IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of Some Security Comments | | | | |
| Date: 2013-10-05 | | | | |
| 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 proposes resolutions to CIDs 2021, 2151, 2193, 2206, 2249, 2268, 2270, 2394, 2449, 2576, 2585, 2586, 2587, 2721, 2797, 2800, 2801, 2810, 2923, 2981, 3015, 3020, 3021, 3022, 3023, 3024, 3025, 3159, 3160, 3263, 3264, 3273, 3274, 3277.

***Instruct the editor to modify section 4.5.4.2 as indicated:***

**4.5.4.2 Authentication**

IEEE Std 802.11 defines five [CID #1279, 1335, 1399 ~~four~~ 802.11 authentication methods: Open System authentication, Shared Key authentication, FT authentication, ~~and~~ simultaneous authentication of equals (SAE), and **fast initial link setup (**FILS) authentication. Open System authentication admits any STA to the DS. Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key. FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 12 (Fast BSS transition). SAE authentication uses finite field cryptography to prove knowledge of a shared password. FILS authentication uses either trusted public keys or a shared key derived out-of-band. The IEEE Std 802.11 authentication mechanism also allows definition of new authentication methods.

***Instruct the editor to modify section 4.5.4.3 as indicated:***

**4.5.4.3 Deauthentication**

In an RSNA, deauthentication also destroys any related pairwise transient key security association (PTKSA), group temporal key security association (GTKSA), station-to-station link (STSL) master key security association (SMKSA), STSL transient key security association (STKSA), and integrity group temporal key security association (IGTKSA) that exist in the STA andcloses the associated IEEE Std 802.1X Controlled Port, if one exists. If pairwise master key (PMK) caching is not enabled, deauthentication also destroys the pairwise master key security association (PMKSA) from which the deleted PTKSA was derived.

***Instruct the editor to modify section 4.10.3.6 as indicated:***

**4.10.3.6 AKM operations using FILS shared key authentication**

The following operations (see Figure 4-21a (FILS authentication)) are carried out when FILS shared key authentication:

1. The STA sends an Association Request frame to the AP and receives an Association Response frame from the AP. This exchange provides proof-of-possession of the PMK and enables the creation of a PTKSA.

***Instruct the editor to modify section 4.10.3.7 as indicated:***

**4.10.3.7 AKM operations using FILS public key authentication**

It is assumed that both STAs and APs using FILS have obtained a public key certificate from a certificatation authority (CA) and that they are capable of verifying each other’s certificate during execution of FILS authentication. The manner by which these certificates are obtained is outside the scope of this standard.

The following operations are carried out when performing FILS public key authentication:

1. If a STAdetermines that an AP supports FILS authentication (through active or passive scanning) it may initiate FILS authentication

***In 6.3.5.2.2, instruct the editor to change “ILSUserPriority” to”FILSUserPriority” in the MLME-AUTHENTICATE.request() and to modify the additional rows added to the table as indicated:***

**6.3.5.2.2 Semantics of the service primitive**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| FILSUserPriority | Enumeration | NO\_DATA\_TRAFFIC, LOW\_PRIORITY\_TRAFFIC,  HIGH\_PRIORITY\_TRAFFIC | Specifics of the type of traffic for a device to transmit. This parameter is present if dot11FILSActivated is true. |
| FILSWrappedData | Sequence of elements and fields | As defined in 8.4.2.188(FILSSecure Container element) | Used for the STA and AP to communicate data used by the FILS authentication algorithm. This parameter is present if dot11FILSActivated is true. |

***Instruct the editor to modify section 6.3.5.3.2 as indicated:***

***6.3.5.3.2 Semantics of the service primitive***

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| FILSWrappedData | Sequence of elements and fields | As defined in 8.4.2.188(FILS Seccure Container element ) | Used for the STA and AP to communicate data used by the FILS authentication algorithm. This parameter is present if dot11FILSActivated is true. |

***Instruct the editor to modify section 6.3.7.3.2 as indicated:***

***6.3.7.3.2 Semantics of the service primitive***

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Valid range | Description |
| FILSWrappedData | Sequence of elements and fields | As defined in 8.4.2.188 (FILS Secure Container element ) | Used for the STA and AP to communicate data used by the FILS authentication algorithm. This parameter is present if dot11FILSActivated is true. |

***Instruct the editor to modify table 8-22 in section 8.3.3.5 as indicated:***

**8.3.3.5 Association Request frame format**

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| 9 | FILS Public Key | An IE that contains a (certified) public key. Present if a FILS public key authentication is used. Included if dot11FILSActivated is True. |

***Instruct the editor to modify table 8-29 in section 8.3.3.11 as indicated:***

**8.3.3.11 Authentication frame format**

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication algorithm | Authentication transaction sequence no. | Status Code | Presence of fields 4-20 |
| FILS | 1 | Status | FILS Identity is present  FILS Authentication type is present  FILS Nonce is present  FILS Wrapped Data is present if FILS shared key authentication is used  Finite cyclic group is present if FILSAuthentication type field indicates PFS or if FILS public key authentication is used.  Element is present if FILS Authentication type field indicates PFS or if FILS public key authentication is used. |
| FILS | 2 | Status | FILS Identity is present if Status is zero  FILS Authentication type is present if Status is zero  FILS Nonce is present if Status is zero.  FILS Wrapped Data is present if Status is zero and FILS shared key authentication is used.  Finite cyclic group is rpesent if FILSAuthentication type indicates PFS or if FILS public key authentication is used.  Element is present if FILS Authentication type field indicates PFS or if FILS public key authentication is used. |

