IEEE P802.11
Wireless LANs

|  |
| --- |
| BIP-GMAC-256 |
| Date: 2013-05-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission adds GMAC-256 as a valid option for BIP and addresses CID 10140.

***Instruct the editor to request assignment of a new Suite type from the appropriate ANA repository, replace <ANA-1> below (in two places) with the newly assigned Suite type.***

***Instruct the editor to update Table 8-99 and Table 8-100 as indicated:***

 **Table 8-99—Cipher suite selectors**

|  |  |  |
| --- | --- | --- |
|  OUI |  Suite type |  Meaning |
| 00-0F-AC |  8 | GCMP-128 – default for a DMG STA |
| 00-0F-AC |  9  | GMCP-256 |
| 00-0F-AC |  10 | CCMP-256 |
| 00-0F-AC |  11 | BIP-GMAC-128 |
| 00-0F-AC |  12 | BIP-GMAC-256 |
| 00-0F-AC |  <ANA-1> | BIP-CMAC-256 |

|  |  |  |  |
| --- | --- | --- | --- |
|  Cipher Suite selector |  GTK |  PTK |  IGTK |
|  GCMP-128 |  Yes |  Yes |  No |
|  GCMP-256 |  Yes |  Yes |  No |
|  CCMP-256 |  Yes |  Yes |  No |
|  BIP-GMAC-128 |  No |  No |  Yes |
|  BIP-GMAC-126 |  No |  No |  Yes |
|  BIP-CMAC-256 |  No |  No |  Yes |

***Instruct the editor to update section 8.4.2.27.3 as indicated:***

**8.4.2.27.3 AKM suites**

The AKM suite selector value 00-0F-AC:11 shall only be used with cipher suite selector values 00-0F-AC:8 (GCMP-128) and 00-0F-AC:11 (BIP-GMAC-128). The AKM suite selector value 00-0F-AC:12 shall only be used with cipher suite selector values 00-0F-AC:9 (GCMP-256), 00-0F-AC:10 (CCMP-256), 00-0F-AC:<ANA-1> (BIP-CMAC-256), and 00-0FAC:12 (BIP-GMAC-256).

***Instruct the editor to modify section 8.4.2.57 as indicated:***

**8.4.2.57 Management MIC element**

The MIC field contains a message integrity code calculated over the robust management frame as specified in 11.4.4.5 and 11.4.4.6. The length of the MIC field depends on the specific cipher negotiated, either BIP (8 octets) or BIP-CMAC-256 (16 octets), or BIP-GMAC-128 (16 octets), or BIP-GMAC-256 (16 octets).

***Instruct the editor to modify section 11.4.4.5 as indicated:***

**11.4.4.5 BIP transmission**

1. Compute an integrity value over the concatenation of (AAD || Management Frame Body including MME), and insert the 64-bit output into the MME MIC field. For BIP, the integrity value is 64-bits and is computed using AES-128-CMAC; for BIP-CMAC-256, the integrity value is 128-bits and is computed using AES-256-CMAC; for BIP-GMAC-128, the integrity value is 128-bits and is computed using AES-128-GMAC; and, for BIP-GMAC-256, the integrity value is 128-bits and is computed using AES-256-GMAC.

***Instruct the editor to modify section 11.4.4.6 as indicated:***

**11.4.4.6 BIP reception**

When a STA with management frame protection negotiated receives a group addressed robust management

frame protected by BIP, BIP-CMAC-256, BIP-GMAC-128 or BIP-GMAC-256, it shall

1. Extract and save the received MIC value, and compute a verifier over the concatenation of (AAD || Management Frame Body || MME) with the MIC field masked to 0 in the MME. For BIP, the verifier is AES-128-CMAC; for BIP-CMAC-256, the verifier is AES-256-CMAC; for BIP-GMAC-128, the verifier is AES-128-GMAC; and, for BIP-GMAC-256, the verifier is AES-256-GMAC. If the result does not match the received MIC value, then the receiver shall discard the frame and increment the dot11RSNAStatsCMACICVErrors counter by 1.

***Instruct the editor to append the following row to Table 11-4:***

|  |  |  |
| --- | --- | --- |
|  Cipher suite |  Key length (octets) |  TK bits (bits) |
| BIP-CMAC-256 |  32 |  256 |

**References:**