IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment Resolution to cids for sec 11.11.2.3 to 11.11.2.7 |
| Date: 2013-12-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Rob Sun | Huawei Technology | Suite 400, 303 Terry Fox drive, Kanata, On | +1 613 2781948 | Rob.sun@huawei.com  |
|  |  |  |  |  |

Abstract

This document presents suggested proposal towards CID

2493, 2204, 2194, 3086, 3259, 2805, 2896, 2897, 2199, 3088, 3086, 2195, 3153, 3192, 2495, 2198, 2497, 2877, 2876, 3003, 3155, 3194, 3089, 2995, 2201, 2997, 2996, 2202, 3154, 3193, 3002, 2205, 2197, 3245, 3087, 3243, 2991, 2986, 2987, 3001

***Modify the following definition into 10.3.1 as highlighted in red texts:***

* STA authentication and association

***Discussion:***

Clause 11.11.2.3 to 11.11.2.7 outlines the procedures and key confirmation after the FILS authentication. Lots of the CIDs are related to the confusion of how to define the FILS key hierarchy and the length of the keys should be depending on the cipher suites selected. Also some of comments are regarding the definition of the PMKIDs which needs to be generated for the purpose of PMK management. Some CIDs are towards the problems of AEAD scheme which currently utilizes the static nonce.

Notes to Editor: modifiy section 11.11.2.3 to 11.11.2.7

**11.11.2.3 Key derivation with FILS authentication**

**[ CID 2493, 2204, 2205,2194,3086,3259,2805, 2896, 2897,3243,2986]**

 Key derivation with FILS Authentication generates 5 keys KCK2, KEK2, KCK, KEK and a temporal key (TK) respectively. The FILS key hierarchy follows the key structure specified in subclause 11.6.1.3. When the AKM for FILS (00-0F-AC:<ANA>) is selected, the length of the KEK2/KCK2 are 256 bits .

 The HKDF (RFC 5869) function shall be employed to generate the PMK. PMK 🡨 HKDF-256([ss]||rMSK, “PMK Generation from Shared Secret”, MAC\_a||MAC\_s)). [Note: 2197,2987]

The FILS PMKSA is managed and distributed as the PMKSA (section 11.5.1.1.2)

 Figure xx: FILS Key Hierarchy

The pairwise key hierarchy takes a PMK and generates a PTK. Then the PTK is partitioned into KCK2, KEK2 that are used to protectthe FILS association frame, the KCK, KEK that are used for the EAPoL key frame integrity protection and encryption, and the TK that is used for session encryption. Upon completion of the key derivation computation, the shared secret ss and rMSK, as applicable shall be irretrievably destroyed.

1. sNonce is the random or pseudorandom value contributed by the STA.
2. aNonce is the random or pseudorandom value contributed by the AP.
3. MAC\_s is the MAC address from the STA
4. MAC\_a is the MAC address from the AP
5. PMK is derived from rMSK and/or Shared Secret ss

PTK 🡨KDF-X ( PMK, “FILS PTK Generation”, Min(MAC\_s, MAC\_a)||Max(MAC\_s, MAC\_a)

||Min(sNonce,aNonce)|| Max(sNonce, aNonce))

Where X =1024+TK\_bits, the TK\_bits is the length of the keys of selected cipher suites. The Min and Max operations for IEEE 802 addresses are with the address converted to a positive integer treating the first transmitted octet as the most significant octet of the integer. The Min and Max operations for nonces are with the nonces treated as positive integers converted as specified in 8.2.2 (Conventions).

1. The KCK2 shall only be used with FILS key confirmation (see 11.11.2.4) and shall be computed as the first 256 bits of the PTK

 KCK2 <- L ( PTK,0, 256)

The KCK2 is ONLY used to protect the association request/response frames of the FILS authentication (Section 11.11.2.4)

1. The KEK2 shall shall only be used with FILS key confirmation (see 11.11.2.4) and shall be computed as the second 256 bits of the PTK:

 KEK2 <- L (PTK, 256,256)

The KEK2 is shall only be used to protect the association request/response frames of the FILS authentication (11.11.2.6 and 11.11.2.7)

 [Note: CID 3245]

1. The KCK and KEK are used to construct EAPOL-Key frames as described in section 11.6.3
2. The Temporal Key (TK) shall be computed as bits 1024 -> (1024+TK\_bits) of the PTK.

TK <- L(PTK, 1024, TK\_bits)

 The TK is used to protect data frames between the AP and STA.

 The value of the TK\_bits shall be dependent on the selected cipher suites for data frame encryption (, 128 or 256 bits for AES-CCMP and AES-GCMP )

1. A PMKID is computed as: [CID 2195,3153,3192,3001]

 PMKID = L(SHA-256( aNonce||sNonce||MAC\_a ||MAC\_s),0,128)

**11.11.2.4 Key confirmation with FILS authentication**

~~Key confirmation for FILS Authentication is an Association Request followed by an Association Response.~~ Key confirmation for FILS Authentication is carried over the Association Request and the Association Response. [CID 2495]

The Association Request and Association Response shall be protected using the KEK2 according to

11.11.2.6 and 11.11.2.7.

For FILS Authentication using a trusted third party, the Key Auth field of the Key Confirmation element of

the Association Request shall be:

~~Key-Auth = HMAC-SHA256(KCK2, NSTA | NAP | STA-MAC | AP-BSSID)~~.

Key-Auth = hashalg (KCK2, sNonce|| aNonce|| MAC\_s|| MAC\_a).

 Where hashalg is the HMAC version of the hash algorithm from the AKM negotiated during FILS authentication. (CID 2198)

For FILS Authentication without a trusted third party, the Key Auth field of the Key Confirmation element

in the Association Request shall contain a digital signature using the STA's private key, the specific construction of the digital signature depends on the crypto-system of the public/private key pair

~~Key-Auth = Sig-STA(gSTA | gAP | NSTA | NAP | STA-MAC | AP-BSSID)~~.

