IEEE P802.11
Wireless LANs

|  |
| --- |
| Use SIV Instead |
| Date: 2013-07-15 |
| 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 addresses CIDs 1006 and 1334 and also cleans up two errors that everyone missed during review.

### 11.11.1 Assumptions on FILS authentication

The security of FILS authentication depends on the following assumptions:

* Communication between the STAs and the trusted third party, when applicable, is protected with a secure deterministic authenticated encryption function.
* When using a TTP, each STA shares a symmetric key (or keys) with the trusted third party that is (are) capable of being used with ERP; when not using a TTP, each STA shall have a means to trust the public key of the other STA.
* When PFS is used, a finite cyclic group is negotiated for which solving the discrete logarithm problem is computationally infeasible.
* When PFS is used, both the STA and AP have at least one finite cyclic group from the dot11RSNAConfigDLCGroupTable in common.

All FILS Association frames shall be encrypted and authenticated (see 11.11.2.5).

### 11.11.2.3 Key derivation with FILS authentication

The KCK2 shall only be used with key confirmation (see 11.11.2.4). The KEK2 shall only be used with the encrypt-and-authenticate and decrypt-and-verify functions (see 11.11.2.5). Both keys KCK2 and KEK2 are temporary keys shall only be used during the FILS authentication protocol.

### *Instruct the editor to modify section 11.11.2.4 as indicated:*

### 11.11.2.4 Key confirmation with FILS authentication

Key confirmation for FILS Authentication is an Associate Request followed by an Associate Response. The Association Request and Association Response shall be protected using the KEK2 according to 11.11.2.5.

If the output from 11.11.2.6 returns a failure, authentication shall be deemed a failure. If the output returns plaintext, the Key-Auth from the decrypted Association 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 shall check the Key-Auth field in the Key Confirmation element.

The received 802.11 Association Request frame shall be processed as follows:

* The input key shall be the KEK2
* The input ciphertext shall be the contents of the Association Request frame that follow the FILS Session element
* The input AAD shall be:
1. The STA MAC
2. The AP BSSID
3. The STA's nonce
4. The AP's nonce
5. The contents of the Association Request frame from the capability (inclusive) to the FILS Session element (inclusive)
* The input keys, the ciphertext, and the AAD shall be passed to the decrypt-and-verify operation specified in 11.11.2.5.

If the output from 11.11.2.5 returns a failure, authentication shall be deemed a failure. If the output returns plaintext, the Key-Auth from the decrypted Association 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 shall check the Key-Auth field in the Key Confirmation element.

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

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

If Key-Auth' differs from the Key-Auth field in the Key Confirmation element, authentication shall be deemed a failure.

The 802.11 Association Response frame shall be protected as follows:

* The input keys shall be the KEK2
* The input plaintext shall be the contents of the Association Responseframe 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)

***Instruct the editor to modify sections 11.11.2.5, 11.11.2.6 and 11.11.2.7 as indicated:***

### 11.11.2.5 AEAD scheme

AES-SIV in its deterministic authenticated encryption mode, as specified in RFC 5297, shall be used as the AEAD scheme for FILS. Individual components of the AAD shall be expressed as separate input vectors. The keylength used by AES-SIV shall be the length of the KEK2.

The SIV encrypt operation shall be used to encrypt and authenticate FILS frames and the SIV Decrypt operation shall be used to decrypt and verify FILS frames.

**References:**