IEEE P802.11
Wireless LANs

|  |
| --- |
| Remove FILS Identity |
| Date: 2013-12-01 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr, San Diego, CA, USA | +1 858 651 6645 | gcherian@qti.qualcomm.com |

Abstract

Remove FILS Identity.

Addresses following CIDs

2440, 2439, 3182, 3202, 3295, 2723

4. Frame formats

**8.3 Format of individual frame types**

**8.3.3 Management frames**

* Beacon frame format

***Delete the rows as shown below;***

|  |
| --- |
| * Beacon frame body
 |
| Order | Information | Notes |
| 203 | ANQP Configuration Sequence Number (see  8.4.2.175 (ANQP Configuration Sequence Number element)) [13/0725r1 | [previous edits by CID #1102, 13/0573r3 deleted] ANQP Configuration Sequence Number element is optionally present when dot11FILSActivated is true. [13/0725r1 |
| 204 | Reduced Neighbor Report | The Reduced Neighbor Report element is optionally present if dot11FILSActivated is true |
| 205 | FILS Indication  | The FILS Indication is present if dot11FILSActivated is true. |
| 206 | AP Configuration Change CountAP-CCC | The AP Configuration Change CountAP-CCC is optionally present if dot11FILSActivated is true. |
| 207 | Differentiated Initial Link Setup element  | The Differentiated Initial Link Setup element [CID #1101, 1181] is optionally present when dot11FILSActivated is true. |
|  |  |  |

***Delete the rows as shown below;***

|  |
| --- |
| * Probe Response frame body
 |
| Order | Information | Notes |
| 70 | ANQP Configuration Sequence Number  8.4.2.175 (ANQP Configuration Sequence Number element) [13/0735r1 | ANQP Configuration Sequence Number element is optionally present when dot11FILSActivated is true. [13/0725r1 (replaces changes proposed by CID #1102, 13/0573r3 |
| 71 | Reduced Neighbor Report | The Reduced Neighbor Report element is optionally present if dot11FILSActivated is true |
| 72 | AP Configuration Change CountAP-CCC | The AP Configuration Change CountAP-CCC element is optionally present if dot11FILSActivated is true. |
| 73 | FILS Indication | The FILS Indication is present if dot11FILSActivated is true. |
| 74 | Differentiated Initial Link Setup element  | The Differentiated Initial Link Setup element, as specified in  8.4.2.187 (Differentiated Initial Link Setup element), is optionally present if[CID # 1262, 1264] dot11FILSActivated is true |
|  |  |  |
| Last–n | Requested elements | Elements requested by the Request element of the Probe Request frame are present if dot11MultiDomainCapabilityActivated is true. See  10.1.4.3.7 ( Criteria to respond to probe request) (Sending a probe response) ~~10.1.4.3.2~~. |

|  |
| --- |
| ***Delete the rows as shown below;***  |
| * Authentication frame body
 |
| Order | Information | Notes |
| 16 | FILS Session | The FILS Session is present in FILS Authentication frames as defined in Table  8-29 (Presence of fields and elements in Authentication frames). |
|  |  |  |
| 18 | FILS Authentication Type | The FILS Authentication Type is present in FILS Authentication frames as defined in Table  8-29 (Presence of fields and elements in Authentication frames). |
| 19 | FILS Nonce | The FILS Nonce is present in FILS Authentication frames as defined in Table  8-29 (Presence of fields and elements in Authentication frames). |
| 20 | FILS Wrapped Data | The FILS Wrapped Data is present in FILS Authentication Table  8-29 (Presence of fields and elements in Authentication frames) [CID #1103, 1414. |

***Delete the rows as shown below:***

|  |
| --- |
| * Presence of fields and elements in Authentication frames
 |
| Authentication algorithm | Authentication transaction sequence no. | Status code | Presence of fields 4-20 |
| FILS | 1 | Status | FILS Authentication type is present.FILS Nonce is present. FILS Wrapped Data is present if FILS authentication uses a TTP. Finite cyclic group is present if FILSAuthentication type field indicates PFS.Element is present if FILSAuthentication type field indicates PFS. [CID #1346] |
| FILS | 2 | Status | FILS Authentication type is present if Status is zero.FILS Nonce is present if Status is zero. FILS Wrapped Data is present if Status is zero and a TTP is used. Finite cyclic group is present if FILSAuthentication type field indicates PFS.Element is present if FILSAuthentication type field indicates PFS.[CID #1346] |

