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 DrSan 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.
* Rev 1: modified the resolution of 1005

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.Clarify that for MLO, the Authentication frames can be sent on any setup links and 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 wrappeddata 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)**

**12.14.8.3.1 Overview**

This subclause defines the procedures for establishing a PTKSA and the corresponding shared keys between

an EDPKE capable STA and AP (for non-MLO) as well as between EDPKE capable non-AP MLD and AP MLD (for MLO). The same procedures as specified in 12.12.3.1 (Overview) are used except with the following modifications:

— The three Authentication frames have the Authentication Algorithm Number field set to <ANA>

(EDPKE Authentication).

— EDPKE AKMP is used instead of PASN AKMP.

— RSNE indicates EDPKE instead of PASN.

— For MLO, the PMKSA association is between the AP MLD and the non-AP MLD.

**12.14.8.3.2 EDPKE Frame Construction and Processing**

The same procedures as specified in 12.12.3.2 (PASN Frame Construction and Processing) are used except

with the following modifications:

— The three Authentication frames have the Authentication Algorithm Number field set to <ANA>

(EDPKE Authentication).

— EDPKE AKMP is used instead of PASN AKMP.

— RNSE indicates EDPKE instead of PASN.

— The PTK is generated as specified in 12.14.8.3.4 (PTKSA derivation and MIC Computation with EDPKE authentication).

For MLO, the first Authentication frame can be sent on any of the setup links. 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.

[…]

**12.14.8.3.4 PTKSA derivation and MIC Computation with EDPKE authentication**

The same procedures as specified in 12.13.8 (PTKSA derivation with PASN authentication) are used. For MLO, the following modifications shall be used:

— The AP MLD MAC address is used instead of the BSSID.

— The non-AP MLD MAC address is used instead of the SPA.

The same procedures as specified in 12.13.9.2 (MIC computation for third PASN frame) are used. For MLO, the following modifications shall be used for HMAC-HASH computation:

— The AP MLD MAC address is used instead of the BSSID.

— The non-AP MLD MAC address is used instead of the SPA.

The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from EDPKE authentication shall be 0.

NOTE—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).