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.

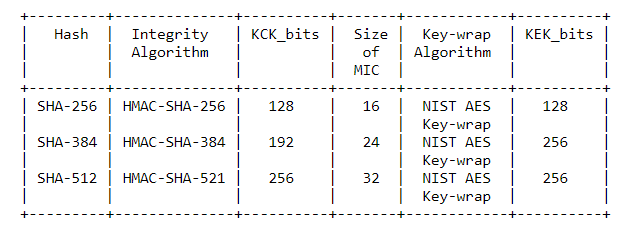
R1: Editorial fix based on comments received offline.

# 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. Propose to revise table 12-11 to have subcolumns to provide the same level of clarity.



Note we do not change AKM 17 and AKM 18 beucase “/” has other meanings for AKM 16 and 17.

*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*

## Proposed Resolution: CID 3753

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for CID 3753 in 11-23/0156r1

## 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**

…(existing texts)….

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| * **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 | 128 | 16 | NIST AES Key Wrap | 128 | 0 | 0 |
| HMAC-SHA-384 | 192 | 24 | 256 |
| HMAC-SHA-512 | 256 | 32 | 256 |
| 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 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | (M67)128 | (M67)16 | NIST AES Key Wrap | (M67)128 | 0 | 0 |
| (M67)HMAC-SHA-384 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | (M67)192 | (M67)24 | (M67)256 |
| (M67)HMAC-SHA-512 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | (M67)256 | (M67)32 | (M67)256 |
| 00-0F-AC:25(M21) | (M67)HMAC-SHA-256 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | (M67)128 | (M67)16 | NIST AES Key Wrap | (M67)128 | 0 | 0 |
| HMAC-SHA-384 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | 192 | 24 | 256 |
| HMAC-SHA-512 (see Table 12-12 (Hash identified in SAE and integrity algorithm(M67))) | 256 | 32 | 256 |

**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)….