IEEE P802.11
Wireless LANs

|  |
| --- |
| Issues with 8.4.2.179 |
| Date: 2014-03-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr., San Diego, CA 92121 | +1 858 651 6645 | g |
|  |  |  |  |  |

Abstract

Editorial issues + a few changes (marked yellow)

***Insert new clause as follows:***

* 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 | Domain information (conditional) [14/0003r3] | Public Key Information (conditional) |
| Octets: | 1 | 1 | 2 | Variable  | Variable |
| * FILS Indication element
 |

 [13/1311r3, CID 2821]

The definitions of FILS Information field is as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| [13/1311r3] | B0 B2 | B3 B5 | B6 | B7 | B8 B9 | B10 B15 |
|  | FILS Security Type | Number of Domains | FILS IP Address Configuration [14/0138r4] | Subnet-ID Token present | Public Key Information type[14/0003r3] | Reserved |
| Bits: | 3 | 3 | 1 | 1 | 2 | 6 |
| * FILS Information field definition
 |

Table  8-183 (FILS Security Type [13/1311r3]) shows the possible field values for the FILS security indication element

|  |
| --- |
| * FILS Security Type [13/1311r3]
 |
| Bit values | FILS Security type |
| 0 | The FILS authentication exchange using FILS shared key without PFS. |
| 1 | The FILS authentication exchange using FILS shared key with PFS |
| 2 | The FILS authentication exchange with public key and with PFS |
| 3-7 | Reserved |

 [13/1311r3, CIDs 2664, 2823, 2215, 2570, 3114, 3204, 3045]

[Para deleted per 11/1311r3 and CID 3205 prior to deletion had resolved CID 2665 per 13/1354r2]

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. If the FILS Security type is set to 0 or 1 (FILS Shared key authentication), then 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 as follows: [CID2447, CID2824, CID2666] If Number of Domains indication is set to 7, it indicates that more than 6 domains are available, and only the first six domain information are present in the Per domain information of the FILS indication Element. The STA shall use ANQP to obtain domain information of other domains that are not included in the FILS indication element

[CID2666, CID2825, CID2402, CID2309, CID3046] [CID2447, CID2824] If the FILS Security type is set to 2 (Public Key authentication), then the number of domains is set to 0.

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

[CID2826, CID3207] The 1-bit Subnet-ID Token present subfield in FILS Information field indicates whether or not a subnet-ID Token corresponding to the IP subnet to which the domain is connected is present in the Domain information field, as defined in Table 8-183ah

|  |
| --- |
| * Subnet ID Token present
 |
| Bit Value | Subnet ID Token present |
| 0 | A subnet-ID Token corresponding to the IP subnet to which the [CID2543] IP routing domain is connected is not present in the Domain information field |
| 1 | A subnet-ID Token corresponding to the IP subnet to which the [CID2543] IP routing domain is connected is present in the Domain information field |

The Domain Information field is comprised of between one and six 4 octet fields formatted as defined in Figure 8-401cz (Domain Information field) and

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0 B15 | B16 B18 | B19 B23 | B24 B31 |
|  | Hashed Domain Name | IP Address Type | Reserved | Subnet ID Token [CID 2667] |
| Bits: | 16 | 3 | 5 | 8 |
| * Domain Information field
 |

 [CID 3071][13/1311r3] 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). The exact computation method for the hashed domain name is given in  10.44.4 (FILS Authentication and higher layer setup capability indications [CID 2869]).

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.

|  |
| --- |
| * IP Address Type [CID #1430
 |
| Bit Value | IP address type |
| 000 | IPv4 only |
| 001 | IPv6 only |
| 010 | IPv4 & IPv6 |
| 011 – 111 | Reserved |

The Subnet-ID Token[CID #1432 is an identifier derived from the subnet using a hash of the subnet or other means that is out of scope of this specification. The Subnet-ID Token is used by the STA to select an AP that is connected to the same IP domain as the current AP.

Public Key Information is set as follows: When a certified public key is used, the Public Key Information type field of the FILS information 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 Information type 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. [14/0003r3 paragraph and table here]