IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11bi D0.4 CR for EDPKE related CIDs | | | | |
| Date: 2024-10-28 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Duncan Ho | Qualcomm Technologies Incorporated | 5665 Morehouse Dr  San Diego, CA 92121 | (858) 845-3214 | dho@qti.qualcomm.com |

Abstract

This submission proposes resolutions for the following CIDs:

1005, 1121, 1180, 1198, 1199, 1217, 1218, 1389, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1498

Revisions:

* Rev 0: Initial version of the document.

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 D0.6 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.6 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.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1005 | Jay Yang | 12.14.8 | 84.16 | seems EDPKE feature only cover pre-11be device, please extend it to cover 11be/MLD device. | extend EDPKE feature to protect the association frame(s) between two MLDs. E.g. association frame can be deliveryed on any set-up links, the PTK generated in EDPKE PASN procedure should be MLD level. | **Revised**  Agreed with the comment.  Modified text in REVme D7.0 sections 12.13.8 and 12.13.9 to clarify that for MLO, the MLD MAC addresses (AA and SPA) will be used.  See the proposed changes in this document. |
| 1121 | stephane baron | 4.5.4.2 | 22.38 | missing space between "EDPKE authentication" and "is" | add missing space | **Accepted** |
| 1180 | Stephen McCann | 4.5.4.2 | 22.38 | Typo "is" | Change "PASN authentication or EDPKE authenticationis" to "PASN or EDPKE authentication are" | **Accepted** |
| 1198 | Mark RISON | 4.5.4.2 | 21.61 | "enhanced data privacy key exchange authentication" should be "enhanced data privacy key exchange (EDPKE) authentication" | As it says in the comment | **Accepted** |
| 1199 | Mark RISON | 4.5.4.2 | 22.38 | "authenticationis" missing space | As it says in the comment | **Accepted** |
| 1217 | Mark RISON | 9.3.3.11 | 34.12 | "Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero" doesn't make sense: a format isn't a number. Many instances | As it says in the comment | **Revised** The sentence was borrowed from PASN. To fix the occurrences, change "if wrapped data format" to "if the wrapped data format field" |
| 1218 | Mark RISON | 9.3.3.11 | 34.16 | "Fragment element may be present if any of the elements are fragmented." -- isn't this the case in all Authentication frames? And anyway, isn't it guaranteed to be present if an element is fragmented? Many instances | Delete | **Revised**  The text was borrowed from PASN. Can just remove the sentence. |
| 1389 | Mark RISON | 11.3.4.3 | 61.36 | ", or 12.13" should be ", 12.13" | As it says in the comment | **Accepted** |
| 1489 | Mark RISON | 12.14.8.1 | 84.21 | "If dot11EDPKEActivated is true, then dot11EDPEncryptionOfTheFrameBodyFieldOfTheReAssociation RequestResponseFrameSupportActivated is true." -- if one necessarily implies the other (does it go both ways?) then the long one is superfluous | As it says in the comment | **Rejected**  One implies the other but not in the reverse direction, so the existing text (logic) is needed. |
| 1490 | Mark RISON | 12.14.8.2 | 0.00 | "When EDPKE AKMP" missing article | As it says in the comment | **Revised**  Add "the" in front of "EDPKE" |
| 1491 | Mark RISON | 12.14.8.3.1 | 84.53 | "except with the following modifications:" is weird. Ditto next subclause | Change to "with the following differences" as above | **Accepted** |
| 1492 | Mark RISON | 12.14.8.3.1 | 85.05 | "RNSE" should be RSNE, and is missing an article (as are other bullets) | As it says in the comment | **Accepted** |
| 1493 | Mark RISON | 12.14.8.3.4 | 85.17 | "Key Confirmation Key (KCK), Key Encryption Key (KEK), Temporal Key (TK) and the Key Derivation Key (KDK) which" -- things outside parens should be lowercase, and which should be that | As it says in the comment | **Revised**  That sentence was removed by the resolution of CID1041 so no further edits are needed. |
| 1494 | Mark RISON | 12.14.8.3.4 | 85.33 | "If a KDK is derived," -- above there's no indication this is optional | As it says in the comment | **Revised**  That sentence was removed by the resolution of CID1041 so no further edits are needed. |
| 1495 | Mark RISON | 12.14.8.3.4 | 85.36 | "is the Bits required for KCK," -- no idea what "the bits required", let alone "the Bits required", means | As it says in the comment | **Revised**  That sentence was removed by the resolution of CID1041 so no further edits are needed. |
| 1498 | Mark RISON |  | 0.00 | EPASN is mentioned twice but otherwise not described | As it says in the comment | **Revised**  Replace "EPASN" with "EDPKE" in page 34/line 33 and page 89/line 65 |

