/BIGTK updates. Further, the non-AP MLD need not perform PGTK updates. A STAs in WNM sleep mode can transition to awake state as infrequently as once every WNM sleep interval to check whether its corresponding TIM bit is set or group addressed traffic is pending. The WNM sleep interval advertised by a non-AP STA affiliated with a non-AP MLD is applied at the MLD level and the WNM procedures described in this subclause and in 11.2.3.15 (WNM sleep mode) are performed at the MLD level and apply to all the STAs affiliated with the MLD.

* WNM sleep mode
* WNM sleep mode capability

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

To prevent key reinstallation attacks, a non-AP STA in which dot11WNMSleepModeActivated is true shall maintain a copy of the most recent GTK, most recent IGTK and most recent BIGTK installed when exiting WNM sleep mode and shall not install a GTK, IGTK or BIGTK when the key to be set upon exiting WNM sleep mode matches any of the maintained keys (see 6.5.14 (SetKeys)). A non-AP MLD, having all affiliated non-AP STAs in which dot11WNMSleepModeActivated is true, shall maintain a copy of the most recent PGTK when exiting WNM sleep mode and shall not install a PGTK when the key to be set upon exiting WNM sleep mode matches the maintained key.

***TGbi editor: Change the fourth paragraph as follows:***

WNM sleep mode enables an extended power save mode for non-AP STAs in which a non-AP STA need not listen for every DTIM beacon, and need not perform GTK/IGTK/BIGTK updates. Further, the non-AP MLD need not perform PGTK updates. A non-AP STA can sleep for extended periods as indicated by the WNM Sleep Interval field of the WNM Sleep Mode element, which is present in WNM Sleep Mode Request frames transmitted by the non-AP STA.

* WNM sleep mode non-AP STA operation

***TGbi editor: 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 Group EDP epoch is supported by both the AP MLD and the non-AP MLD, the non-AP MLD shall delete the PGTKSA if the response indicates success.

* WNM sleep mode AP operation

***TGbi editor: 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 Group EDP epoch 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.

* STA authentication and association
* Association, reassociation, and disassociation
* Non-AP STA, non-AP MLD and non-PCP STA association initiation procedures

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

The SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA, and TPKSA (including temporal keys) held for communication with the AP MLD by using MLME-DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)) before invoking MLME-ASSOCIATE.request primitive.

* AP, AP MLD or PCP association receipt procedures

***TGbi editor: Change bullet m as follows:***

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)).
* Non-AP STA, non-AP MLD and non-PCP STA reassociation initiation procedures

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

Except when the association is part of a fast BSS transition, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA and TPKSA (including temporal keys) held for communication with the AP, AP MLD, or PCP by using the MLME-DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)) before invoking an MLME-REASSOCIATE.request primitive.

* AP, AP MLD, or PCP reassociation receipt procedures

***TGbi editor: Change bullet k as follows:***

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

* If management frame protection is not in use, or the ResultCode in the MLME-REASSOCIATE.response primitive is SUCCESS and the reassociation is not part of a fast BSS transition, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA and TPKSA (including temporal keys) held for communication with the STA or the non-AP MLD by using the MLME-DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)).
* Non-AP STA, non-AP MLD, and non-PCP STA disassociation initiation procedures

***TGbi editor: Change bullet c as follows:***

Upon receipt of an MLME-DISASSOCIATE.request primitive, a non-AP STA, non-AP MLD, and non-PCP STA’s MLME shall disassociate from an AP, AP MLD, or PCP, respectively, using the following procedure:

* Upon receiving an MLME-DISASSOCIATE.confirm primitive, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA and TPKSA (including temporal keys) held for communication with the AP, AP MLD or PCP by using the MLME‑DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)) and by invoking an MLME-SETPROTECTION.request(None) primitive. In the case of an MM-SME coordinated STA, the MLME shall perform this for each STA whose address was included in the MMS parameter of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive that established the association.
* Non-AP STA, non-AP MLD and non-PCP STA disassociation receipt procedure

***TGbi editor: Change bullet c as follows:***

Upon receipt of a Disassociation frame from an AP, AP MLD, or PCP for which the state is State 3 or State 4, if management frame protection was not negotiated when the PTKSA(s) were created, or if management frame protection was negotiated when the PTKSA(s) were created and the frame is not discarded per management frame protection processing, a non-AP STA, non-AP MLD, and non-PCP STA, respectively, shall disassociate from the AP, AP MLD, or PCP using the following procedure:

* Upon receiving the MLME-DISASSOCIATE.indication primitive, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA and TPKSA (including temporal keys) held for communication with the AP, AP MLD or PCP by using the MLME‑DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)) and by invoking an MLME-SETPROTECTION.request(None) primitive. The MM-SME shall perform this process for each STA whose address was included in the MMS parameter of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive that established the association.

