IEEE P802.11
Wireless LANs

|  |
| --- |
| AES-CCM Mode to be Used wtih FILS Association frames |
| Date: 2012-11-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON | +1 415 690-7363+1 647 867-5658Skype: rstruik | rstruik.ext@gmail.com |

Abstract

This submission proposes to use the AES-CCM mode of operation as the authenticated encryption and authentication mode to be used with the Association frames for the FILS AEAD mode for Association frames as defined in 12/1045r6. This well-understood mode of operation is standardized with NIST SP 800-38C and has been used with IEEE 802 standards, including 802.11, since 2003 and is widely used elsewhere as well.

***Instruct the editor to modify the specification text in 12/1045r6 as follows:***

***Modify section 11.9a.2.3 as follows:***

**11.9a.2.3 Key Derivation with FILS Authentication**

Key derivation with FILS Authentication uses the KDF from section 11.6.1.7.2 to produce three keys, a key encryption key (KEK), a confirmation key (KCK), and a traffic key (TK). The inputs to the KDF are the two 16 octet nonces produced by the STA and AP, a constant label, the ERP secret result if a TTP is being used, and, the Diffie-Hellman shared secret, *ss*, if PFS is being used. The length of the KEK ~~and KMK~~ shall be 128 bits, and the KCK shall be 256 bits, and therefore the output from the KDF shall be ~~512~~ 384+TK\_bits, where TK\_bits is determined from table 11-4.

KEK | KMK | KCK | TK = KDF-X(NSTA | NAP, “FILS KECK PTK Derivation”, [rMSK][ | *ss*])

Where X is ~~512~~ 384+TK\_bits from table 11-4, rMSK is the output of the ERP exchange if a trusted third party was used, and *ss* is the shared secret resulting from the Diffie-Hellman exchange if PFS was used. The KEK ~~and KMK~~ shall be used with the encrypt-and-authenticate (see 11.9a.2.5) and decrypt-and-verify (see 11.9a.2.6) functions.

***Replace sections 11.9a.2.5 and 11.9a.2.6 by sections 11.9a.2.5, 11.9a.2.6 and add a section 11.9a.2.7, as follows:***

**11.9a.2.5 AEAD scheme**

The authenticated encryption with associated data scheme to be used shall be the AES-CCM mode of operation, which is the CCM scheme specified in NIST SP 800-38C, Appendix A, with the following instantiation:

* + The block cipher shall be AES-128 (see FIPS Pub 197);
	+ The parameter *t*, *q*, *n* and shall be set to *t*=16, *q*=16, and *n*=13.

**11.9a.2.6 Encrypt and Authenticate operation for FILS Association frames**

The AEAD scheme of 11.9a.2.5 shall be used with the 802.11 Associate Request frame (for enciphering by STA) or with the 802.11 Associate Response frame (for enciphering by AP), with the following instantiation:

* The key *K* shall be set to KEK (see 11.9a.2.3b);
* The associated data string *A* shall be set to the string AAD;
* The string *P* shall be set to the plaintext;
* The nonce *N* shall be set to

a) For processing by STA: use the 13-octet all-zero string;

b) For processing by AP: use the 13-octet all-one string.

The function shall output the string *C* as ciphertext.

**11.9a.2.7 Decrypt and Verify operation for FILS Association frames**

The AEAD scheme of 11.9a.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 shall be the KEK (see 11.9a.2.3b);
* The associated data string *A* shall be set to the AAD;
* The string C shall be set to the ciphertext;
* The nonce *N* shall be set to

a) For processing by AP: use the 13-octet all-zero string.

b) For processing by STA: use the *13*-octet all-one string;

The function shall output the payload string *P* as the plaintext if the decryption –verification process is successful and shall output a failure otherwise.

**Motion-1:** To authorize the Editor to incorporate the text changes proposed in contribution 12/1385r0 (*11-12-1385-00-00ai-fils-AEAD-mode-of-operation*) to the relevant portions of 12/1045r6 incorporated with the draft TGai Draft Specification Document.

Yes: \_\_\_\_\_\_\_\_\_\_\_\_; No: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; Abstain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_