IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID 6028, 6641 | | | | |
| Date: 2015-01-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr., San Diego, CA 92121 | +1 858 651 6645 | gcherian@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

***Instruct the editor to modify the following section numbers and edits as indicated:***

[13/1354r2][CID 2975]

***Instruct the editor to modify the following section numbers and edits as indicated:***

11.11.2.2 Key establishment with FILS shared key authentication [13/1354r2]

This section defines the procedure for establishing a shared key between a FILS capable STA and AP using FILS shared key authentication

**11.11.2.2.1** **Overview**[CID 4075]

STA may initiate FILS shared key authentication either with a FILS capable AP that is connected to a TTP authentication server that shares a valid key, called an rRK, as defined in IETF RFC 6696 with the STA; or, to a FILS capable AP with whom it shares a cached PMKSA. If neither of these cases applies, a full EAP exchange may be performed via IEEE Std 802.1X authentication to establish rRK as defined in IETF RFC 6696 or another form of FILS authentication may be used to establish a shared PMKSA. [13/1354r2][14/052r2]EAP-RP signaling as defined in IETF RFC 5295 and IETF RFC 6696 is used to validate the mutual possession of rRK between the STA and the Authentication Server. EAP-RP signaling is encapsulated using FILS wrapped data element in the 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 Authentication frame[CID2978]. [CID 4735]

The message sequence is depicted in Figure 11.54 (FILS shared key authentication).[13/1510r2]******

* FILS shared key authentication

Following sections are organized per each step as shown in Figure 11.54

**11.11.2.2.2** **Step-1 IEEE 802.11 Authentication: STA requirements:**[13/1510r2][CID 4816]

If the STA chooses to initiate FILS shared key authentication, it shall first choose a random 16 octet nonceand then determine whether to attempt PMKSA caching. If PMKSA caching is attempted, it shall generate a list of PMKSA identifiers.[14/052r2] Otherwise, it shall construct an EAP-Initiate/Re-Auth packet IETF RFC6696, with the following additional clarification: [13/1354r2][14/0823r2] [14/1278r3]

* Regarding EAP-RP Flags
* The B flag shall be set to 0, indicating that this is not an EAP-RP bootstrap message. [CID 2102]
* The L flag shall be set to 1, indicating that the TTP with whom the STA shares the rRK is to provide the lifetimes of rRK and rMSK in the EAP-Finish/Re-auth Packet. [13/1354r2][14/0565r16 CID 4277]
* The Cryptosuite field shall not be set to 1. [CID 2101]

If PFS is desired, the STA selects a finite cyclic group from the dot11RSNAConfigDLGGroupTable, generates an ephemeral private key, and performs the group's scalar-op (see 11.3.4.1 (General)) with its random ephemeral private key and the generator from the selected finite cyclic group to compute an ephemeral public key. [CID 4326]

The STA then constructs an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2] and the Authentication transaction sequence number set to one (1). The [13/1514r1]random nonce shall be encoded in the FILS nonce field (see 8.4.1.59 (FILS Nonce field)), and the FILS authentication type shall be set to indicate the specific type of FILS authentication. If a list of PMKSA identifiers was generated, it shall be used to construct the PMKID list elements. The EAP-Initiate/Re-auth packet, if generated, shall be copied into the FILS [CID 2873]wrapped data field (see 8.4.2.184 (FILS Wrapped Data element)). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)) and the ephemeral public key shall be encoded in the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion). [14/0052r2[14/0823r2, CID 4384]

[CID 4385]

**11.11.2.2.3** **Step-1 IEEE 802.11 Authentication: AP requirements** [13/1510r2]

Upon reception of the Authentication frame, the AP shall do the following: [13/1510r2]

