IEEE P802.11
Wireless LANs

|  |
| --- |
| Comments related to Section 11.11.2.2.1 |
| 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

Comments related to Section 11.11.2.2.1

Addresses following CIDs:

CID2874, CID2978, CID2979, CID2980, CID2873, CID2977, CID3085, CID3366.

**11.11.2.2.1 Key establishment with FILS shared key authentication**

STA may initiate FILS authentication with a FILS capable AP that is connected to a trusted third party authentication server that shares a valid shared key, called an 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]. EAP-RP signaling as defined in [IETF RFC 5295 & IETF RFC 6696] is used to validates the mutual possession of rRK between the STA and the Authentication Server. EAP-RP signaling is encapsulated using FILS wrapped data element in the IEEE 802.11 Authentication frame[CID2977]. AP unwraps the encapsulated EAP-RP packet received from the STA in the FILS wrapped data element and forwards the EAP-RP packet to the Authentication server using a transport that is out of scope of this specification. When the AP receives an EAP-RP packet from the Authentication Server, the AP forwards the packet to the STA by encapsulating the EAP-RP packet in the FILS wrapped data element of the IEEE 802.11 Authentication frame[CID2978].

To initiate FILS shared key authentication 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 Flags

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

o The 'L' flag shall be set to 1, indicating that the trusted third party with whom the STA shares the rRK 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 STA's FILS Identity shall be indicated using the FILS Identity element (see 8.4.2.179[CID #1386]), the random nonce shall be encoded in the FILS nonce field (see 8.4.1.54), 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 [CID2873] 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 [CID2873] wrapped data field[CID #[CID3366]] (see 8.4.2.188(CID #1208)) and shall forward it to the Authentication Server. 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 6942-2013).

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 Authentication Server.

The Authentication Serverprocesses 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 Authentication Server, the Authentication Serverreturns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet.

If the Authentication Serverresponds 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 Authentication Server 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 Authentication Server. 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 as follows.

* 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 and key confirmation per 11.11.2.4 [CID3085].

If the STA doesn't successfully receive Authentication response within the time of dot11AuthenticationResponseTimeOut, [CID2874,2979], then the STA should perform retransmission procedure as defined in IETF RFC 6696. If the retransmission procedure fails, then the STA shall abandon the FILS authentication and should perform full EAP authentication via IEEE 802.1X authentication [CID2980].