***Delete the rows as shown below:***

|  |
| --- |
| * Element IDs
 |
| Element | Element ID | Length of indicatedelement (in octets) | Extensible |
| ANQP Configuration Sequence Number ( 8.4.2.175 (ANQP Configuration Sequence Number element)) [13/0725r1 | <ANA> | 4 |  |
| Reduced Neighbor Report (see  8.4.2.176 (Reduced Neighbor Report element)) | <ANA> | 6 o 257 |  |
| FILS Request Parameters (see  8.4.2.177 (FILS Request Parameters element)) | <ANA> | 3 to 11 |  |
| Probe Response Reception Time (see  8.4.2.178 (Probe Response Reception Time element)) | <ANA> | 3 |  |
|  |  |  |  |
| FILS Key Confirmation (see  8.4.2.180 (FILS Key Confirmation element))  | <ANA> | Variable |  |
| FILS KDE Container (see  8.4.2.181 (FILS KDE container element))  | <ANA> | Variable |  |
| FILS Session (see  8.4.2.182 (FILS Session element))  | <ANA> | 10 |  |
| FILS Public Key (see 8 8.4.2.183 (FILS Public Key element)) | <ANA> | Variable |  |
| AP Configuration Change CountAP-CCC (See  8.4.2.184 (AP Configuration Change Count element)) | <ANA> | 3 |  |
| FILS Indication (see  8.4.2.185 (FILS Indication element)) | <ANA> | 3 to 257 |  |
| Higher Layer Encapsulation (see  8.4.2.186 (FILS Secure Container element) | <ANA> | 8 to 257 |  |
| Differentiated Initial Link Setup (see  8.4.2.187 (Differentiated Initial Link Setup element)) | <ANA> | Variable | Yes |
| FILS Wrapped Data (see 8.4.2.188 8.4.2.188 (FILS Wrapped Data element)) [CID # 1208 | <ANA> | Variable |  |

***Delete the following subsection:***

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

***Modify the following subsection as follows:***

* FILS key establishment with trusted third party

STA may initiate FILS authentication with a FILS capable AP that is connected to a trusted third party authentication server that shares a valid rRK as defined in [IETF RFC 6696] with the STA. If there is no valid rRK, a full EAP exchange may be performed via IEEE Std 802.1X authentication to establish rRK as defined in [IETF RFC 6696]. [13/0860r0]

If the STA chooses to initiate FILS authentication using a trusted third party[13/0860r0] the STA first chooses a random 16 octet nonce, and constructs an EAP-Initiate/Re-auth packet as specified in [IETF RFC6696], with the following additional clarification:

* Regarding EAP-RP[CID #1154] Flags

o The 'B' flag shall be set to 0, indicating that this is not an EAP-RP[CID #1154] bootstrap message.

o The 'L' flag shall be set to 1, indicating that the trusted third party is to provide the lifetimes of rRK and rMSK in the EAP-Finish/Re-auth Packet.

* The "Cryptosuite" field shall not be set to 1.

If PFS is desired, the STA selects a finite cyclic group from the dot11RSNAConfigDLGGroupTable, generates an ephemeral secret private key, and performs the group's scalar-op (see 11.3.4.1) with its random ephemeral private key and the generator from the selected finite cyclic group to compute an ephemeral public key.

The STA then constructs an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The random nonce shall be encoded in the FILS nonce field (see 8.4.1.55), the FILS authentication type shall be set to indicate the specific type of FILS authentication, and the EAP-Initiate/Re-auth packet shall be copied into the FILS authentication wrapped data field[CID #1415] (see 8.4.2.188(CID #1208)). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42) and the ephemeral public key shall be encoded in the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4.

The STA shall transmit the Authentication frame to the AP.

If Authentication frame includes a Finite Cyclic Group field, then the AP shall first determine whether the indicated finite cyclic group in the received FILS authentication frame is supported. If not, it shall respond with an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Status set to 77 (Authentication is rejected because the offered finite cyclic group is not supported) and shall terminate the exchange. If the group is supported or if PFS is not being used in this exchange, the AP shall extract the EAP-Initiate/Re-auth data from the FILS authentication wrapped data field[CID #1415] (see 8.4.2.188(CID #1208)) and shall forward it to the TTP. When applicable, the AP communicates with the trusted third party using the same protocols with which it uses when authenticating with EAP. Suitable protocols include, but are not limited to, remote authentication dial-in user service (RADIUS) (IETF RFC 2863-2000) and Diameter (IETF RFC 3588-2003).

