IEEE P802.11
Wireless LANs

|  |
| --- |
| An Authenticated Enryption Scheme for FILS Authentication |
| Date: 2012-11-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission proposes a scheme to perform authenticated encryption of the IEs that comprise a FILS Association frames. The proposed scheme is a composite authenticated encryption scheme comprised of NIST-approved cipher modes, notably AES-CMAC and AES-CTR. Two levels of security are provided.

***Modify table 8-22 from section 8.3.3.5 as indicated:***

|  |
| --- |
| Table 8-22—Association Request frame body |
| Order | Information | Notes |
| 8 | FILS session | The FS IE is an identifier for the FILS session  |
|  |  |  |
| 9 | FILS Public Key | An IE that contains a (certified) public key. Present if a TTP is not used for FILS Authentication. |
| 10 | FILS Key Confirmation | A field that performs a cryptographic proof of authentication for the FILS Authentication protocol. Present if FILS authentication is used. |
| Last | Vendor Specific | One or more vendor-specific (#1684)elements are optionally present(#29). These (#1684)elements follow all other (#1684)elements(#1221). |

***Modify table 8-23 in section 8.3.3.6 as indicated:***

|  |
| --- |
| Table 8-23—Association Response frame body |
| Order | Information | Notes |
| 6 | FILS session | The FS IE is an identifier for the FILS session  |
|  |  |  |
| 7 | FILS Public Key | An IE that contains a (certified) public key. Present if a TTP is not used for FILS Authentication. |
| 8 | FILS Key Confirmation | A field that performs a cryptographic proof of authentication for the FILS Authentication protocol |
| 9 | FILS KDE Container | A field that contains the KDE information. |
| Last | Vendor Specific | One or more vendor-specific (#1684)elements are optionally present(#29). These (#1684)elements follow all other (#1684)elements(#1221). |

***Modify table 8-101 from section 8.4.2.27.3 as indicated and increment the <ANA-XXX> numbers following this change in the draft.***

|  |
| --- |
| * Table 8-101-- AKM suite selectors
 |
| OUI | Suite type | Meaning |
| Authentication type | Key management type | Key derivation type (11w) |
| 00-0F-AC | <ANA-12> | FILS-128 | FILS key management as defined in 11.9a  | Defined in 11.9.a |
| 00-0F-AC | <ANA-13> | FILS-256 | FILS key management as defined in 11.9a | Defined in 11.9a |
| 00-0F-AC | <ANA-13 > +1 –255  | Reserved | Reserved | Reserved |
| Vendor OUI | Any | Vendor-specific | Vendor-specific | Vendor-specific |
| Other | Any | Reserved | Reserved | Reserved |

***Instruct the editor to remove section 8.4.2.121d and change subsequent sections “e”, “f” to “d”, “e”***

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |

***Modify section 11.9a.1 as indicated:***

**11.9a.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 authenticatedusing AES-SIV in deterministic authenticated encryption mode from RFC 5297. AES-SIV-256 and AES-SIV-512 shall be supported.

For the purposes of interoperability, when negotiating <ANA-12>, FILS-128, with PFS conformant STAs shall support group nineteen (19), an ECC group defined over a 256-bit prime; and when negotiating <ANA-13>, FILS-256, with PFS conformant STAs shall support group twenty (20), an ECC group defined over a 384-bit prime.

***Modify Table 11-9 in section 11.6.3 as indicated:***

**11.6.3 EAPOL-Key frame construction and processing**

|  |  |  |  |
| --- | --- | --- | --- |
|  AKM |  Integrity Algorithm |  Size of MIC | Key Wrap Algorithm |
| 00-0F-AC:6 | AES-128-CMAC |  16 |  AES Key Wrap |
| <ANA-12> |  SIV-256 |  16 |  SIV-256  |
| <ANA-13> |  SIV-512 |  16 |  SIV-512 |

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

**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 the KCK depend on the FILS AKM negotiated. For <ANA-12>, FILS-128, the KEK shall be 256 bits and the KCK shall be 256 bits., therefore the output from the KDF shall be 512+TK\_bits, where TK\_bits is determined from table 11-4. For <ANA-13>, FILS-256, the KEK shall be 512 bits and the KCK shall be 384 bits, therefore the output from the KDF shall be 896+TK\_bits, where TK\_bits is determined from table 11-4.

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

Where X is 512+TK\_bits from table 11-4 when the AKM is <ANA-12>, and X is 896+TK\_bits from table 11-4 when the AKM is <ANA-13>, 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 If a trusted third party was used, the rMSK shall be irretrievably destroyed upon completion of key derivation; if PFS was employed the shared secret, *ss*, shall be irretrievably destroyed upon completion of key derivation.

***Modify section 11.9a.2.4 as indicated:***

**11.9a.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 KEK and KMK according to section 11.9a.2.5 and 11.9a.2.6.

Upon the completion of key establishment (11.9a.2.2) and key derivation (11.9a.2.3) the STA shall construct a nascent 802.11 associate request frame indicating its selected ciphersuite and the FILS AKM, and the FILS Key Confirmation element. The content of the Key Auth field of the Key Confirmation element depends on the type of FILS authentication.

