IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 802.11bi EDPKE comments (LB288) | | | | |
| Date: July, 2025 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Duncan Ho | Qualcomm Technologies, Inc | 5665 Morehouse Dr, San Diego CA 92131 USA | +1 (858) 845-3214 | dho@qti.qualcomm.com |

Abstract

This document contains the proposed resolution of the following CIDs received for TGbi LB288:

890, 168, 170, 171, 172, 179, 180, 293, 294, 295, 296, 413, 414, 720, 725, 727, 729, 730, 731, 732, 916

**Revision information**

**Introduction**

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 Draft. The abstract, revision information, introduction, explanation of the proposed changes and references sections are not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

Details of the CIDs and proposed resolution:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **Pg/Ln** | **Comment** | **Proposed Change** | **Resolution** |
| 890 | Julien Sevin | 10.71.3 | 82.15 | The generation and distribution of the KDK are not defined | Please define the generation and distribution of the KDK | **Revised**  Agreed in principle. For easier long-term maintenance, consolidate the requirements of KDK and WTK derivation in a single place - 12.6.1.1.6 (PTKSA) and refer to it when needed in other places of the spec.  Adopt the text changes (wrt REVme D7.0) shown in this document. |
| 168 | Po-Kai Huang | 4.5.4.2 | 23.47 | "PASN and EDPKE authentication  allows for the protection of Management frames without association by establishing a PTKSA using authentication  frames." This sentence may be confusing because EDPKE does go to association eventually. Perhaps, a way to clarify is to have a separate sentence "EDPKE authentication  allows for the protection of (Re)Association Request/Response frame by establishing a PTKSA using authentication  frames." | As in comment | **Accepted** |
| 170 | Po-Kai Huang | 12.16.9.1 | 132.65 | Perhaps adding a note to clarify that we need KEK in PASN because PTK-KEK is used for group key handshake that may be used later even if PTK-KEK is not used in EDPKE frame exchange. | As in comment | **Revised**  Agreed in principle. Add the following note: "The PTK-KEK derived in PASN will be used for group key handshake after association even if PTK-KEK is not used in EDPKE frame exchange". |
| 171 | Po-Kai Huang | 12.16.9.3.1 | 133.27 | The reference should be "12.13.3.1 (Overview)" rather than "12.12.3.1 (Overview)". | As in comment | **Accepted** |
| 172 | Po-Kai Huang | 12.16.9.3.2 | 133.40 | in RSNE construction of 12.13.3.2, we have "Group Data Cipher Suite and Group Management Cipher Suite set to 00-0F-AC:7, indicating that  group addressed traffic is not allowed." Since we will do association afterwards under EDPKE, this rule should not be followed. As a result, we should also list this as a difference. Based on baseline, just indicate group cipher of the BSS | As in comment | **Revised**  Agreed in principle. Add the following bullet at the end of the bullet list:  "- The rule of group addressed traffic not allowed in PASN shall not apply for EDPKE". |
| 179 | Po-Kai Huang | 12.16.9.3.1 | 133.32 | "-- EDPKE AKMP is used instead of PASN AKMP. -- The RSNE indicates EDPKE instead of PASN." The two bullets needs to be deleted. The algorithm number is EDPKE, but the base AKMP is whatever AKMP we use and does not include PASN AKMP or EDPKE AKMP as defined in 12.16.9.1 General | As in comment | **Accepted** |
| 180 | Po-Kai Huang | 12.16.9.3.2 | 133.46 | -- EDPKE AKMP is used instead of PASN AKMP. -- The RSNE indicates EDPKE instead of PASN. The two bullets needs to be deleted. The algorithm number is EDPKE, but the base AKMP is whatever AKMP we use and does not include PASN AKMP or EDPKE AKMP as defined in 12.16.9.1 General | As in comment | **Accepted** |
| 293 | Jay Yang | 12.16.9.3.2 | 133.52 | not sure whether the 2-authentication and 3-authentication frame are exchanged on the same link or a different links? | please add some texts to say "the 2nd authentication frame and 3rd authentication frame shall be exchanged on the same link as the first authentication frame" | **Revised**  Agreed in principle. Replaced the paragraph with "For MLO, the three Authentication frames of EDPKE shall be transmitted on the same link between the non-AP MLD and the AP MLD." |
