IEEE P802.11
Wireless LANs

|  |
| --- |
| A Re-Write of Section 8.4.2.179 |
| Date: 2015-01-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman avenue, Sunnyvale, California 94089, United States of America | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission proposes a rewrite of section 8.4.2.179 to simplify it and simultaneously make it more extensible.

***Instruct the editor to remove row 70 (Public Key Indicator) from Table 8-35 (Beacon frame body) and column 72 (Public Key Indicator) from Table 8-42 (Probe Response frame body).***

***Instruct the editor to remove the Public Key Indicator row from Table 8-85 (Element IDs).***

***Instruct the editor to move table 8-257d from section 8.4.2.177 to the bottom of 8.4.2.179 modifying the column titles as indicated, then delete the rest of section 8.4.2.177, and modify section 8.4.2.179 as indicated:***

**8.4.2.179 FILS Indication element**

The FILS Indication element contains information related to FILS authentication and higher layer setup capabilities of the AP.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  Element ID |  Length |  FILS Information | Cache Identifier (optional) | Domain Identifiers(optional) | Public Key Identifiers(optional) |

Octets: 1 1 1 0 or 16 Variable Variable

 **Figure 8-574I- FILS Indication element format**

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

The FILS Information field provides information on the presence of the further optional fields in the FILS Indication element. The format of the FILS Information field is shown in Figure 8-574m (FILS Information field definition):

 B0 B2 B3 B5 B6 B7 B8 B9 B10 B11 B15

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  Number of Public Key Identifiers | Number of Domain Identifiers | FILS IP Address Configuration |  |  | Cache Supported |  |

Bits: 3 3 1 1

 **Figure 8-574m—FILS Information field definition**

The Number of Public Key Identifiers lists the number of Public Key Identifiers that are present in the Public Key Identifers field in the FILS Indication element. When it is set to zero (0) the Public Key Identifier field is not present in the FILS Indication element. Each Public Key Identifier is formatted per Figure <ASSIGN-FIGURE-NUMBER> (Public Key Identifier). Up to 6 Public Key Identifiers may be carried in a FILS Indication element.

The Number of Domain Identifiers lists the number of Domain Identifier that are present in the Domain Identifiers field in the FILS Indication element. When it is set to zero (0) the Domain Identifier field is not present in the FILS Indication element. Each Domain Identifier is formatted per Figure 8-574n (Domain Identifier entry). Up to 6 Domain Identifiers may be carried in FILS Indication element.

The Cache Supported bit is set in the FILS Indication element when PMK caching is supported. When the Cache Supported bit is set to one (1) a 16 octet Cache Identifier is present in the FILS Indication element. When the Cache Supported bit is set to zero (0) the Cache Identifier is not present in the FILS Indication element. The content of the Cache Identifier is an opaque octet sring that identifies the scope in which PMKSAs are cached. Its construction is outside the scope of this standard.

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

An AP sets the FILS IP Address Configuration field to 1 if the AP supports FILS IP address configuration.

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

 B0 B15

|  |  |  |  |
| --- | --- | --- | --- |
| Hashed Domain Name |  |   |   |

 **Figure 8-574n—Domain Identifier**

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

The value of the Hashed Domain Name field of the Domain Information entry is computed from the domain name that is compliant with the preferred name syntax defined in IETF RFC 1035 (same as the domain name used in 8.4.4.15 (Domain Name ANQP-element)). The exact computation method for the hashed domain name is given in 10.45.4 (FILS authentication and higher layer setup capability indications).

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

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

|  |  |  |
| --- | --- | --- |
|  Key Type |  Length |  Public Key Indicator |

 Octets: 1 1 variable

**Figure <ASSIGN-FIGURE-NUMBER>-- Public Key Indicator**

The Key Type and Public Key Indicator values are described in Table 8-257c. The Length indicates the length in octets of the Public Key Indicator.

|  |  |
| --- | --- |
|  Key Type |  Public Key Indicator |
|  0 |  Reserved |
|  1 |  The Issuer, per IETF RFC 5280, of the AP’s certificate |
|  2 |  A SHA-256 hash of the AP’s uncertified IETF RFC 5480 public key |
|  3 |  A SHA-256 hash of the AP’s uncertified IETF RFC 3279 public key |
|  4-255 |  Reserved |

**Table 8-257c—Key Type and Public Key indicator**

**References:**