11.3.5.8 AP, AP MLD, or PCP disassociation initiation procedure

**11.3.5.8.1 General**

***TGbi editor: Change bullet d as follows:***

Upon receipt of an MLME-DISASSOCIATE.request primitive, an AP, AP MLD, or PCP shall disassociate a STA (with respect to the AP or PCP) or a non-AP MLD (with respect to the AP MLD) using the following procedure:

* Upon receiving an MLME-DISASSOCIATE.confirm primitive, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA and TPKSA (including temporal keys) held for communication with the STA by using the MLME‑DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)) and by invoking an MLME-SETPROTECTION.request(None) primitive. The MM-SME shall perform this process for each STA whose address was included in the MMS parameter of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive that established the association.
* AP, AP MLD, or PCP disassociation receipt procedure

***TGbi editor: Change bullet c as follows:***

Upon receipt of a Disassociation frame from a STA or a non-AP MLD for which the state is State 3 or State 4, if management frame protection was not negotiated when the PTKSA(s) were created, or if management frame protection was negotiated when the PTKSA(s) were created and the frame is not discarded per management frame protection processing, the AP or PCP(with respect to the STA) or AP MLD (with respect to the non-AP MLD) shall disassociate the STA or the non-AP MLD using the following procedure:

* Upon receiving an MLME-DISASSOCIATE.indication primitive the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA, WIGTKSA, WTKSA, PGTKSA and TPKSA (including temporal keys) held for communication with the STA or the non-AP MLD by using the MLME‑DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)) and by invoking an MLME-SETPROTECTION.request(None) primitive. The MM-SME shall perform this process for each STA whose address was included in the MMS parameter of the MLME-ASSOCIATE.request or MLME-REASSOCIATE.request primitive that established the association.
* **Security**
* Framework
* RSNA establishment

***TGbi editor: Insert a new bullet in a) after the 9) bullet and in b) after 8) bullet of the first paragraph as follows:***

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:
* If the STAs negotiate WUR frame protection, the SME programs the WTK and WTPN into the MAC for protection of individually addressed WUR Wake-up frames, and programs the WIGTK and WIPN into the MAC for the protection of broadcast and group addressed WUR Wake-up frames.
* If the Group EDP epoch 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 the STAs negotiate WUR frame protection, the SME programs the WTK and WTPN into the MAC for protection of individually addressed WUR Wake-up frames, and programs the WIGTK and WIPN into the MAC for the protection of broadcast and group addressed WUR Wake-up frames.
* If the Group EDP epoch 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

e) If an RSNA allows for confidentiality only (no authentication) in an infrastructure BSS, an SME establishes an RSNA as follows:

* If the STAs negotiate WUR frame protection, it programs the WTK into the MAC for protection of individually addressed WUR Wake-up frames, and programs the WIGTK into the MAC for protection of broadcast and group addressed WUR Wake-up frames.
* If the Group EDP epoch 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
* RSNA security association management
* Security associations
* Security association definitions
* General

***TGbi editor: Insert a new bullet at the end of the 2nd paragraph as follows:***

A security association is a set of policy(ies) and key(s) used to protect information. The information in the security association is stored by each party of the security association, needs to be consistent among all parties, and needs to have an identity. The identity is a compact name of the key and other bits of security association information to fit into a table index or an MPDU. The following types of security associations are supported by an RSNA STA:

* PGTKSA: A result of a successful group key handshake, the Reassociation Response frame of the fast BSS transition protocol, the encrypted Reassociation Response frame specified in 12.14.5.2 (Encryption of the Frame Body Field of the (Re)Association Request/Response Frame for MLO), or successful FILS authentication.

***TGbi Editor: Insert the following subclauses as the last subclause of 12.6.1.1:***

12.6.1.1.xx PGTKSA

An Authenticator’s SME creates a PGTKSA when dot11GroupEpochActivated is true. A PGTKSA has the lifetime of the AP MLD.

A Supplicant’s SME creates a PGTKSA when dot11GroupEpochActivated is true and the SME receives a PGTK from its Authenticator.

A PGTKSA consists of the following:

* PGTK
* Authenticator MAC address

**12.6.1.2.2 Security association in an ESS**

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

The MLME-DELETEKEYS.request primitive deletes the temporal key(s) established for the security association so that they cannot be used to protect subsequent IEEE 802.11 traffic. An SME uses this primitive when it deletes a PTKSA, GTKSA, IGTKSA, BIGTKSA, PGTKSA, WIGTKSA or TPKSA.

**12.6.16 RSNA security association termination**

***TGbi editor: 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) 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

***TGbi editor: Change the 7th paragraph as follows:***

An Authenticator may initiate a group key handshake for the purpose of GTK rekeying (with a GTKSA), IGTK keying (with an IGTKSA), BIGTK rekeying (with a BIGTKSA), PGTK rekeying (with a PGTKSA) or WIGTK rekeying (with a WIGTKSA).

