IEEE P802.11
Wireless LANs

|  |
| --- |
| CCM resolution text |
| Date: 2014-07-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA/IAD | 7150 Moorland DriveClarksville, MD 21029 | +1 415 215 7733 | peter at akayla dot com |

Abstract

This submission proposes resolutions to CIDs 4073, 4922, 4939, and 4962.

***Update the modification to table 8-113 as indicated:***

|  |  |  |
| --- | --- | --- |
| OUI | Suite type | Meaning |
| Authentication type | Key management type | Key derivation type |
| 00-0F-AC | <ANA-> | FILS | FILS key management as defined in 11.11.2.2 (Key establishment with FILS authentication)using SHA256 and GCM-128 | Defined in 11.11.2 (FILS authentication protocol). |
| 00-0F-AC | <ANA-> | FILS | FILS key management as defined in 11.11.2.2 (Key establishment with FILS authentication) using SHA384 and GCM-256 | Defined in 11.11.2.3 (Key derivation with FILS authentication). |

***Update the modification to table 11-8 as indicated:***

|  |  |  |  |
| --- | --- | --- | --- |
| AKM | Integrity Algorithm | Size of MIC | Key-wrap algorithm |
| 00-0F-AC-<ANA-1> | AES-GCM-128 | 16 | AES-GCM-128 |
| 00-0F-AC-<ANA-1> | AES-GCM-256 | 16 | AES-GCM-256 |

***Modify the proposed text in the new clause 11.11.2.5 (page 114, lines 64-65) as indicated:***

AES-GCM-128 is used if the AKM is 00:0F-AC-<ANA-1> and AES-GCM-256 is used if the AKM is 00- 0F-AC-<ANA-2>.

* When the AEAD cipher mode used is GCM, the nonce, N, shall be set to the AEAD counter in the PTKSA as passed in the frame being protected.

Each successive invocation of the encryption operation of GCM shall increment the AEAD counter by one (1). Processing of a received EAPOL-Key frame shall include verification that the received frame contains a 11 counter that is strictly greater than the counter in the last received frame, and shall update its copy of the peer's AEAD counter in its PTKSA to the value of the AEAD counter in the received, and verified, frame.