IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of Miscellaneous Security CIDs |
| Date: 2014-07-09 |
| 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

CIDs 4074, 4106, 4191, 4279, 4635, 4738, 4794, 5053, 5178

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

**4.5.4.2 Authentication**

IEEE Std 802.11 defines fivefour 802.11 authentication methods: Open System authentication, Shared Key authentication, FT authentication, andsimultaneous 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 performs fast initial setup of a secure link.. The IEEE Std 802.11 authentication mechanism also allows definition of new authentication methods.

***Instruct the editor to modify section 4.10.3.6.2 as indicated:***

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

It is assumed that both non-AP STAs and APs using FILS have either: 1) obtained a public key certificate from a certificate authority (CA) and that they are capable of verifying each other’s certificate during execution of FILS authentication procedures; or 2) an a priori knowledge of and trust in, a raw (uncertified) public key. The manner by which trust is obtained in these certificates and public keys is outside the scope of this standard.

***Instruct the editor to modify section 4.10.7 as indicated:***

**4.10.7 PMKSA Caching**

Using FILS authentication, the STA supplies a list of PMK identifiers in itsAuthentication Request frame. Each PMK identifier names a PMKSA; the PMKSA contains a single PMK. If the AP has retained an identified PMKSA and wishes to facilitate a faster connection, it indicates use of a single identified PMKSA in its Authentication Response frame. The STA and AP then use the PMK from the cached PMKSA in FILS handshaking to mutually authenticate. FILS authenticators that support PMK caching identify themselves to STAs using a cache identifier. A STA that has successfully established a PMKSA at an AP identifying a particular FILS authenticator can attempt to use PMK caching in a subsequent attempt at an AP that uses the same cache identifier.

***Instruct the editor to make the following change to 6.3.5.2.2, 6.3.5.3.2 and 6.3.5.5.2:***

Multi-band peer,

FILSWrappedData,

PMKID List,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
|  Name |  Type |  Valid range |  Description |
| FILSWrappedData | Sequence of elements and fields | As defined in 8.4.2.184 FILS Wrapped Data element | Data used by the FILS authentication algorithm. This parameter is optionally present when dot11FILSActivated is true |
| PMKID List | Element | As defined in 8.4.2.186 PMKID list element | Data used by the FILS authentication algorithm. This parameter is optionally present when dot11FILSActivated is true. |

***Instruct editor to modify table 8-26 in section 8.3.3.5 as indicated:***

**8.3.3.5 Association Request frame format**

|  |  |  |
| --- | --- | --- |
|  Order | Information |  Notes |
|  25 |  FILS Public Key | An element that contains a public key. Present if FILS public key authentication is used and dot11FILSActivated is true.  |

***Instruct editor to modify table 8-27 in section 8.3.3.6 as indicated:***

**8.3.3.6 Association Response frame format**

|  |  |  |
| --- | --- | --- |
|  Order | Information |  Notes |
|  31 |  FILS Public Key | An element that contains a pubic key. Present if for FILS public key authentication is used and dot11FILSActivated is true.  |

***Instruct the editor to modify table 8-32 in section 8.3.3.11 as indicated:***

**8.3.3.11 Authentication frame format**

|  |  |  |
| --- | --- | --- |
|  Order |  Information |  Notes |
|  18 |  FILS Authentication Type | The FILS Authentication Type is present in FILS Authentication frames asdefined in Table 8-33 (Presence of fields and elements in Authentication frames). |
|  19 |  FILS Nonce | The FILS Nonce is present in FILS Authentication frames as defined in Table8-33 (Presence of fields and elements in Authentication frames). |
|  20 | PMKID List  |  The PMKID List is present in FILS Authentication frames as defined in Table8-33 (Presence of fields and elements in Authentication frames). |
|  21 |  FILS Session |  The FILS Session is present in FILS Authentication frames as defined in Table8-33 (Presence of fields and elements in Authentication frames). |
|  22 |  FILS Wrapped Data | The FILS Wrapped Data is present in FILS Authentication frames as definedin Table 8-33 (Presence of fields and elements in Authentication frames). |

***Instruct the editor to modify section 8.4.2.177 as indicated:***

**8.4.2.177 FILS Public Key element**

0: Reserved

1: An X.509v3 certificate encoded according to RFC 5280.

2: A raw (uncertified) public key encoded according to RFC 5480

3: A raw (uncertified) public key encoded according to RFC 3279

The device's key type plus public key might not fit into a single element and therefore the data following the length field of a FILS Public Key element might require fragmentation using Fragment elements (see 8.4.2.185 (Fragment element)).

***Instruct the editor to add new section as 8.4.2.178 and to increment all subsequent subections in 8.4.2:***

**8.4.2.178 FILS Public Key Indicator element**

The FILS Public Key Indicator element is used to discover whether FILS Public Key authentication is feasible or not. An AP includes a FILS Public Key Indicator indicating the issuer of its certificate or a hash of its raw (uncertified) public key, as appropriate, in beacons and probe responses it emits. Multiple FILS Public Key Indicator elements are allowed in a single beacon or probe response. Nothing is inferred by the order in which multiple FILS Public Key Indicator elements are presented. The format of the FILS Public Key Indicator element is shown in Figure 8-401zzz (FILS Public Key Indicator element format).

Element ID Length Key Type Public Key

 Indicator

 Octets 1 1 1 variable

 **Figure 8-401zzz—FILS Public Key Indicator element**

The Element ID and Length fields are defiend in 8.4.2.1 (General).

Where the Key Type subfield is as follows:

 0: Reserved

 1: The Issuer, per RFC 5280, of the AP’s certificate

 2: A SHA-256 hash of the AP’s raw (uncertified) RFC 5480 public key

 3: A SHA-256 hash of the AP’s raw (uncertified) RFC 3279 public key

**8.4.2.186 PMKID list element**

The PMKID list contains a PMKID count followed by that number of PMKIDs. The size of each PMKID is 16 octets so the length of the PMKID list element is based on the number of PMKIDs included. The maximum number of PMKIDs in the list is 15 due to limitations on the size of an element (255 octets).

The Element ID and Length fields are defined in 8.4.2.1 (General).

The PMKID count indicates the number of PMKIDs in the Sequence of PMKIDs.

The Sequence of PMKIDs is one or more PMKIDs (as defined in 11.11.2.3) concatenated together.

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

**11.11.2.1 Authentication discovery of a FILS capable AP**

A STA discovers a FILS-capable AP through advertisment public key indicators (see 8.4.2.178 (FILS Public Key Indicator element)). A STA that trusts, or has an ability to gain trust, through validation of an X.509v3 certificate issued by an known certificate issuer, or that trusts a raw (uncertified) public key identified through its hash, may begin the FILS Authentication protocol to the AP and perform mutual authentication using trusted public keys.

**References:**