***TGbi editor: modify the following paragraph after the fourth paragraph of the subclause (“The IEEE 802.11 MAC shall issue an...”) 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 PGTK through a group key handshake between the AP MLD and non-AP MLD.

* Keys and key distribution
* Key hierarchy
* General

***TGbi editor: Insert a new bullet g at the end of the first paragraph as follows:***

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 to provide anonymization for individually addressed frames

***TGbi Editor: Insert the following subclauses as the last subclause of 12.7.1.X:***

12.7.1.xx Privacy group key hierarchy

The Authenticator shall select the PGTK as a random value each time it is generated.

The Authenticator may update the PGTK for any reason, including:

* The disassociation or deauthentication of a non-AP MLD.
* An event within the SME that triggers a group key handshake.

The PGTK is configured via the MLME-SETKEYS.request primitive; see 6.5.14 (SetKeys). PGTK configuration is described in the EAPOL-Key state machines; see 12.7.9 (RSNA Supplicant key management state machine) and 12.7.10 (RSNA Authenticator key management state machine).

* EAPOL-Key frames

***TGbi editor: Insert*** ***a new row after value 22 in Table 12-10 KDE selectors and change corresponding reserved value as follows:***

|  |
| --- |
| * KDE selectors
 |
| OUI | Data type | Meaning |
| … | … | … |
| 00-0F-AC | 23 | PGTK KDE |
| 00-0F-AC | ~~23~~24–255 | Reserved |
| Other OUI or CID | Any | Vendor specific |

***Insert the following at the end of the section as follows***

The format of the PGTK KDE is shown in Figure 12-49a (PGTK KDE format).

|  |  |  |
| --- | --- | --- |
|  | PGTK Switch Time Indication | PGTK |
| Octets: | 8 | 32 |

**Figure 12-49a – PGTK KDE Format**

The PGTK Switch Time Indication field indicates the time at which the PGTK indicated in the Key field shall be applied replacing the PGTK in use by the EDP AP MLD and EDP non-AP MLDs. The 8 octet PGTK Switch Time Indication is set to the time at which the PGTK contained in the PGTK field shall be applied by the EDP AP MLD and EDP non-AP MLDs using as a timebase 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.

* EAPOL-Key PDU notation

***Insert the following after WIPN as follows:***

 PGTK is the PGTK KDE,

* Group key handshake
* General

***TGbi editor: 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, and if Group EDP epoch is supported by both AP MLD and non-AP MLD, a new PGTK. 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.

***TGbi editor: 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] )

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

***TGbi editor: Insert a new bullet after WIGTK[R] of the 3rd paragraph as follows:***

* PGTK, when present, denotes the PGTK as encapsulated using the KDE as defined in 12.7.2 (EAPOL-Key frames).

* **Group key handshake message 1**

***TGbi editor: Insert a new bullet at the end of key Data specification of the 1st paragraph***

* For MLO, when present, PGTK, PGTK Switch Time Indication (see 12.7.2 (EAPOL-Key frames))

***TGbi editor: Change bullet d of the 3rd paragraph as follows:***

* 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.
* Group key handshake implementation considerations

***TGbi editor: Add the following paragraph after the second paragraph:***

To prevent key reinstallation attacks, the non-AP MLD shall maintain a copy of the most recent PGTK installed as part of the FILS authentication protocol as if they were installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation considerations)) and shall refuse to update a PGTK when the key to be set matches the maintained key.

12.11 Authentication for FILS

* FILS authentication protocol
* (Re)Association Response for FILS key confirmation

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

The FILSR constructs a Key Delivery element indicating the current GTK and GTK PN, and the current IGTK and IPN if management frame protection is enabled, and the current BIGTK and BIPN if beacon protection is enabled, and the current WIGTK and WIPN if WUR frame protection is enabled, and the current PGTK if Group EDP epoch is supported by both AP MLD and non-AP MLD. For non-MLO, the GTK is carried in a GTK KDE. The IGTK and IPN are carried in an IGTK KDE, the BIGTK and BIPN are carried in a BIGTK KDE and the WIGTK and WIPN are carried in a WIGTK KDE. For MLO, the PGTK is carried in a PGTK KDE, GTKs for all setup links are carried in MLO GTK KDEs, the IGTKs in MLO IGTK KDEs, and the BIGTKs in MLO BIGTK KDEs.

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

Upon successful completion of the FILS authentication procedure, the FILSO shall process the Key Delivery element in the (Re)Association Response frame. The FILSO installs the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and WIGTK and WIGTK RSC if present in the Key Delivery element and dot11RSNAWURFrameProtectionActivated is true and PGTK if present in the Key Delivery element and group EDP epoch is supported by both AP MLD and non-A PMLD. For MLO, the FILSO installs the PGTK and installs GTKs, IGTKs and BIGTKs for each setup link.

