IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolution on BPE AP MLD Group Keys  |
| Date: 2025-06-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jarkko Kneckt | Apple Inc. | Cupertino, CA |  | jkneckt@apple.com |
| Jerome Henry  | Cisco |  |  |  |

This submission is a comment resolution to the CIDs: 258, 292, 632, and 896.

This submission clarifies BPE MLDs key hierarchy. A BPE MLD has:

* **PTK** to encrypt all unicast frames and to anonymize all STA specific fields in MAC headers
* **GTK** per affiliated AP to encrypt group addressed data and management frames
* **PGTK** to anonymize AP MLD specific fields in MAC headers
* **Identity Key** to identify the AP MLD that is the transmitter of the Privacy Beacons

A BPE non-AP MLD setups GTK, PGTK and Identity key in encrypted association.

All these keys, except the identity key, are deleted in disassociation and deauthentication.

This submission proposes a lifetime for the identity key. The identity key and its lifetime are configured to the non-AP MLD in a protected association. The non-AP MLD deletes the identity key when its lifetime has expired, which helps a non-AP MLD to reduce the number of stored identity keys. Large number of stored identity keys consumes memory and makes the AP MLD identification from a received Privacy Beacon frame slower and computation intensive.

Revision History:

* R0 Initial draft

# **Solved comments:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| 258 | 96.33 | 10.71.8 | A BPE AP MLD discovery key should be possible to share in protected management frames to enable STA to roam to another BPE AP MLD. | Please define a signaling to share a neighbor BPE AP MLD identity key by using unicast protected management frames to associated non-AP MLDs. | Revised. Agree in principle with the comment. The Discovery Key is added as part of the protected association. The associated STAs operation is simplified when it has all the keys of the associated AP MLD. TGbi editor, please make the changes as shown in the 11-25-1029r0 and identified with #258. |
| 292 | 96.33 | 10.71.8 | It should be possible to share a neighboring BPE AP MLD identity key in protected management frames, in order to enable a STA to roam to another BPE AP MLD. Please define such a mechanism. | As in comment. | Revised. Agree in principle with the comment. The Discovery Key is added as part of the protected association. The associated STAs operation is simplified when it has all the keys of the associated AP MLD. TGbi editor, please make the changes as shown in the 11-25-1029r0 and identified with #292. |
| 632 | 0.00 | 10.71.8.2 | There are references to "identity key" or "Identity Key" but it is not clear what this is. Is it an alias for the PGTK, perhaps? | As it says in the comment | Revised. The Identity Key is added to the definitions. TGbi editor, please make the changes as shown in the 11-25-1029r0 and identified with #632.  |
| 896 | 96.09 | 10.71.8.3 | The payload of the Privacy Beacon is encrypted with the GTK used originally for the encryption of group addressed Data frames and not group addressed management frame. Using the same key (GTK) for encrypting different type of frames (data/management) and different purposes (security/privacy) is not a recommended security practice and constitutes a bad key hygiene / key separation in terms of security. | Please define a new key dedicated to the encryption of the privacy beacon | Rejected. The Beacon frame is a management frame and GTK is used to encrypt all group addressed data and management frames. A new key definition only for a single frame payload adds memory requirements for non-AP MLD and AP MLD. The GTK is not used for privacy purposes in Privacy beacon, it used to encrypt, and integrity protect the Privacy Beacon frame.  |

**Normative Text**

**3.2 Definitions specific to IEEE 802.11**

*Instructions to the Editor: Please add the following new definition in the correct alphabetical order*

**Identity key** (#632)**:** A random value, assigned by the BPE access point (AP) multi-link device (MLD), that is used to detect the identity of the BPE AP MLD.

**10.71.8 BSS Privacy Operations**

*Instructions to the Editor: Please modify the third paragraph as shown below.*

A BPE AP MLD does not use beacon protection with a BIGTK or BIP with IGTK. A BPE non-AP MLD obtains from the protected (re)association response frame a GTK for each affiliated AP that it has a link, a BGTK and an Identity Key of the associated BPE AP MLD. (#258, #292)

NOTE1- An AP affiliated with a BPE MLD does not have BIGTK, because they do not transmit Beacon frames. Instead, they transmit Privacy Beacon frames, see (10.71.8.2(BPE AP MLD Beaconing). (#258, #292)

NOTE2 – An AP affiliated with a BPE MLD does not have IGTK, because all group addressed management frames are encrypted by using the group cipher suite indicated for the BSS. IGTK integrity protects group addressed management frames. Integrity protected group addressed management frames can be received by eavesdroppers, which would reduce privacy of the BPE AP MLD. (#258, #292)

The associated non-AP BPE MLDs and BPE AP MLD operate in a single EDP group named as a(#Ed) BPE group. The BPE group has a single schedule and a single PGTK(#258, #292). At the beginning of each epoch, the BPE non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see10.71.3 (Establishing frame anonymization parameter sets (#1002)). The BPE MLD affiliated AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.4 (Establishing BPE frame anonymization parameter sets(#1521)).