**Discussion:**

None

**Proposal: (#1005)**

**12.13.8 PTKSA derivation with PASN authentication**

For PTKSA key derivation, the inputs to the PRF are the PMK of the PMKSA, a constant label, and a concatenation of non-AP STA’s MAC address, AP’s BSSID, and the DH shared secret from the ephemeral

exchange.

For non-MLO:

PTK = KDF-HASH-NNN (PMK, “PASN PTK Derivation”, SPA || BSSID || DHss)

For MLO:

PTK = KDF-HASH-NNN (PMK, “PASN PTK Derivation”, SPA || AA || DHss)

where

PMK (#7185)is the pairwise master key for the base AKMP if the AKMP is other than

PASN AKMP; see 9.4.2.23.3 (AKM suites). Otherwise, if the base AKMP is

PASN AKMP, that is, the PASN PTKSA is being setup without mutual

authentication in a non-RSN, the PMK shall be set to the string “PMKz” padded

with 28 0s.

NOTE—The PMK for the derivation can come from a cached PMKSA for the AKMP or

from the PMKSA established with PASN by tunneling Wrapped Data or Authentication

frames.

DHss is the shared secret derived from the PASN ephemeral key exchange encoded as an

octet string (12.4.7.2.2 (Integer to octet string conversion)).

KDF-HASH-NNN (#7185)is the key derivation function defined in 12.7.1.6.2 (Key derivation

function (KDF)) using the hash algorithm defined for the base AKMP; see Table 9-

190 (AKM suite selectors). When there is no base AKMP, the hash algorithm is

selected based on the pairwise Cipher Suite provided in the RSNE provided by the

AP in the second PASN frame. SHA-256 is used as the hash algorithm, except for

the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which SHA-384 is used.

NNN is the Bits required for KCK, TK, and KDK depending on the pairwise cipher and

whether a KDK is derived.

[…]

**12.13.9 MIC computation with PASN authentication**

**12.13.9.1 MIC computation for second PASN frame(#8118)**

The MIC field of the MIC element in the (#8118)second PASN frame is set by the AP to first MMM octets of:

For non-MLO:

HMAC-HASH (KCK, BSSID || SPA || Beacon RSNE || Beacon RSNXE || Frame Data)

For MLO:

HMAC-HASH (KCK, AA || SPA || Beacon RSNE || Beacon RSNXE || Frame Data)

where

HASH is the hash algorithm used in 12.13.8 (PTKSA derivation with PASN authentication)

KCK is the key confirmation key for the PASN PTKSA

BSSID is the BSSID for the AP’s BSS

SPA is the MAC address of the non-AP STA, the transmitter of the first PASN frame

Beacon RSNE is the RSN element sent in the Beacons transmitted by the AP

Beacon RSNXE is the RSNXE sent in the Beacons transmitted by the AP

Frame Data is the body of the (#8118)second PASN frame including the MIC element with the

octets in the MIC field of the MIC element set to 0

MMM is half of the output length in octets for the hash function used, that is, 16 or 24 octets

for SHA-256 and SHA-384, respectively\

Beacon RSNE and Beacon RSNXE are included in the MIC computation so that a downgrade attack with

forged RSNE Beacons will result in a MIC mismatch and thus PASN authentication failure.