12.14 Client Privacy Enhancement

* 12.14.5 Encryption of the Frame Body Field of the (Re)Association Request/Response Frame

**12.14.5.2 MLO**

***TGbi editor: Change the nineth paragraph as follows***

If a Key delivery element is included in the (Re)Association Response frame, the EDP AP MLD shall construct

the Key Delivery element with the RSC field set to 0, with the MLO GTK KDE for each setup link, with the MLO IGTK KDE for each setup link if management frame protection is negotiated, with the MLO BIGTK KDE for each setup link if beacon protection is enabled, with the PGTK KDE if Group EDP epoch is supported by both AP MLD and non-AP MLD.

***TGbi editor: Change the last bullet of the paragraph as follows***

On successful (re)association,

— the EDP non-AP MLD installs the GTK and GTK RSC, and IGTK and IGTK RSC if management frame protection is enabled, and BIGTK and BIGTK RSC if present in the Key Delivery element and dot11BeaconProtectionEnabled is true, and PGTK if Group EDP epoch is supported by both AP MLD and non-AP MLD.

* Fast BSS transition
* Key holders
* Authenticator key holders

***TGbi editor: Change the 7th 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 Group EDP epoch is supported by both AP MLD and non-AP MLDs, the R1KH shall derive and distribute the PGTK to all connected non-AP MLDs
* 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.

13.5 FT protocol

* Overview

***TGbi editor: Add the following paragraph at the end of the section:***

To prevent key reinstallation attacks, the non-AP STA shall maintain a copy of the most recent PGTK when present, installed as part of the FT protocol as if they were installed as a result of receipt of EAPOL-Key PDUs (see 12.7.7.4 (Group key handshake implementation considerations)) and shall refuse to update a PGTK when the key to be set matches the maintained key (see 6.5.14 (SetKeys)).

* FT resource request protocol
* Over-the-air fast BSS transition with resource request

***TGbi editor: Change the 12th paragraph as follows:***

In an RSN, on successful completion of the FT authentication exchange of the FT resource request protocol, the PTKSA has been established and proven live. The key replay counter shall be initialized to 0, and the subsequent EAPOL-Key PDUs (e.g., GTK, IGTK, BIGTK, PGTK and WIGTK updates) shall use the key replay counter to detect and discard replays. The PTKSA shall be deleted by the target FTR if it does not receive a Reassociation Request frame from the FTO within the reassociation deadline timeout value.

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

***TGbi editor: Change the 12th paragraph as follows:***

In an RSN, on successful completion of the FT Confirm/Acknowledgment frame exchange, the PTKSA has been established and proven live. The key replay counter shall be initialized to 0, and the subsequent EAPOL-Key frames (e.g., GTK, IGTK, BIGTK, ~~and~~ WIGTK and PGTK updates) shall use the key replay counter to detect and discard replays. The PTKSA shall be deleted by the target FTR if it does not receive a Reassociation Request frame from the FTO within the reassociation deadline timeout value. Resource request procedures are specified in 13.11 (Resource request procedures).

* FT reassociation
* FT reassociation in an RSN

***TGbi editor: Change the 2nd paragraph as follows:***

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

FTO®Target FTR: Reassociation Request(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request, RSNXE, Basic Multi-Link element)

Target FTR®FTO: Reassociation Response(RSNE[PMKR1Name], MDE, FTE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N], IGTK[M], BIGTK[Q], WIGTK[R], PGTK, MLO GTKn, MLO

IGTKn, MLO BIGTKn], RIC-Response, RSNXE, Basic Multi-Link element)

where

* MLO GTK is the MLO GTK subelement for the AP affiliated with the AP MLD for the link speci- fied by the value in the Link ID field,
* MLO IGTK is the MLO IGTK subelement for the AP affiliated with the AP MLD for the link speci- fied by the value in the Link ID field,
* MLO BIGTK is the MLO BIGTK subelement for the AP affiliated with the AP MLD for the link specified by the value in the Link ID field.
* The GTK[N], IGTK[M], ~~and~~ BIGTK[Q]are present when the FTR is an AP.
* The MLO GTKn, MLO IGTKn, MLO BIGTKn, PGTK and the Basic Multi-Link element are present when the FTR is an AP MLD.
* FT authentication sequence
* FT authentication sequence: contents of fourth message

***TGbi editor: Change the 5th paragraph as follows:***

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 subelements or PGTK, MLO GTK, MLO IGTK and MLO BIGTK subelements. If a GTK, an IGTK, a BIGTK, WIGTK, a PGTK, an MLO GTK, an MLO IGTK or an MLO BIGTK are 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 GTK, IGTK, BIGTK, PGTK, WIGTK, MLO GTK, MLO IGTK, or MLO BIGTK subelement.