IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| LB270 CR for CID 3753 |
| Date: 2023-1-24 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

 |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVme D2.0:

3753

**Revision History:**

R0: Initial version.

R1: Editorial fix based on comments received offline.

R2: Revision based on the discussion in the teleconference call

R3: Revision based on the discussion in the teleconference call

# CID 3753

|  |  |  |
| --- | --- | --- |
| **CID****Clause****Page.Line** | **Comment** | **Proposed Change** |
| 3753 | Table 12-11 and 12-12 needs to be combined to know the corresponding bits of KCK, KEK, and size of MIC. One clarification can be to expand table 12-12 to have 3 more columns to clarify the the size of correspoding KCK, KEK and size of MIC. Note that Table 2: Integrity and Key Wrap Algorithms in RFC 8110 lists all the corresponding size. | expand table 12-12 to have 3 more columns to clarify the the size of correspoding KCK, KEK and size of MIC. |

## Discussion:

In OWE RFC, the following table is provided to avoid any ambiguity rather than using “/”.



AKM 17 and AKM 18 specifically uses “/” with definition as shown below.

*For the 00-0F-AC:16 and 00-0F-AC:17 AKMs (FILS with FT), different keys and algorithms are used in EAPOL-Key frames and FT authentication sequence. These different cases are indicated in the table in <EAPOL-Key> / <FT authentication> format*

Propose to also have separate sentences for AKM 18, 24, 25.

In offline discussions two options are proposed to have separate sentences. Propose to have full description to provide full clarity.

Option 1: Full description below.

*Existing texts: For the 00-0F-AC:16 and 00-0F-AC:17 AKMs (FILS with FT), different keys and algorithms are used in EAPOL-Key frames and FT authentication sequence. These different cases are indicated in Table 12-11 (Integrity and key wrap algorithms) in <EAPOL-Key> / <FT authentication> format.*

For the 00-0F-AC:18 AKM, different keys and algorithms are used as defined in IETF RFC 8110 (Opportunistic Wireless Encryption) based on the selected hash algorithm. These different cases are indicated in Table 12-11 in <value when SHA-256 is used> / <value when SHA-384 is used> / <value when SHA-512 is used> format. For the 00-0F-AC:24 and 00-0F-AC:25 AKMs, different keys and algorithms are used based on the hash algorithm identified in 12.4.2 and Table 12-12. These different cases are indicated in Table 12-11 in <value when SHA-256 is used> / <value when SHA-384 is used> / <value when SHA-512 is used> format.

Option 2: Reduced description without mentioning AKM.

*Existing texts: For the 00-0F-AC:16 and 00-0F-AC:17 AKMs (FILS with FT), different keys and algorithms are used in EAPOL-Key frames and FT authentication sequence. These different cases are indicated in Table 12-11 (Integrity and key wrap algorithms) in <EAPOL-Key> / <FT authentication> format.*

For the other rows in Table 12-11 (Integrity and key wrap algorithms), the /-separated lists of options indicate keys and algorithms based on the selected hash algorithm, and each row shows the values for different keys and algorithms respective to the hash algorithm.

## Proposed Resolution: CID 3753

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for CID 3753 in 11-23/0156r3

## Proposed Text Update: CID 3753

*Instruction to TGme Editor: Update REVme D2.0 12.4 as shown below (track change on).*

* **EAPOL-Key PDU construction and processing**

EAPOL-Key frames are constructed and processed according to the negotiated AKM at association time. The negotiated AKM determines what algorithm is used to construct and verify a MIC, the size of the MIC, and the algorithm used to wrap and unwrap the Key Data field.

