IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB274 CID Resolutions for PASN | | | | |
| Date: 2023-10-30 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Okan Mutgan | Nokia |  |  | okan.mutgan@nokia-sbell.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions and discussions for the following CIDs about PASN on 802.11bh D1.0:

84, 85, 87

R0. Initial Version. Thanks Nehru Bhandaru for some feedback.

R1. PASN-PROT-KEY definition is modified.

aa

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Line | Comment | Proposed Change | Resolution |
| 84 | 30 | 6 | The details of encrypting IRM element in PASN frame 3 and device ID element in PASN frame 2 is missing.. | Add the details of encrypting IRM element in PASN frame 3 and device ID element in PASN frame 2 | ACCEPT. |
| 85 | 36 | 30 | This sentence talks about sending device ID IE encrypted in the second PASN frame (from AP to non-AP STA).  In this case, device ID IE should be encrypted.  This sentence does not mention encryption. | Change the sentence to:  If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in (9.4.2.296a Device ID element), if any. The Device ID element shall be encrypted with the chosen cipher suite. | ACCEPT. |
| 87 | 36 | 48 | This statement talks about sending IRM Element encrypted in the third PASN frame.  The cipher suite (AES-128-CMAC) is strictly specified in this statement.  It is better not to mention a specific cipher suite. | Change  "The IRM element shall be encrypted with the cipher suite of AES-128-CMAC."  to  "The IRM element shall be encrypted with the chosen cipher suite." | ACCEPT. |
|  |  |  |  |  |  |

**Proposed Changes**

**1) CID84**

*Change the paragraph of 12.7.1.3 Pairwise key hierarchy (as amended by IEEE Std 802.11az-2022) as follows:*

The PTK is partitioned into KCK, KEK, a temporal key, and a KDK. A KDK is derived *if and only if* any of the following are true:

- WUR frame protection is negotiated

- dot11SecureLTFImplemented is true and the peer STA has advertised secure HE-LTF 11 support capability in its RSNXE (see 9.4.2.241 (RSN Extension element (RSNXE))

- dot1IRMActivated is true

- dot11DeviceIDActivated is true

*Change the sentence in 12.13.7 PTKSA derivation with PASN authentication (as amended by IEEE Std 802.11az-2022) as follows:*

KDK shall be derived if and only if any of the following are true: ~~if dot11SecureLTFImplemented is true and the peer STA has indicated Secure HE-LTF support capability in its advertised Extended Capabilities.~~

- if dot11SecureLTFImplemented is true and the peer STA has indicated Secure HE-LTF support capability in its advertised Extended Capabilities.

- dot1IRMActivated is true

- dot11DeviceIDActivated is true

*Add a subsection under 12.2.11 Changing MAC Address (as amended by IEEE Std 802.11bh-D1.0) as follows:*

12.2.11.3 Encryption of Device ID IE and IRM IE in PASN

When using PASN authentication, device ID element shall be encrypted in PASN frame 2 (if present) and IRM element shall be encrypted in PASN frame 3 (if present).

To encrypt device ID element in PASN frame 2 or IRM element in PASN frame 3, the following key may be used:

PASN-PROT-KEY = KDF-HASH-NNN (KDK, “PASN Protection Key”, SPA || BSSID)

Where

- the KDK is derived as part of PTKSA of PASN Authentication (see 12.13.7 PTKSA derivation with PASN authentication)

- SPA is the non-AP STA’s MAC address

- BSSID is the AP’s MAC address

- KDF-HASH-NNN is the key derivation function defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm. The hash algorithm is selected based on the pairwise Cipher Suite provided in the RSNE provided by the non-AP STA in the first PASN frame.

- NNN is the Bits required for PASN-PROT-KEY depending on selected the pairwise cipher provided by the non-AP STA in the first PASN frame.

**2) CID85**

36.30

Original:

If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as

defined in 9.4.2.307a (Device ID element), if any.

Proposed:

If dot11DeviceIDActivated is true, including a Device ID element containing a device identifier as defined in (9.4.2.296a Device ID element), if any. The Device ID element shall be encrypted with the chosen cipher suite.

**3) CID87**

36.48

Original:

—If dot11IRMActivated is true, including a IRM element containing an IRM as defined in Figure 9.4.2.307b (IRM element), if any. The IRM element shall be encrypted with the cipher suite of AES-128-CMAC.

Proposed:

—If dot11IRMActivated is true, including a IRM element containing an IRM as defined in Figure 9.4.2.307b (IRM element), if any. The IRM element shall be encrypted with the chosen cipher suite.