**10.71.8.2 BPE AP MLD beaconing**

*Instructions to the Editor: Please modify as shown below.*

A BPE non-AP MLD may discover an AP MLD by using the configured Identity Key. The Identity Key may be configured to the STA by using mechanisms that are out of the scope of the specification. A BPE Non-AP MLD receives the Identity Key of the associated BPE AP MLD in the protected (re)association response frame. (#258, #292)

**6.5.3.3 MLME-SCAN.confirm**

**6.5.3.3.2 Semantics of the service primitive**

*Instructions to the Editor: Please modify as shown below.*

*The primitive parameters are as follows:*

*MLME-SCAN.confirm(*

*BSSDescriptionSet,*

*BSSDescriptionFromMeasurementPilotSet,*

*BSSDescriptionFromFDSet,*

*BSSDescriptionFromPrivacyBeacons,* (#258, #292)

*ResultCode,*

*Multi-band local,*

*Multi-band peer,*

*ScannedChannelList,*

*VendorSpecificInfo*

*)*

*Instructions to the Editor: Please add the following row after the BSSDescriptionFromFDSet.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| BSSDescriptionFromPrivacyBeaconSet (#258, #292) | Set of BSSDescriptionFrom PrivacyBeacons  | N/A | The BSSDescriptionFromPrivacyBeaconSet is returned to indicate the results of the scan request derived from the Privacy Beacon frames. It contains zero or more instances of a BSSDescriptionFromPrivacyBeacon. Present if dot11EPDPKEActivatedis nonzero, otherwise not present.  |

*Instructions to the Editor: Please add the following text and table after the BSSDescriptionFromFDSet table.*

The BSSDescriptionFromPrivacyBeaconSet parameter is present if dot11EPDPKEActivated is true; otherwise, it is not present. Each BSSDescriptionFromPrivacyBeacon consists of the parameters shown in the following table(#258, #292):

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| Address 2 | MAC address  | N/A | The transmitter address of the Privacy Beacon frame.  |
| Identity Hash  | MAC address  | N/A | The Identity Hash of the Privacy Beacon frame.  |

**6.5.14.1 MLME-SETKEYS.request**

**6.5.14.1.2 Semantics of the service primitive**

*Instructions to the Editor: Please modify the Key Type as shown below.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Type**  | **Valid range**  | **Description** |
| Key Type  | Enumeration  | Group, Pairwise,PeerKey, IGTK, BIGTK, WIGTK, PGTK, Identity Key (#258, #292) | Defines whether this key is a GTK, TK, TPK-TK, IGTK, BIGTK, or WIGTK, PGTK, or Identity Key (#258, #292)respectively. |

**6.5.14.1.4 Effect of receipt**

*Instructions to the Editor: Please modify as shown below.*

When the Key Type is Group, IGTK, BIGTK, or WIGTK, or PGTK and the key matches the GTK, IGTK,BIGTK, or WIGTK, ~~or~~ PGTK, or Identity Key(#258, #292) 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 such that the successive start times of the EDP Epochs are processed using that key.

–– When the Key Type parameters is Identity Key, the MAC installs the key such that the transmitted and received Privacy Beacon frames are processed by using that key. The Identity Key is maintained in the non-AP MLD for a lifetime of the key that is configured together with the Identity key, or as long as the non-AP MLD desires to discover and identify the AP MLD, whichever is shorter. A non-AP MLD does not delete the AP MLD specified Identity Key if the non-AP MLD is disassociated or deauthenticated from the non-AP MLD. (#258, #292)

— 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, Peer-

Key, or BIGTK, ~~or~~ PGTK, or Identity Key (#258, #292) 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**

*Instructions to the Editor: Please add the new subelement to the end of the list and number correctly.*

**Table 9-221—Subelement IDs**

|  |  |
| --- | --- |
| **Value**  | **Subelement Name** |
| <ANA> | Identity Key |

The Identity Key subelement contains the Identity Key, used to encrypt the identity of the AP MLD in the Privacy Beacons. The Identity Key subelement format is shown in Figure 9–XX (Identity Key subelement format). (#258, #292)

|  |  |  |  |
| --- | --- | --- | --- |
| Subelement ID | Length | Wrapped Key | Key Lifetime |
| 1 | 1 | 16 | 3 |

**Figure 9-442d—Identity Key subelement format**

The Wrapped Key field contains the wrapped Identity Key being distributed.