Table 12-11 (Integrity and key wrap algorithms) indicates the particular algorithms to use when constructing and processing EAPOL-Key frames and FT authentication sequence. The AKM of “Deprecated” indicates an AKM of 00-0F-AC:1 or 00-0F-AC:2 when either TKIP or “Use group cipher suite” is the negotiated pairwise cipher. For all other AKMs the negotiated pairwise cipher suite does not influence the algorithms used to process EAPOL-Key frames. For the 00-0F-AC:16 and 00-0F-AC:17 AKMs (FILS with FT), different keys and algorithms are used in EAPOL-Key frames and FT authentication sequence. These different cases are indicated in Table 12-11 (Integrity and key wrap algorithms) in <EAPOL-Key> / <FT authentication> format. For AKM 00-0F-AC:18, different keys and algorithms are used as defined in IETF RFC 8110 (Opportunistic Wireless Encryption) based on the selected hash algorithm. These different cases are indicated in Table 12-11 in <value when SHA-256 is used> / <value when SHA-384 is used> / <value when SHA-512 is used> format. For AKMs 00-0F-AC:24 and 00-0F-AC:25, different keys and algorithms are used based on the hash algorithm identified in 12.4.2 and Table 12-12. These different cases are indicated in Table 12-11 in <value when SHA-256 is used> / <value when SHA-384 is used> / <value when SHA-512 is used> format.

HMAC is defined in IETF RFC 2104. MD5 is defined in IETF RFC 1321. SHA-1 is defined by FIPS 180-4. The NIST AES key wrap algorithm is defined in IETF RFC 3394. AES-128-CMAC is defined by NIST Special Publication 800-38B and also found in IETF RFC 4493 [B43].

|  |
| --- |
| * **Integrity and key wrap algorithms**
 |
| **AKM** | **Integrity algorithm** | **KCK\_bits** | **Size of MIC** | **Key wrap algorithm** | **KEK\_bits** | **KCK2\_bits** | **KEK2\_bits** |
| Deprecated | HMAC-MD5 | 128 | 16 | ARC4 | 128 | 0 | 0 |
| 00-0F-AC:1 | HMAC-SHA-1-128 | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:2  | HMAC-SHA-1-128 | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:3 | AES-128-CMAC | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:4 | AES-128-CMAC | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:5 | AES-128-CMAC | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:6 | AES-128-CMAC | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:8 | AES-128-CMAC | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:9 | AES-128-CMAC | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:11 | HMAC-SHA-256 | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| 00-0F-AC:12 | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |
| 00-0F-AC:13 | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |
| 00-0F-AC:14 | AES-SIV-256 | 0 | 0 | AES-SIV-256 | 256 | 0 | 0 |
| 00-0F-AC:15 | AES-SIV-512 | 0 | 0 | AES-SIV-512 | 512 | 0 | 0 |
| 00-0F-AC:16 | AES-SIV-256/ AES-128-CMAC | 0 | 0/16 | AES-SIV-256/ NIST AES Key Wrap | 256 | 128 | 128 |
| 00-0F-AC:17 | AES-SIV-512/ HMAC-SHA-384 | 0 | 0/24 | AES-SIV-512/ NIST AES Key Wrap | 512 | 192 | 256 |
| 00-0F-AC:18(#1084) | HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 | 128/192/256 | 16/24/32 | NIST AES Key Wrap | 128/256/256 | 0 | 0 |
|  |
| 00-0F-AC:19(M20) | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |
| 00-0F-AC:20(M20) | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |
| 00-0F-AC:22(M20) | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |
| 00-0F-AC:23(M20) | HMAC-SHA-384 | 192 | 24 | NIST AES Key Wrap | 256 | 0 | 0 |
| 00-0F-AC:24(M21) | (M67)HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | (M67)128/192/256 | (M67)16/24/32 | NIST AES Key Wrap | (M67)128/256/256 | 0 | 0 |
|  |
| 00-0F-AC:25(M21) | (M67)HMAC-SHA-256/HMAC-SHA-384/HMAC-SHA-512 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | (M67)128/192/256 | (M67)16/24/32 | NIST AES Key Wrap | (M67)128/256/256 | 0 | 0 |

**Table 12-12** **Hash identified in SAE and integrity algorithm(M67)**

|  |  |
| --- | --- |
| **Hash identified in 12.4.2 (Assumptions on SAE)** | **Integrity algorithm** |
| SHA-256 | HMAC-SHA-256 |
| SHA-384 | HMAC-SHA-384 |
| SHA-512 | HMAC-SHA-512 |

…(existing texts)….