| 294 | Jay Yang | 12.16.9.3.2 | 133.52 | add the text to clarify the 2nd Authentication frame will be sent by the coreponding AP affliciated with AP MLD. Otherwise, the 2nd Authentication frame will be sent by the AP if we follow the baseline rule. | "add the following text ""the second Authentication frame will be sent on correponding AP affiliated with the AP | **Revised**  Agreed in principle. Duplicate of CID293. |
| 295 | Jay Yang | 12.16.9.3.2 | 133.52 | add some text to clarify the RA field and TA field are the affiliciated non-AP or affiliciated AP MAC address. | as the comments | **Revised**  Agreed in principle. Duplicate of CID293. |
| 296 | Jay Yang | 12.16.9.3.4 | 134.09 | the MLD MAC address should be included in basic ML element in the three authentication frames. | as the comments | **Revised**  Agreed in principle. Add the following to eh bullet list. "The MLD MAC address corresponding to the affiliated STA that transmits the frame shall be included in the Basic Multi-link element in the three Authentication frames" |
| 413 | Mark RISON | 9.3.3.11 | 42.57 | "wrapped data format in PASN Parameters element" -- not clear what field this is referring to | Refer to an actual field name | **Revised**  Agreed in principle.  Replace "wrapped data format" with "Wrapped Data Format field". |
| 414 | Mark RISON | 9.3.3.11 | 43.05 | "RSNE is present and PASN Parameters  element is present if Status Code field is 0." is ambiguous as to scope of "if" | 414 | **Revised**  Agreed in principle. Replace "RSNE is present and PASN Parameters element is present if Status Code field is 0." with "RSNE is present if Status Code field is 0. PASN Parameters element is present if Status Code field is 0.". |
| 720 | Mark RISON | 12.16.9.1 | 132.63 | "If dot11EDPKEActivated is true, then dot11EDPReAssociationFrameEncryptionSupportActivated and dot11KEKPASNActivated are set to true. " is too wishy-washy | Change "are" to "shall be" | **Accepted** |
| 725 | Mark RISON | 12.16.9.3.1 | 133.47 | "-- The RSNE indicates EDPKE instead of PASN." -- indicates where? If in the AKM list, then the previous bullet already says this | Delete the cited text | **Accepted** |
| 727 | Mark RISON |  | 0.00 | I think the convention is to use normal case for headings, not Uppercase the Key Words | E.g. "EDPKE Frame Construction and Processing" should be just "EDPKE frame construction and processing" | **Accepted** |
| 729 | Mark RISON | 12.16.9.3.2 | 133.53 | "The RA field of an Authentication frame in response to an Authentication frame from the peer shall be set to the TA field of the Authentication frame from the peer. " -- by definition a response is to the peer | Delete "from the peer" 2x | **Accepted** |
| 730 | Mark RISON | 12.16.9.3.2 | 133.65 | "The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) are used." is followed by "the following modifications shall be used:". Similarly at 134.6 | Change to "The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) shall be used, except that for MLO:" and then use "shall be used" instead of "is used" in the bullets | **Accepted** |
| 731 | Mark RISON | 12.16.9.3.2 | 134.07 | "HMAC-HASH computation" -- not clear what this is, even less with the uppercase HASH | As it says in the comment | **Rejected**  The "HMAC-HASH" is defined in the 12.13.9.2 (MIC computation for 3rd PASN frame). |
| 732 | Mark RISON | 12.16.9.3.2 | 134.14 | "NOTE 1--In order to ensure KEK derivation, the KEK In PASN field in the RSNXE from the peer STA is set to 1 (see 12.13.8 (PTKSA derivation with PASN authentication)." -- is this a new requirement? If so delete NOTE--- | As it says in the comment | **Accepted** |
| 916 | Duncan Ho | 12.16.9.2 | 133.12 | It is not clear if the combination of EDPK capable but not (re)Assoc encryption capable is allowed. | Clarify in the spec whether such combination is allowed. Will follow up with a contribution. | **Revised**  Agreed in principle. Resolved by resolution of CID720. |