The Key Lifetime contains the Lifetime of the Key in units of the seconds. Value 0 indicates that the key has no lifetime. (#258, #292)

**11.3.5.3 AP or PCP association receipt procedures**

*Instructions to the Editor: Please change the first paragraph as shown with track changes.*

**Change the first paragraph as follows**:

m) If the ResultCode in the MLME-ASSOCIATE.response primitive is SUCCESS, the SME shall delete any PTKSA, GTKSA, IGTKSA, BIGTKSA(11ba), (#3344)WIGTKSA, WTKSA, PGTKSA, Identity Key SA(#258, #292), and TPKSA (including temporal keys)(#205) held for communication with the STA by using the MLME-DELETEKEYS.request primitive (see 12.6.16 (RSNA security association termination)).

**11.3.5.5 AP, AP MLD, or PCP reassociation receipt procedures**(#1001)

*Instructions to the Editor: Please change the first paragraph as shown with track changes.*

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

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:

k) 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, Identity Key SA(#258, #292), 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)).

**12.2.4 RSNA establishment**

*Instructions to the Editor: Please change as shown with track changes below:*

**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:

a) 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:

1. It identifies the AP as an RSNA AP from the AP’s Beacon, Privacy Beacon(#258, #292), DMG Beacon, Announce, Information Response, FILS Discovery, or Probe Response frames.

NOTE- As described in 10.71.8.3(Steering to BPE AP MLD), the STA might identify an AP affiliated with a BPE AP MLD by using the AP’s anonymized link address and the Neighbor Report element that is received from the associated AP. (#258, #292)

11) If the AP is affiliated with a BPE AP MLD, the SME programs the Identity Key into the MAC to identify the AP MLD from its Privacy Beacon frames. (#258, #292)

b) If an RSNA is based on a PSK or password in an infrastructure BSS, an SME establishes an RSNA

as follows:

10) If the AP is affiliated with a BPE AP MLD, the SME programs the Identity Key into the MAC for identifying the AP MLD from its Privacy Beacon frames. (#258, #292)

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

establishes an RSNA as follows:

10) If the AP is affiliated with a BPE AP MLD, the SME programs the Identity Key into the MAC for identifying the AP MLD from its Privacy Beacon frames. (#258, #292)

**12.6.1 Security associations**

**12.6.1.1.1 General**

*Instructions to the Editor: Please change the second paragraph by adding a new subbullet at the end of the list as shown below*

* Identity Key Security Association: A result of a successful group key handshake with a BPE AP MLD, the Reassociation Response frame of the fast BSS transition protocol, the encrypted (Re)association Response frame specified in 12.16.6.2(MLO), or successful FILS authentication. (#258, #292)

**12.6.1.1.15 Identity Key Security Association**

*Instructions to the Editor: Please add the new clause as shown below*

An Authenticator's SME creates an Identity Key Security Association for BPE AP MLD. (#258, #292)

A Supplicant's SME creates an Identity Key Security Association when the SME receives an Identity Key from its Authenticator. The Identity Key Security Association has a lifetime that is signaled by the authenticator together in the Identity Key KDE. (#258, #292)

An Identity Key Security Association consists of the following:

–– Director vector (whether the Identity Key is used for transmit or receive).

— Identity Key

–– Lifetime of the Identity Key(#258, #292)

**12.6.1.2.2 Security association in an ESS**

*Instructions to the Editor: Please add the following text as the last paragraph of the clause.*

The Identity Key Security Association has a separate lifetime, and the identity key is deleted when its lifetime expires. A STA may use the Identity Key to identify the AP from its Privacy beacons after the STA has been disassociated or deauthenticated from the AP MLD. An SME uses the MLME DELETEKEYS.request primitive when it deletes an Identity Key. (#258, #292)

**12.6.2 RSNA selection**

*Instructions to the Editor: Please modify the clause as shown below.*

A STA not affiliated with a BPE MLD(#258, #292) and prepared to establish RSNAs shall advertise its capabilities by including the RSNE in Beacon, Information Response, and Probe Response frames and may also include the RSNE in DMG Beacon and Announce frames. The included RSNE shall specify all of the authentication and cipher suites enabled by the STA’s policy. A STA shall not advertise any authentication or cipher suite that is not enabled. (11ba)If WUR frame protection is enabled, a WUR AP shall advertise such capability by setting to 1 the Protected WUR Frame Support subfield in the RSNXE in its Beacon and Probe Response frames.

