IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LB274 CID Resolutions for PASN | | | | |
| Date: 2023-11-6 | | | | |
| 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, 212, 283

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

R1. PASN-PROT-KEY definition is modified.

R2. PASN-PROT-KEY is removed. Instead, KEK is defined and used. Pairwise cipher related text is also added. CID212 is added to this document as part of comment resolution.

R3. KEK definition is modified. CID283 is added to this document as part of comment resolution.

R4. Integrity and key wrap algorithm is defined for encryption. Relevant text is modified.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | REVISED. |
| 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. | REVISED. |
| 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." | REVISED. |
| 212 | 26 | 47 | "The IRM element shall be encrypted with the cipher suite of AES-128-CMAC." -- needs to explain exactly how it is so encrypted | As it says in the comment | REVISED. |
| 283 | 36 | 45 | Should the Device ID element be encrypted (with AES-128-CMAC?) like the IRM element? | Add a sentence, "The IRM element shall be encrypted with the cipher suite of AES-128-CMAC." to the end of the Device ID paragraph. | REVISED.  Note: This CID’s page and number should be 36.30 as in CID85, because 36.45 is resolved in 11-23/1285 (i.e., 36.45 is removed). |

**Discussion**

There is only one AKM suite selector is defined for PASN (Table 9-151).

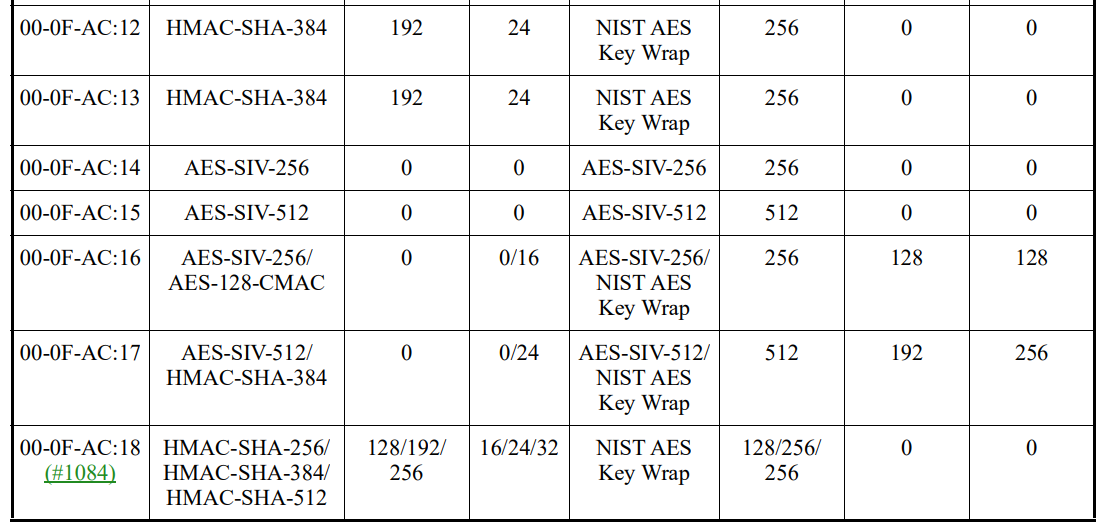
A table of key management selectors

Description automatically generated

Here are the integrity and key wrap algorithms (Table 12-11):

A table with numbers and text

Description automatically generated



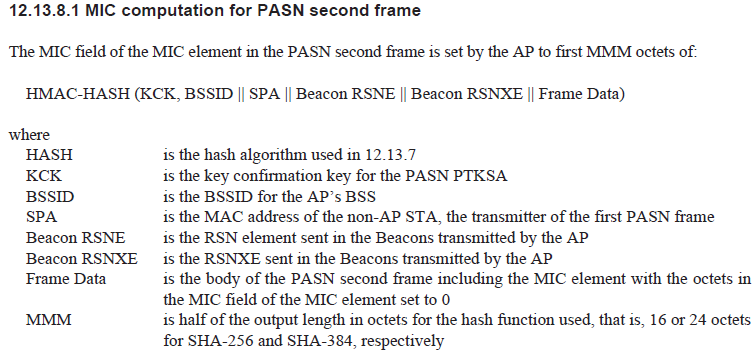
A white sheet with black text and numbers

Description automatically generated

Note that if we define a new integrity and key wrap algorithm for PASN (00-0F-AC:21), we only can define one algorithm because there is only one AKM suite selector for PASN (00-0F-AC:21). So, we have to choose single integrity and key wrap algorithms.