***Instruct the editor to move table 8-53m into section 8.4.1.53 and modify it as indicated:***

|  |  |
| --- | --- |
| Value | Description |
| 0 | The FILS authentication exchange using a shared key andwithout PFS. |
| 1 | The FILS authentication exchange using a shared key andwith PFS. |
| 2 | The FILS authentication exchange using a public key |
| 3-255 | Reserved |

***Instruct the editor to modify section 8.4.2.185 as indicated:***

**8.4.2.185 FILS indication element**

When the FILS shared key authentication is used (with or without PFS), information on IP address type is carried in the domain information fields. With FILS public key authentication, the IP address type information is carried in B2 to B4.

***Instruct the editor to modify section 8.4.2.189 as indicated:***

**8.4.2.189 Fragment element**

Each Information element is limted to a maximum of 255 octets since the length field is a single octet (see Figure 8-104).

***Instruct the editor to add another row to table 8-183ak with Element set to “FILS Secure Container” and Element ID set to “<ANA>”.***

***Instruct the editor to modify section 8.4.2.189.2 as indicated:***

**8.4.2.189.2 Reassembly of Data**

Fragment IEs that: 1) are not the first Fragment IE; 2) do not follow another Fragment IE; or 3) that fragment an IE which is not listed in Table 8-18ak (IEs that may be fragmented) shall be ignored.

***Instruct the editor to modify section 10.44.4 as indicated:***

**10.44.4 FILS Indication element**

When FILS Shared key authenticaitonis used, an AP can indicate up to 7 realms that the AP is connected to using the hashed domain name field of the Domain Information field of the FILS Indication element.

***Instruct the editor to modify section 11.5.1.3.2 as indicated:***

**11.5.1.3.2 Security association in an ESS**

1. The last step is key management. The authentication process, whether SAE authentication or FILS authentication utilizing IEEE 802.11 authentication frames or IEEE 802.1X authentication utilizing data frames post association, creates cryptographic keys shared between the cryptographic endpoints-the AP and STA, or the IEEE 802.1X AS and the STA, when using SAE/FILS or IEEE 802.1X, respectively. When using IEEE 802.1X the AS transfers these keys to the AP, and the AP and STA uses one of the key confirmation handshakes, e.g., the 4-Way Handshake or FT 4-Way Handshake, to complete security association establishment. When using SAE authentication there is no AS and therefore no key transfer; the 4-way Handshake is performed directly between the AP and STA. The key confirmation handshake indicates when the link has been secured by the keys and is ready to allow normal data traffic and protected robust management frames. When FILS authentication is performed, the key confirmation is performed as part of the FILS exchange using association frames. Hence, no additional handshake is necessary.

* In the case of FILS authentication, the STA repeats the same actions as for initial contact and authentication. Note that a STA can take advantage of the fact that it can initiate FILS authentication to multiple APs while maintaining a single association with one AP, and finish the FILS authentication with one AP.

***Instruct editor to modify section 11.11 as indicated:***

**11.11 Authentication for Fast Initial Link setup**

The FILS Authentication protocol authenticates STAs to each other, using either a shared key or a public key. When shared key authenticaitonis used the authentication exchange can optionally be performed with PFS. When public key authentication is used, PFS shall be used. When the FILS authentication protocol is performed with PFS, the STA and AP derive ephemeral public and private keys with respect to a particular set of domain parameters that define a finite cyclic group and then exchange public keys. The result of the FILS Authentication protocol is a PTKSA. FILS Authentication is an RSNA authentication protocol.

***Instruct the editor to modify section 11.11.1 as indicated:***

**11.11.1 Assumptions on FILS authentication**

* When usingshared key authentication, each STA shares a valid rRK as defined in IETF RFC 5295 & IETF RFC 6696 with a trusted third party that is capable of being used with EAP-RP; when usingpublic key authentiation, each STA shall have a means to trust the public key of the other STA.

***Instruct the editor to modify section 11.11.2 as indicated:***

**11.11.2 FILS authentication protocol**

When a shared keyis used for FILS authentication, then EAP-RP as defined in [IETF RFC 5295/6696] shall be used.

***Instruct the editor to modify section 11.11.2.1 as indicated:***

**11.11.2.1 Discovery with FILS authentication**

When shared key authenticationis used, AP may advertise up to seven realms using a 2 octet hashed domain name of the domain information of FILS Indication IE in Beacon, Probe Response and FILS Discovery frames.

***Instruct the editor to modify section 11.11.2.2 as indicated:***

**11.11.2.2 Key establishment with FILS authentication**

A FILS-capable STA and AP establish a shared key by exchanging Authentication frames. The specific contents

of the Authentication frame depend on the particular authentication technique-whether shared key authentication or public key authentication is beingused-and whether PFS is obtained in the exchange or not.