A STA affiliated with a BPE MLD does not advertise its capability or transmit Beacon, Information Response, and Probe Response frames. The STA sends Privacy Beacons to be identifiable for the STAs that have the configured Identity Key and the RSNE of the AP MLD as defined in 10.71.8.1(BPE AP MLD Discovery). (#258, #292)

**12.7.4 EAPOL-Key PDU notation**

*Instructions to the Editor: Please add the last sentence in blue font as shown.*

**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

....

{Key Data} is a sequence of zero or more elements and KDEs, concatenated and contained in the

Key Data field, where

...

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

PGTK is the PGTK KDE

Identity Key is the Identity Key KDE(#258, #292)

**12.7.7.2 Group key handshake message 1**(#1001)

*Instructions to the Editor: Please modify as shown with track changes below.*

**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, PGTK Switch Time Indication (see 12.7.2 (EAPOL-Key

frames(#1001)))

— For BPE MLO, when present, Identity Key (see 12.7.2 (EAPOL-Key frames)) (#258, #292)

On reception of message 1, the Supplicant:

d) Uses the MLME-SETKEYS.request primitive to configure the (#1567)GTK and, the PGTK when present, the Identity Key when present(#258, #292), the IGTK when present, and the BIGTK if (#1486)beacon protection is enabled at the non-AP STA(11ba), and the WIGTK if WUR frame protection is negotiated, into the MAC.

**12.11.2.6.3 (Re)Association Response for FILS key confirmation**

*Instructions to the Editor: Please modify as shown.*

**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 EDP epoch operation is supported by both the AP MLD and the non-AP MLD, and the Identity Key if the AP MLD is BPE AP MLD(#258, #292).(#Ed) 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, Identity Key is carried in Identity Key KDE(#258, #292), GTKs for all setup links are carried in MLO GTK KDEs, the IGTKs in MLO IGTK KDEs, and the BIGTKs in MLO BIGTK KDEs.

**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 EDP epoch operation is supported by both the AP MLD and the non-AP MLD.(#Ed) For MLO, the FILSO installs the Identity Key(#258, #292) and PGTK and installs GTKs, IGTKs and BIGTKs for each setup link.

**12.16.6.2 MLO**

*Instructions to the Editor: Please modify as shown.*

If a Key Delivery(#1447) 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 Identity Key KDE if the AP MLD is BPE(#258, #292) and with the PGTK KDE if EDP epoch is supported by both AP MLD and non-AP MLD.(#1001)

…

On successful (re)association,

— The(#1450) EDP non-AP MLD shall process the Key Delivery element in the (Re)Association

Response frame if present. (#1127)

— The(#1450) EDP non-AP MLD shall install(#1452) 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 EDP epoch is supported by both AP MLD and non-AP MLD, and Identity Key if AP MLD is BPE AP MLD(#258, #292). (#1127, #1001)

**13.2.2 Authenticator key holders**

*Instructions to the Editor: Please modify as shown.*

**Change the seventh paragraph as follows**

The R1KH shall meet the following requirements:

* For MLO, if EDP epoch is supported by both the AP MLD and the non-AP MLDs, the R1KH shall derive and distribute the PGTK to all connected non-AP MLDs
* For BPE MLO, the R1KH shall derive and distribute the Identity Key to all connected non-AP BPE MLDs. (#258, #292)

**13.8.5 FT authentication sequence: contents of fourth message**(#1001)

*Instructions to the Editor: Please modify as shown.*

**Change the fifth 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 Identity Key(#258, #292), PGTK, MLO GTK, MLO IGTK and MLO BIGTK subelements. If a GTK, an IGTK, a BIGTK,WIGTK, a PGTK, an Identity Key(#258, #292), 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, Identity Key(#258, #292), WIGTK, MLO GTK, MLO IGTK, or MLO BIGTK subelement.