For integrity algorithm (MIC calculation), current IEEE Std 802.11az-2022 defines two integrity algorithm and MIC size for a fixed KCK length=256 bits:

* HMAC-SHA256 for 16 octets MIC (KCK=256bits)
* HMAC-SHA384 for 24 octets MIC (KCK=256bits)



A close up of text

Description automatically generated

A close up of a text

Description automatically generated

**For keywrap algorithm, there is currently no definition. This document proposes a fixed KEK (256 bits) for AES-SIV-256.**

**Proposed Changes (Baseline document is P802.11REVme\_D4.1)**

**1) CID84, CID212**

*Add the following rows in Table 12-11—Integrity and key wrap algorithms in* *12.7.3 EAPOL-Key PDU construction and processing as follows:*

***Table 12-11****—Integrity and key wrap algorithms*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *AKM* | *Integrity*  *algorithm* | *KCK\_bits* | *Size of*  *MIC*  *(octets)* | *Key wrap*  *algorithm* | *KEK\_bits* | *KCK2\_bits* | *KEK2\_bits* |
| 00-0F-AC:21 | HMAC-SHA256/ HMAC-SHA384 | *256 bits* | *16/24* | *AES-SIV-256* | *256* | *0* | *0* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

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

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.

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

where,

|  |  |
| --- | --- |
| PMK | is the pairwise master key for the Base AKMP if the AKMP is other than PASN AKMP; see 9.4.2.24.3. Otherwise, if the Base AKMP is PASN AKMP i.e. 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). |
| KDF-HASH-NNN | is the key derivation function defined in 12.7.1.6.2 using the hash algorithm defined for the Base AKMP; see Table 9-151. 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, KEK, TK and KDK depending on the pairwise cipher and whether a KEK and a KDK is derived. |
|  |  |

* Except when dot1IRMActivated is true or dot11DeviceIDActivated is true, PTK is composed of the Key Confirmation Key (KCK), Temporal Key (TK) and the Key Derivation Key (KDK) which are derived as follows (see Table 12-11—Integrity and key wrap algorithms):

KCK = L(PTK, 0, 256)

KCK is the first 256 bits of the PTK.

TK = L(PTK, 256, TK\_Length\_Bits)

TK is the transient key whose length is the same as a key for the pairwise cipher in RSNE provided by the AP in the second PASN frame This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets.

KDK = L(PTK, 256 + TK\_Length\_Bits, KDK\_bits)

The KDK is of bit length KDK\_bits which has the value 256 if a KDK is derived (see 12.7.1.3 (Pairwise Key Hierarchy)) or 0 otherwise.

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

The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from PASN authentication shall be 3 0.

* When dot1IRMActivated is true or dot11DeviceIDActivated is true, PTK is composed of the Key Confirmation Key (KCK), Key Encryption Key (KEK), Temporal Key (TK) and the Key Derivation Key (KDK) which are derived as follows (see Table 12-11—Integrity and key wrap algorithms):

KCK = L(PTK, 0, 256)

KCK is the first 256 bits of the PTK.

KEK = (PTK, 256, KEK\_Length\_Bits)

KEK is used to provide encryption for certain Information Elements (such as device ID Information Element and IRM Information Element) in PASN frames, as defined in 12.13.3.2 PASN frame construction and processing. Its length is 256 bits.

NOTE- KEK\_Length\_Bits is equal to KEK\_bits in Table 12-11—Integrity and key wrap algorithms).

TK = L(PTK, 256 + KEK\_Length\_Bits, TK\_Length\_Bits)

TK is the transient key whose length is the same as a key for the pairwise cipher in RSNE provided by the AP in the second PASN frame. This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets.

KDK = L(PTK, 256 + KEK\_Length\_Bits + TK\_Length\_Bits, KDK\_bits)

The KDK is of bit length KDK\_bits which has the value 256 if a KDK is derived (see 12.7.1.3 (Pairwise Key Hierarchy)) or 0 otherwise.

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

The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from PASN authentication shall be 3 0.

*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) with AES-SIV-256

To encrypt device ID element in PASN frame 2 or IRM element in PASN frame 3, KEK shall be used, as derived as part of PTK (see 12.13.7 PTKSA derivation with PASN authentication), with AES-SIV-256.

**2) CID85, CID283**

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:

*Change the following sentence in 12.13.3.2 PASN frame construction and processing (as amended by IEEE Std 802.11bh-D1.0) as follows:*

* 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 as defined in 12.2.11.3 (Encryption of Device ID IE and IRM IE in PASN)

**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:

*Change the following sentence in 12.13.3.2 PASN frame construction and processing (as amended by IEEE Std 802.11bh-D1.0) as follows:*

* 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 as defined in 12.2.11.3 (Encryption of Device ID IE and IRM IE in PASN)