The AP transfers any necessary KDEs to the STA in the Association Response frame. The AP may include one or more KDEs using the FILS KDE container. The format and the rules for transferring the KDE shall follow section 11.6.2 (EAPOL Key Frames).

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-SHA-K(KCK, NSTA | NAP | STA-MAC | AP-BSSID)

Where SHA-K is SHA-256 for AKM <ANA-12>, FILS-128, and SHA- is SHA-384 for AKM <ANA-13>, FILS 256. 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)

Where Sig-STA indicates a digital signature using the STA’s private key, gSTA is the octet-string representation of the STA’s public Diffie-Hellman value, gAP is the octet-string representation of the AP’s public Diffie-Hellman value, NSTA is the nonce selected by the STA, and NAP is the nonce selected by the AP.

The 802.11 Association Request frame shall be secured as follows:

* The input key shall be the KEK
* The input plaintext shall be the contents of the Association Request frame that follow the FILS Key Confirmation element
* The input AAD shall be a vector of the following components in order:
	+ 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 Key Confirmationelement (exclusive)
* The input keys, the plaintext, and the vector of AAD shall be passed to AES-SIV encrypt
* The output ciphertext from AES-SIV encrypt shall become the remainder of the Association Request frame that follows the FILS Key Confirmation element.

The resulting 802.11 Association Request frame shall be transmitted to the AP.

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

* The input key shall be the KEK
* The input ciphertext shall be the contents of the Association Request frame that follow the FILS Key Confirmation element
* The input AAD shall be a vector of the following components in order:
	+ 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 Key Confirmation element (exclusive)
* The input keys, the ciphertext, and the vector of AAD shall be passed to AES-SIV decrypt

If the output from AES-SIV decryptreturns a 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 KEK, KCK, TK, and all shared secrets 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-SHA-K(KCK, NSTA | NAP | STA-MAC | AP-BSSID)

Where SHA-K is SHA-256 for AKM <ANA-12>, FILS-128, and SHA- is SHA-384 for AKM <ANA-13>, FILS 256. If Key-Auth’ differs from the Key-Auth field in the Key Confirmation element, authentication shall be deemed a failure.

For FILS Authentication without a trusted third party, the AP shall use the STA’s (certified) public key from the Public Key IE in the Association frame to verify the contents of the Key-Auth field of the Key Confirmation element. The specific technique for verification depends on the crypto-system used by the public key. If verification fails, authentication shall be deemed a failure.

If authentication is a failure, the KEK,KCK, TK, and all shared secrets shall be irretrievably destroyed. Otherwise, the AP shall then construct a nascent 802.11 associate response frame confirming the selected ciphersuite and the FILS AKM, and containing the FILS KDE Container, and its own Key-Auth.

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-SHA-K(KCK, NAP | NSTA | AP-BSSID | STA-MAC)

Where SHA-K is SHA-256 for AKM <ANA-12>, FILS-128, and SHA- is SHA-384 for AKM <ANA-13>, FILS 256. 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 )

Where Sig-AP indicates a digital signature using the AP’s private key, and where gSTA, gAP, NSTA, and NAP are the same as in the construction of the Association Request.

The 802.11 Association Response frame shall be protected as follows:

* The input key shall be the KEK
* The input plaintext shall be the contents of the Association Request frame that follow the FILS Key Confirmationelement
* The input AAD shall be a vector of the following components in order:
	+ 1. The AP BSSID
		2. The STA MAC
		3. The AP’s nonce
		4. The STA’s nonce
		5. The contents of the Association Response frame from the capability (inclusive) to the FILS Key Confirmationelement (exclusive)
* The input keys, the plaintext, and the vector of AAD shall be passed to AES-SIV encrypt
* The output ciphertext shall become the remainder of the Association Response frame that follows the FILS Key Confirmation element.

The resulting 802.11 Association Response frame shall be transmitted to the STA.

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

* The input key shall be the KEK
* The input ciphertext shall be the contents of the Association Response frame that follow the FILS Key Confirmationelement
* The input AAD shall be a vector of the following components in order:
	+ 1. The AP BSSID
		2. The STA MAC
		3. The AP’s nonce
		4. The STA’s nonce
		5. The contents of the Association Response frame from the capability (inclusive) to the FILS Key Confirmationelement (exclusive)
* The input keys, the ciphertext, and the vector of AAD shall be passed to AES-SIV decrypt

If the AES-SIV decryptreturns 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 KEK, KCK, PMK, and all shared secrets 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 STA shall construct a verifier as follows:

 Key-Auth’ = HMAC-SHA-K(KCK, NAP | NSTA | AP-BSSID | STA-MAC)

Where SHA-K is SHA-256 for AKM <ANA-12>, FILS-128, and SHA- is SHA-384 for AKM <ANA-13>, FILS 256. If Key-Auth’ differs from the Key-Auth field in the Key Confirmation element, authentication shall be deemed a failure .

For FILS Authentication without a trusted third party, the STA shall use the AP’s (certified) public key from the Public Key IE in the Association frame to verify the contents of the Key-Auth field of the Key Confirmation element. The specific technique for verification depends on the crypto-system used by the public key. If verification fails, authentication shall be deemed a failure.

***Instruct the editor to delete sections 11.9a.2.5 and 11.9a.2.6***

**References:**