IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of Some More Security Comments |
| Date: 2014-01-06 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA 94089 | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission proposes resolution to CIDs 2240, 2330, 2331, 2491, 2577, 2621, 2962, 3000, 3262 and 3276

***Instruct the editor to modify section 3.3. as indicated:***

**3.1 Abbreviations and acronyms**

trusted third party (TTP): an entity that is relied upon for attestation by two parties in a pairwise authentication protocol.

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

**4.5.4.2 Authentication**

SAE authentication, FILS authentication, and Open System 802.11 authentication are used by non-DMG STAs in an RSN for an infrastructure BSS.

***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 using FILS have either: 1) obtained a public key certificate from a certificate authority (CA) and that each STA is capable of verifying this certificate during execution of the FILS authentication procedures; or 2) an a priori knowledge of, and trust in, a raw public key. The manner by which trust is obtained in these certificates and public keys is outside the scope of this standard.

The following operations are carried out when FILS authentication does not use an online TTP:

1. The STA discovers the AP’s policy through passive scanning or through active scanning. If a FILS STA discovers that the AP supports FILS public key authentication by inspecting the FILS Discovery frame,the STA can initiate FILS public key authentication.
2. The STA initiates FILS authentication by sending an Authentication frame to the AP, after which the AP responds with an Authentication frame. The STA and AP generate a PMK as a result of this exchange.
3. 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 and further establishment of FILS state.

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

**8.4.2.185 FILS indication element**

The FILS Indication element contains information related to FILS Capabilities of the AP.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  Element ID |  Length |  FILS Information |  Domain information(conditional) | Public KeyInformation(conditional) |

Octets 1 1 2 Variable Variable

 **Figure 8-401cz—FILS Indication element**

The definitions of FILS Information field is as follows:

 B0 B2 B3 B5 B6 B7 B8 B9 B10 B11 B15

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FILS Security Type | Number of Domains | IP AddressAssignmentMethod | Subnet-IDToken present |  Public Reserved Key Info  |

Bits 3 3 2 1 2 5

 **Figure 8-401da—FILS Information field definition**

Table 8-183af (FILS Security type) shows the possible field values for the FILS security indication element.

When the FILS Security Type of the FILS Information field is 0 or 1 (indicating shared key authentication) the Domain Information field shall be present and the Public Key Information shall be absent. The AP sets the Number of Domains field in the FILS Information field to the number of domain information fields (Fig 8-401df) included in the FILS indication element and shall set the Public Key Info field to 0. . The domain information field is comprised of between one and six 4 octet fields formatted as defined in Figure 8-401df (Domain information field) and

the hashed domain name is computed from the Domain Name that is compliant with the “Preferred Name Syntax” as defined in IETF RFC 1035 (same as the domain name used in 8.4.4.15[CID #1187). The exact computation method for the hashed domain name is given in  10.44.5 (FILS Indication element)[CID #.1429, 1316, 1187 except the submission gives reference to 10.43.11 and there is no such clause, assume it is 10.43.1.If more than 7 domains are supported with EAP-RP authentication, the AP shall set the Number of Domains to 7 to indicating that more than 6 domains are available, and only the first six domain information shall be present in the the domain information of the FILS indication Element. In that case, the STA shall use ANQP to obtain domain information of other domains that are not included in the FILS indication element.When the FILS Security type is set to 2 (public key authentication), the Domain Information field shall be absent and the Public Key Information shall be present and the AP shall set the number of domains is set to 0 and the Public Key Information field shall represent information about a public key. When a certified public key is used, the Public Key Info field shall be set to one (1) and the Public Key Information field shall be the X.500 Distinguished Name (DN) of the issuer of the AP’s certificate. When a raw public key is used, the Public Key Info field shall be set to two (2) and the Public Key Information field shall be the SHA256 hash of the AP’s raw public key. In either case, the length of the key information can be inferred from the length of the FILS Indication element and the length of the Public Key Identifier field. Public Key Info values 0 and 3-255 are reserved.

The IP Address Type field of the Domain Information field indicates the IP address type supported by the domain to which the AP is connected.

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

**8.4.2.189 Fragment element**

Each information element is limited to a maximum of 255 octets since their length field is a single octet (Figure 8-104). If data to be represented in an IE is too large and the generic advertisement service (GAS) is not used, it is necessary to fragment the data (see section 9.33 and 9.34).. The format of the Fragment IE is indicated in Figure 8-183du (Fragment IE).

***Instruct the editor to delete sections 8.4.2.189.1 and 8.4.2.189.2, including Table 8-183ak***

***Instruct the editor to change the headings of sections 9.5 and 9.6 as indicated:***

**9.5 MPDU Fragmentation**

**9.6 MPDU Defragmentation**

***Instruct the editor to insert new sections 9.33 and 9.34***

**9.33 Element Fragmentation**

The general format of elements limits the size of each element to 255 octets. Data that is too large for a single element may be fragmented into a series of elements consisting of the original element into which the data would not fit, immediately followed by a number of Fragment elements.

The data to be fragmented is divided into M + N chunks, where

• M is the result of the integer division of the length of the data by 255

• N is equal to 1 if the length of the data modulo 255 is greater than 0, and equal to 0 otherwise

The original element into which the data would not fit is filled with the first chunk of data and is termed the leading element. The length of the leading element shall be 255. This element is immediately followed by M-1 Fragment elements, each containing the next chunk of data and with a length of 255. If N = 1 these elements are immediately followed by the last chunk of data in a Fragment element which has a length equal to the length of the data modulo 255.

A Fragment element shall only follow another element whose length is 255. A Fragment element shall not be fragmented.

**9.34 Element Reassembly**

Elements which have had their information fields fragmented are those that are followed by one or more Fragment elements. To reconstruct the original data the chunk of data from the leading element is concatenated, in order, with the chunks of data from the series of Fragment elements that follow it. The reassembly procedure finishes when any element other than a Fragment element is encountered or the end of the MMPDU is reached.

***Instruct the editor to modify section 10.44.2 as indicated:***

**10.44.2 FILS Discovery Frame Generation and Usage**

A FILS Discovery frame may contain a Reduced Neighbor Report Information Element (IE) as defined in

Figure 8.4.2.176 and specified in Figure 10.44.3. The Reduced Neighbor Report IE in the FILS Discovery

frame provides the receiving non-AP STAs the information about Neighbor APs for a fast AP discovery.

A FILS Discovery frame may contain a FILS Indication element, as defined in section 8.4.2.185, that may include an identifier used during FILS authentication. The FILS Indication element in the FILS Discovery frame allows the receiving non-AP STA to know whether the FILS authentication protocol has a chance of succeeding.

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

**11.5.1.3.2 Security association in an ESS**

* 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 and finishing t FILS authentication with, one AP.

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

**11.11.2.1 Discovery with FILS authenticaiton**

A STA that discovers a FILS-capable AP that advertises a public key (see section 8.4.2.183) that the STA trusts, or has an ability to gain trust through validation of an X.509v3 certificate, may begin the FILS Authentication protocol to the AP and perform mutual authentication using trusted public keys.

***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**

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 according to section 5.6.2.3 of SP 800-56a.

**References:**