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**

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 FILS authentication does not use an online trusted third party:

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

**11.11.2.2.2. FILS key establishment without a trusted third party**

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 authentication without a trusted third party (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).

**References:**