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 "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2] 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 check whether PMKSA caching is being attempted by the presence of the PMKID list element. If so, the AP checks whether any PMKSA identifier offered in the PMKID list matches an identifier for a cached PMKSA. If so, the AP selects a PMKID that matches and continues the FILS shared key authentication protocol using the PMK from the identified PMKSA. If not, the AP checks whether an EAP-Initiate/Re-Auth packet was included. If not, the AP shall respond with an Authentication frame with the Authentication algorithm number set to <ANA-1> and the Status set to 53 (invalid PMKID) and shall terminate the exchange. Otherwise, the AP shall [14/052r2]extract the EAP-Initiate/Re-auth data from the FILS [CID 2873]wrapped data field (see 8.4.2.184 (FILS Wrapped Data element)) and shall forward it to the Authentication Server. When applicable, the AP communicates with the Authentication Server using the same protocols [CID 2715]it uses when authenticating with EAP. Suitable protocols include, but are not limited to, remote authentication dial-in user service RADIUS (as specified in IETF RFC 2863-2000) and Diameter (as specified in IETF RFC 6942-2013).[13/1510r2][CID 2729][14/0823r2]

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 (General)) 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, if applicable[14/052r2].[13/1510r2][CID 4076]The Authentication Server 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 Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet. [13/1510r2][14/052r2]If the Authentication Server responds with a failure indication, then the AP shall produce an Authentication frame with the Authentication algorithm number set to "Fast Initial Link Setup authentication" <ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field)) and the Status set to 15 (Authentication rejected because of challenge failure). In the case of successful authentication by the Authentication Server, the Authentication Server returns the associated EAP-RP rMSK with the EAP-Finish/Re-auth packet and processing continues. [14/0823r2]

**11.11.2.2.4** **Step-2 IEEE 802.11 Authentication: AP requirements**[13/1510r2]

If the AP is not connected to, or does not recognize the Authentication server identified by the STA using the realm in the keyName-NAI field of the EAP-Initiate/Re-auth message, then the AP shall send Authentication frame with Status set to <ANA+1>, "Authentication rejected due to Unknown Authentication Server" to the non-AP STA.

[13/1510r2]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.[13/1510r2] [14/0823r2]

[14/052r2] [14/0341r5]If PFS is being used for the exchange, STA's public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5 (Octet string to element conversion). Then the AP shall verify the STA's public key in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56a-2013. If verification fails, the AP shall terminate the FILS authentication protocol. Otherwise, the AP shall perform the group's scalar-op (see 11.3.4.1 (General)) with the STA's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss. [14/1236r0]

Upon transmission of the FILS authentication response, the AP shall perform key derivation per 11.11.2.3 (Key derivation with FILS authentication).

**11.11.2.2.5** **Step-2 IEEE 802.11 Authentication: STA requirements**[13/1510r2]

The STA processes the received Authentication frame as follows.[13/1510r2]

* If the received Authentication frame does not include the Authentication algorithm number equal to "Fast Initial Link Setup authentication"<ANA-1> (see 8.4.1.1 (Authentication Algorithm Number field))[13/1510r2]. ,[14/052r2][14/0823r2] If PMKSA caching was attempted and the received Authentication frame includes a PMKID that does not match a PMKID sent in the Authentication request; or if the Authentication response does not include either a PMKID or an EAP-Finish/Re-auth packet, the STA shall abandon FILS authentication. [14/0823r2]
* If the received Authentication frame includes the Status equal to 15 (Authentication rejected because of challenge failure) or 53 (invalid PMKID), 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).
* 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.
* If applicable, the STA processes the EAP-Finish/Re-auth packet as per RFC6696.
* If the 'R' flag = 0, indicating success, then the STA shall derive rMSK. [CID 4327]
* If the 'R' flag = 1, indicating failure, then the STA shall abandon the FILS authentication.
* If PFS is being used for the exchange, the AP's public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5 (Octet string to element conversion). Then the STA shall verify the AP's public key in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56a-2013. If verification fails, the STA shall terminate the FILS authentication protocol. Otherwise, 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. [14/1236r0]
* The STA shall perform key derivation per 11.11.2.3 (Key derivation with FILS authentication) and key confirmation per 11.11.2.4 (Key confirmation with FILS authentication) [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. [CID 2980]