If PFS is being used, the AP shall also generate an ephemeral private key and perform the group's scalar-op (see 11.3.4.1) to produce its own ephemeral public key. The AP may delay the generation of its ephemeral public/private key pair until after receiving a response from the TTP.

The TTP processes the EAP-Initiate/Re-auth packet as specified in RFC6696 and returns an EAP-Finish/Re-auth packet to the AP. In the case of successful authentication by the TTP, the TTP returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet.

If the TTP responds with a(CID #1389) failure indication, then the AP shall produce an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Status set to 15 (Authentication rejected because of challenge failure). If the TTP responds with a(CID #1390) success indication (including the associated EAP-RP rMSK), then the AP shall generate its own nonce and construct an Authentication frame for the STA. This frame shall contain the FILS wrapped data which encapsulates EAP-Finish/Re-auth packet received from the TTP. In addition, if PFS is used, the Element field of the Authentication frame sent by the AP contains the AP's ephemeral public key. In this frame, the AP shall set the Authentication sequence number to (2).[CID #1391 replaces 1251]

If PFS is being used for the exchange, then the AP shall perform the group's scalar-op (see 11.3.4.1) with the STA's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss.

Upon transmission of the FILS Authentication response, the AP shall perform key derivation per 11.11.2.3.

The STA processes the received Authentication frame.

* If the received Authentication frame does not include the Authentication algorithm number set to <ANA-1>, or if the received Authentication frame does not include an(CID #1392) EAP-Finish/Re-auth packet, then the STA shall abandon the FILS authentication
* If the received Authentication frame includes the Status set to 15 (Authentication rejected because of challenge failure), then the STA shall abandon the FILS authentication
* The STA ensures that the AP transmitted PFS parameters consistent with the desire of the STA (indicated by whether or not the STA transmitted an ephemeral public key).[CID #1393]
* If the STA transmitted an ephemeral public key, and the received Authentication frame does not include a well-encoded ephemeral public key, then the STA shall abandon the FILS authentication.
* If the STA did not transmit an ephemeral public key desired PFS, and the received Authentication frame includes an ephemeral public key, then the STA shall abandon the FILS authentication.
* The STA processes the EAP-Finish/Re-auth packet as per RFC6696 -
* If the 'R' flag = 0, indicating success, then the STA shall generate rMSK.
* If the 'R' flag = 1, indicating failure, then the STA shall abandon the FILS authentication.
* If PFS is being used for the exchange, then the STA shall perform the group's scalar-op (see 11.3.4.1) with the AP's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss.
* The STA shall perform key derivation per 11.11.2.3.

If the STA doesn't get Authentication response, then the STA shall perform retransmission procedure as defined in IETF RFC 6696. If the retransmission procedure fails, then the STA shall abandon the FILS authentication and may perform full EAP authentication via IEEE 802.1X authentication.

* FILS key establishment without a trusted third party

When not using a trusted third party, the non-AP STA begins FILS Key Establishment by first selecting a finite cyclic group from the dot11RSNConfigDLCGroup table. It then chooses a random, ephemeral private key, uses the selected group's scalar-op (see 11.3.4.1) with its private key to generate its ephemeral public key, and chooses a random nonce.

The STA then constructs an 802.11 authentication frame with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The random nonce shall be encoded in(CID #1155) the FILS nonce field (see 8.4.1.55), the FILS authentication type shall be set to indicate FILS authentication without a trusted third party (2), the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the STA's public key shall be encoded into the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4.

The STA shall transmit the 802.11 authentication frame to the AP.

The AP processes the STA's 802.11 authentication frame. First, if the finite cyclic group indicated by the Finite Cyclic Group field is not acceptable, the AP shall respond with an 802.11 authentication frame with the status code of 77 (“Authentication is rejected because the offered finite cyclic group is not supported”) and terminate the FILS authentication protocol. If the finite cyclic group is acceptable, the AP shall verify the validity of the STA's public key.

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 SP 800-56a in 5.6.2.3.

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 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).

The STA processes the AP's 802.11 authentication frame. First it ensures that the finite cyclic group in the AP's response matches the group selected by the STA. If they differ, the STA shall terminate the authentication exchange. If they match, the STA shall verify the validity of the AP's public key.

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 SP 800-56a in 5.6.2.3. If public key validation fails the STA shall terminate the authentication exchange. Otherwise it computes the Diffie-Hellman shared secret, ss, by using the AP's ephemeral public key and its private key with the chosen group's scalar-op to derive ss. The STA then performs Key Derivation (see 11.11.2.3) and begins Key Confirmation (see 11.11.2.4).