***Instruct the editor to modify section 11.11.2.2.1 as indicated:***

**11.11.2.2.1 Key establishment with FILS shared key authentication**

STA may initiate FILS authentication with a FILS capable AP that is connected to a trusted third party authentication server that shares a valid shared key, called an rRK as defined in [IETF RFC 6696], with the STA. If there is no valid rRK, a full EAP exchange may be performed via IEEE Std 802.1X authentication to establish rRK as defined in [IETF RFC 6696].

If the STA chooses to initiate FILS shaed key authentication the STA first chooses a random 16 octet nonce, and constructs an EAP-Initiate/Re-auth packet as specified in [IETF RFC6696], with the following additional clarification:

— Regarding EAP-RP Flags

o The 'B' flag shall be set to 0, indicating that this is not an EAP-RP bootstrap message.

o The 'L' flag shall be set to 1, indicating that the trusted third party with whom the STA shares the rRK is to provide the lifetimes of rRK and rMSK in the EAP-Finish/Re-auth Packet.

— The "Cryptosuite" field shall not be set to 1.

***Instruct the editor to modify section 11.11.2.2.2. as indicated:***

**11.11.2.2.2. Key establishment with FILS public key authentication**

Whenperforming FILS public key authentication, the non-AP STA begins FILS Key Establishment by first selecting a finite cyclic group from the dot11RSNConfigDLCGroup table. It then chooses a random, ephemeral private key, uses the selected group's scalar-op (see 11.3.4.1) with its private key to generate its ephemeral public key, and chooses a random nonce.

The STA then constructs an 802.11 authentication frame with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The STA's FILS Identity shall be indicated using the FILS Identity element (see 8.4.2.180), the random nonce shall be encoded in the FILS nonce field (see 8.4.1.55), the FILS authentication type shall be set to indicate FILS public key authentication (2), the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the STA's public key shall be encoded into the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4.

First, the public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5. Then the public key, as a group element, shall be verified in a group-specific fashion as described in section in 5.6.2.3 of FIPS SP 800-56a.

The AP then shall choose a random nonce, and random, ephemeral private key, and then use the agreed-upon group's scalar-op (see 11.3.4.1) with its private key to generate its ephemeral public key. The AP then constructs an 802.11 authentication frame with the Authentication algorithm number set to <ANA-1>, the Authentication transaction sequence number set to two (2), and the FILS authentication type to indicate FILS public key authentication (2). The AP's identity shall be indicated using the FILS Identity element (see 8.4.2.179), its random nonce shall be encoded in(CID #1156) the FILS nonce field (see 8.4.1.55), the finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the AP's public key shall be encoded in(CID #1157) the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4. The AP shall transmit the 802.11 authentication frame to the STA. The AP may choose to derive the Diffie-Hellman shared secret, ss, at this point or it may choose to delay those computations until Key Confirmation (see 11.11.2.4). If it chooses to derive ss at this point, the AP shall use the STA's ephemeral public key and its private key with the chosen group's scalar-op to derive ss, and the AP shall then perform Key Derivation (see 11.11.2.3). If the AP chooses to delay these computations, it shall perform them just prior to Key Confirmation (see 11.11.2.4).

***Instruct the editor to modify section 11.11.2.3 as indicated:***

**11.11.2.3 Key derivation with FILS authentication**

Key derivation with FILS Authentication uses the KDF from 11.6.1.7.2 to produce six keys, two key encryption keys (KEK and KEK2), two confirmation keys (KCK and KCK2), a Pairwise Master Key (PMK), and a traffic key (TK). The inputs to the KDF are the two 16 octet nonces NSTA and NAP produced by the STA and AP, a constant label, the EAP-RP secret result if shared key authenticationis being used, and, the Diffie-Hellman shared secret, ss, if PFS is being used or public key authentication is being used. The length of the KEK and KEK2 shall be 128 bits, and the length of the KCK, KCK2,and PMK shall be 256 bits, and therefore the output from the KDF shall be 1024+TK\_bits, where TK\_bits is determined from table 11-4.

KCK2 | KEK2 | KCK | KEK | PMK | TK = KDF-X(NSTA | NAP, “FILS KECK PTK Derivation”, [rMSK]|[ ss]))

Where X is 1024+TK\_bits from table 11-4, rMSK is the output of the EAP-RP exchange if shared keywas used, and ss is the result of the Diffie-Hellman

exchange if public key authentication was used or if PFS was used with shared key authentication.

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

**11.11.2.4. Key confirmation with FILS authentication**

For FILS shared key authentication, 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).

For FILS public key authentication, 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:

For FILS shared keyauthentication, the AP shall construct a verifier as follows:

Key-Auth' = HMAC-SHA256(KCK, 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.

For FILS public key authentication, the AP shall use the STA's (certified) public key from the FILS Public Key element 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.

For FILS shared key authentication, 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)

For FILS public key authentication, 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:

For FILS shared key authentication, the STA shall construct a verifier as follows:

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

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

For FILS public key authentication, the STA shall use the AP's (certified) public key from the FILS Public Key element 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.

**References:**