IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIDs from 11.11.2.2.1 | | | | |
| Date: 2014-07-09 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

CIDs 4077, 4917, 4947

***Instruct editor to modify section 11.11.2.2.1 as indicated:***

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

Step 1: STA requirements:

If the STA chooses to initiate FILS shared key authentication, the STA first chooses a random 16 octet nonce. It then determines whether to attempt PMKSA caching or not. If it desires to attempt PMKSA caching, it generates a list of one or more PMKSA identifiers. A STA performing PMKSA caching optionally generates an EAP-Initiate/Re-Auth packet.. STAs not attempting PMKSA cachinggenerates an EAP-Initiate/Re-auth packet. as The EAP-Initiate/Re-Auth packet is generated according to IETF RFC6696, the following additional clarification:

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)) and the Authentication transaction sequence number set to one (1). The random nonce shall be encoded in the FILS nonce field (see 8.4.1.57 (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 constructthe PMKID list element. The EAP-Initiate/Re-auth packet, if generated, shall be copied into the FILS 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).

The STA shall transmit the Authentication frame to the AP

Step 1: AP requirements

Upon reception of the Authentication frame, the AP shall do the following:

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)) 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 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 extract the EAP-Initiate/Re-auth data from the FILS 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 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).

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.

Authentication Server procedure (when PMKSA caching is not being used):

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. 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). and processing continues

Step 2: AP requirements

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).

If PFS is being used for the exchange, then 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.

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

Step 2: STA requirements

The STA processes the received Authentication frame as follows.

1. 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)).
2. 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.
3. 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
4. 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).
5. 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.
6. 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.
7. If applicable, the STA processes the EAP-Finish/Re-auth packet as per RFC6696 –
8. If the 'R' flag = 0, indicating success, then the STA shall generate rMSK.
9. If the 'R' flag = 1, indicating failure, then the STA shall abandon the FILS authentication.
10. 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.
11. 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).

If the STA doesn't successfully receive Authentication response within the time of dot11AuthenticationResponseTimeOut, 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.

Step 3

This step is part of Key confirmation. At this step, the STA generates the Association Request frame to the AP as specified in 11.11.2.4 (Key confirmation with FILS authentication). The STA may also include FILS HLPContainer element or FILS IP Address Assignment element to request IP address.

Step 4

This step is part of Key confirmation. At this step, the AP generates the Association Response frame to the STA as specified in 11.11.2.4 (Key confirmation with FILS authentication). The AP may also include FILS HLPContainer element or FILS IP Address Assignment element to assign the IP address for the STA.

**References:**