**Text to be adopted (for CID890) begins here.**

4.10.3.2 AKM operations with AS

***TGbi editor: Please modify the 2nd paragraph of 4.10.3.2 as follows:***

A 4-way handshake or FT 4-way handshake utilizing (#1836)EAPOL-Key PDUs is initiated by the

Authenticator to do the following:

— Confirm that a live peer holds the PMK.

— Confirm that the PMK is current.

— In the case of fast BSS transition, derive PMK-R0s and PMK-R1s.

— Derive a fresh pairwise transient key (PTK) from the PMK or, in the case of fast BSS transition, from the PMK-R1. The derived PTK includes the key derivation key (KDK) under the conditions defined in 12.6.1.1.6 (PTKSA).

—Derive a fresh WTK from the KDK(11ba) under the conditions defined in 12.6.1.1.6 (PTKSA).

— Install the pairwise encryption and integrity keys, and the WTK.(11ba), if derived.

— Transport the group (#1349)keys and sequence number from Authenticator to Supplicant and install the (#1349)group keys and sequence number in the STA and, if not already installed, in the AP.

— Verify that the RSN capabilities negotiated are valid as defined in 9.4.2.23.4 (RSN capabilities).

— Confirm the cipher suite selection.12.6.1.1.6 PTKSA

***TGbi editor: Please modify the 5th paragraph of 12.6.1.1.6 as follows:***

The PTKSA consists of the following:

— PTK(11ba), where the PTK includes the KDK only when any of the following is true:

* WUR frame protection is negotiated.
* dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF support capability in its RSNXE (see 9.4.2.240 (RSNXE)).
* Frame anonymization is negotiated (see 10.71 (Frame anonymization))(11bi).

— Pairwise cipher suite selector(11ba), and when WUR frame protection is negotiated, the cipher suite selector 00-0F-AC:6 (BIP-CMAC-128) for individually addressed WUR Wake-up frames

— (#4109)Supplicant MAC address, depending on the negotiated AKMP(#271)(#3266)

— (#4109)Authenticator MAC address, depending on the negotiated (#3266)AKMP(#271)

— Key ID

— If FT key hierarchy is used,

— R1KH-ID

— S1KH-ID

— PTKName

— (11ba)If WUR frame protection is negotiated,

— WTK

12.7.1.3 Pairwise key hierarchy

***TGbi editor: Please modify the 2nd paragraph of 12.7.1.3 as follows:***

The PTK is partitioned into (#3744)PTK-KCK, PTK-KEK, (11ba)a temporal key, and a KDK, if derived under the conditions defined in 12.6.1.1.6 (PTKSA).

12.7.1.6.5 PTK

***TGbi editor: Please modify the 2nd paragraph of 12.7.1.6.5 as follows:***

Using the KDF defined in 12.7.1.6.2 (Key derivation function (KDF)), the PTK derivation is as follows:

(#478)PTK = KDF-Hash-Length(PMK-R1, “FT-PTK”, SNonce || ANonce || BSSID || STA-ADDR)

where

(#478)KDF-Hash-Length is the key derivation function as defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-190 (AKM suite selectors))

PMK-R1 is the key that is shared between the S1KH and the R1KH

SNonce is a 256-bit random bit string contributed by the S1KH

ANonce is a 256-bit random bit string contributed by the R1KH

STA-ADDR is the non-AP STA’s MAC address

BSSID is the BSSID of the target AP’s BSS

Length(#3686) is the total number of bits to derive, i.e., number of bits of the PTK. The length is dependent on the negotiated cipher suites and (#3266)AKMP as defined by Table 12-8 (Cipher suite key lengths(#1083)(#3532)) in 12.7.2 (EAPOL-Key frames) and Table 12-11 (Integrity and key wrap algorithms(#3244)) in 12.7.3 (EAPOL-Key PDU construction and processing)(11ba), and whether a KDK is derived (see 12.6.1.1.6 (PTKSA) for the conditions of derivation of KDK).

12.7.6.2 4-way handshake message 1

***TGbi editor: Please modify the 2nd paragraph of 12.7.6.2 as follows:***

Processing for PTK generation is as follows:

The Authenticator sends message 1 to the Supplicant at the end of a successful IEEE 802.1X authentication, after (re)association completes for a STA that has authenticated with SAE or for which PSK authentication is negotiated(#3434), when a cached PMKSA is used, or after a STA requests a new key. On reception of message 1, the Supplicant determines whether the Key Replay Counter field value has been used before with the current PMKSA. If the Key Replay Counter field value is less than or equal to the current local value, the Supplicant discards the message. Otherwise, the Supplicant:

a) Generates a new nonce SNonce, if no SNonce has yet been generated for this 4-way handshake. The same SNonce is reused within this 4-way handshake until a valid message 3 has been received.(#6483)

b) Derives PTK,.

c) Constructs message 2.

13.2 Key holders

13.2.1 Introduction

***TGbi editor: Please add the following after the last paragraph of 13.2.1:***

The derived PTK includes a Key derivation key (KDK) under the conditions described in 12.6.1.1.6 (PTKSA).13.2.2 Authenticator key holders

***TGbi editor: Please modify the 4th paragraph of 13.2.2 as follows:***

The R1KH and S1KH each derive the PTK(11ba). If WUR frame protection is negotiated, the R1KH and S1KH each derive a WTK from the KDK, which is part of the derived PTK.

13.2.3 Supplicant key holders

***TGbi editor: Please modify the 4th paragraph of 13.2.3 as follows:***

The S1KH shall derive the PTK mutually with the R1KH(11ba)t. If WUR frame protection is negotiated, the S1KH shall derive a WTK from the KDK, which is part of the derived PTK.

**Text to be adopted (for CID890) ends here.**