Key-Auth = Sig-STA(gSTA || gAP || sNonce ||aNonce || MAC\_s || MAC\_a).

.

For FILS Authentication using a trusted third party, the AP shall construct a verifier as follows:

~~Key-Auth' = HMAC-SHA256(KCK, NSTA | NAP | STA-MAC | AP-BSSID)~~

Key-Auth' = hashalg (KCK2, sNonce || aNonce | |MAC\_s || MAC\_a) [Note: 3087,2198]

For FILS authentication using a trusted third party, the Key Auth field of the Key Confirmation element in

the Association Response shall be:

~~Key-Auth = HMAC-SHA256(KCK2, NAP | NSTA | AP-BSSID | STA-MAC).~~

Key-Auth = hashalg (KCK2, aNonce|| sNonce|| MAC\_a|| MAC\_s)

For FILS Authentication without a trusted third party, the Key Auth field of the Key Confirmation element

in the Association Response shall contain a digital signature using the AP's private key, the specific construction

of the digital signature depends on the crypto-system of the public/private keypair:

~~Key-Auth = Sig-AP(gAP | gSTA | NAP | NSTA | AP-BSSID | STA-MAC ).~~

Key-Auth = Sig-STA(gAP || gSTA || aNonce || sNonce || MAC\_a | |MAC\_s)

The STA shall process the received 802.11 Association Response frame as follows:

— The input key shall be the KEK2

— The input ciphertext shall be the contents of the Association Response frame that follow the FILS

Session element

— The input AAD shall be:

a) The AP BSSID

b) The STA MAC

c) The AP's nonce

d) The STA's nonce

e) The contents of the Association Response frame from the capability (inclusive) to the FILS

Session element (inclusive)

— The input keys, the tag, the ciphertext, and the AAD shall be passed to the decrypt-and-verify operation

specified in 11.11.2.6.

If the output from 11.11.2.6 returns failure, authentication shall be deemed a failure. If the output returns

plaintext, the Key-Auth from the decrypted Authentication frame shall be checked. If it is incorrect, authentication

shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK, KEK, and

TK shall be irretrievably destroyed. If authentication is not deemed a failure, the ~~AP~~ STA [CID 2876] shall check the Key-Auth field in the Key Confirmation element.

For FILS Authentication using a trusted third party, the STA shall construct a verifier as follows:

~~Key-Auth' = HMAC-SHA256(KCK2, NAP | NSTA | AP-BSSID | STA-MAC).~~

Key-Auth' = hashalg (KCK2, aNonce || sNonce | |MAC\_a | MAC\_s),

**11.11.2.5 AEAD scheme [CID: 2877, 3003, 3155, 3194, 2995]**

The authenticated encryption with associated data scheme to be used shall be the negotiated cipher indicated by the cipher suite in the FILS Association Request and Response frames. ~~Currently, the only such scheme specified~~

~~is~~ For the AES-CCM mode of operation, which is the CCM scheme specified in NIST SP 800-38C, Appendix

A, ~~with~~ use the following instantiation:

— The block cipher shall be AES-~~CCM~~-~~128~~ (see FIPS Pub 197);

--- The key length shall be 256 bits

— The parameter t, q, n and shall be set to t=16, q=2, and n=13.

**11.11.2.6 Encrypt and authenticate operation for FILS association frames**

The AKM scheme of 11.11.2.5 shall be used with the 802.11 Associate Request frame (for deciphering byAP) or with the 802.11 Association Response frame (for deciphering by STA), with the following instantiation:

— The key *K* shall be set to KEK2;

—~~The associated data string A shall be set to the AAD~~ ,The AAD shall be constructed as per 11.11.2.4 [CID 2997 ,2996]

— The string *P* shall be set to the plaintext;

— The nonce *N* shall be set to

a) For processing by STA: When the AKM is (OUI: 00-0F-AC:<ANA>) use the 13-octet all-zero bit string and incremented by 1 in each FILS association frame transmission

b) For processing by AP: When the AKM is (OUI: 00-0F-AC:<ANA>) use the 13-octet all-one bit string and decremented by 1 in each FILS association frame transmission [CID 2202, 3154,3193,3002, 3089]

**11.11.2.7 Decrypt and verify operation for FILS association frames**

The AEAD scheme of 11.11.2.5 shall be used with the 802.11 Associate Request frame (for deciphering by

STA) or with the 802.11 Associate Response frame (for deciphering by AP), with the following instantiation:

— The key K shall be set to KEK2;

—~~The associated data string A shall be set to the AAD;~~The AAD should be constructed as per 11.11.2.4

— The string C shall be set to the ciphertext;

— The nonce N shall be set to

 a) For processing by AP: When the AKM is (OUI: 00-0F-AC:<ANA>) use the 13-octet all-zero bit string and increment by 1 in each FILS association frame transmission

 b) For processing by STA: When the AKM is (OUI: 00-0F-AC:<ANA>)) use the 13-octet all- one bit string and decrement by 1 in each Fils association frame transmission

[CID ,2202, 3154,3193,3002]

Note to Editor: Please modify the table 8-101- AKM suite selectors in section 8.4.2.24.3

|  |  |  |
| --- | --- | --- |
| OUI | Suite type |  Meaning |
| Authentication Type  | Key Management type | Key derivation type |
| 00-0F-AC |  ANA | FILS Authentication with AEAD schemes as AES-CCM (256bits) and Hash algorithms as SHA384  | FILS key management defined in 11.11.2.5  | Defined in 11.11.2.3 |
|  |  |  |  |  |
|  |  |  |  |  |