**11.11.2.2.6** **Step-3 IEEE 802.11 Association Request** [13/1510r2]

This step is part of Key confirmation. At this step, the STA generates the (Re)Association Request frame to the AP as specified in 11.11.2.4 (Key confirmation with FILS authentication). The STA may also include FILS HLP Container element or FILS IP Address Assignment element to request IP address. [13/1510r2] [14/0423r0][CID 4821]

**11.11.2.2.7** **Step-4 IEEE 802.11 Association Response** [13/1510r2]

This step is part of Key confirmation. At this step, the AP generates the (Re)Association Response frame to the STA as specified in 11.11.2.4 (Key confirmation with FILS authentication). The AP may also include FILS HLP Container element or FILS IP Address Assignment element to assign the IP address for the STA.[CID 4948] [13/1510r2] [14/0423r0][CID 4821]

***Instruct the editor to modify the following section numbers and edits as indicated:***

11.11.2.3 Key establishment with FILS public key authentication [13/1354r2]

This section defines the procedure for establishing a shared key between a FILS capable STA and AP using FILS public key authentication

When performing FILS public key authentication, 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 (General)) with its private key to generate its ephemeral public key, and chooses a random nonce. [CID 4070]

The STA then constructs an Authentication frame (see 8.3.3.11 (Authentication frame format)) with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The [13/1514r1]random nonce shall be encoded in the FILS nonce field (see 8.4.1.59 (FILS Nonce field)), the FILS authentication type shall be set to indicate FILS public key authentication (2), the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)), and the STA's public key shall be encoded into the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion). [13/1354r2]

The STA shall transmit the Authentication frame to the AP.

Upon receipt, the AP processes the STA's Authentication frame. First, if the finite cyclic group indicated by the Finite Cyclic Group field is not acceptable, the AP shall respond with an 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. [14/180r0]

First, the public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5 (Octet string to element conversion). Then the public key, as a group element, shall be verified in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56a-2013. If verification fails, the AP shall terminate the FILS authentication protocol.[13/1354r2, CID 2981][14/180r0]

Otherwise, 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 (General)) with its private key to generate its ephemeral public key. The AP then constructs an Authentication frame (see 8.3.3.11 (Authentication frame format)) 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 public key authentication (2). The[13/1514r1] random nonce shall be encoded in the FILS nonce field (see 8.4.1.59 (FILS Nonce field)), the finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)), and the AP's public key shall be encoded in the Element field (see 8.4.1.40 (Element field)) according to the element to octet-string conversion in 11.3.7.2.4 (Element to octet string conversion). The AP shall transmit the 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 (Key confirmation with FILS authentication)). Either way, it shall compute the Diffie-Hellman shared secret, ss, based on the STA's ephemeral public key and its own 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 (Key derivation with FILS authentication)). These computations shall be performed prior to Key Confirmation (see 11.11.2.4 (Key confirmation with FILS authentication)). [13/1354r2][14/180r0][CID 4775] [CID 4949]

Upon receipt, the STA processes the AP's Authentication frame. First it verifies that the finite cyclic group in the AP's response is equal to the group selected by the STA. If these differ, the STA shall terminate the authentication exchange. Otherwise, the STA shall verify the validity of the AP's public key.[14/180r0]

First, the public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5 (Octet string to element conversion). Then the public key, as a group element, shall be verified in a group-specific fashion according to 5.6.2.3 of NIST SP 800-56a-2013.[14/003r3] If public key validation fails the STA shall terminate the authentication exchange. Otherwise, it shall compute the Diffie-Hellman shared secret, ss, based on the AP's ephemeral public key and its own private key with the chosen group's scalar-op to derive ss. The STA then performs Key Derivation (see 11.11.2.3 (Key derivation with FILS authentication)) and begins Key Confirmation (see 11.11.2.4 (Key confirmation with FILS authentication)).[14/180r0]