IEEE P802.11
Wireless LANs

|  |
| --- |
| No More Steps |
| Date: 2015-03-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission addresses CID 7268

***Instruct the editor to modify section 11.11.2.2.2 as indicated:***

**11.11.2.2.2 Non-AP STA Construction of Authentication frame**

If the STA chooses to initiate FILS shared key authentication, it shall first choose a random 16 octet nonce and then determine whether to attempt PMKSA caching. If PMKSA caching is attempted, it shall generate a list of PMKSA identifiers. Otherwise, it shall construct an EAP-Initiate/Re-Auth packet IETF RFC6696, with the following additional clarification:

* Regarding EAP-RP Flags
	+ The B flag shall be set to 0, indicating that this is not an EAP-RP bootstrap message.
	+ 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.
* 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 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.

The STA then constructs an Authentication frame with the Authentication algorithm number set to 4 (FILS authentication) (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 8.4.1.59 (FILS Nonce field)), and the FILS Authentication Type field shall be set to FILS shared key authentication as defined in Table 8-257c (Key Type). 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 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 transmits the Authentication frame to the AP.

***Instruct the editor to modify section 11.11.2.2.3 as indicated:***

**11.11.2.2.3 AP Processing of Authentication frame**

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

1. 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.
2. If the indicated finite cyclic group in the received FILS authentication frame is not supported, the AP shall respond with an Authentication frame with the Authentication algorithm number set to 4 (FILS authentication) (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.
3. If the indicated finite cyclic group in the received FILS authentication frame 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.
4. If the PMKID list element is present, 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.
5. If a PMKID list element is not present or if no PMKSA identifier offered in the PMKID list matches any identifier for a cached PMKSA, 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 14 and the Status set to 53 (invalid PMKID) and shall terminate the exchange.
6. If an EAP-Initiate/Re-Auth packet is included, 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) and Diameter (as specified in IETF RFC 6942).

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. The Authentication Server processes the EAP-Initiate/Re-auth packet as specified in IETF 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/Reauth packet. 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“ 14 (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 terminates..

The AP proceeds by constructing an Authentication frame

***Instruct the editor to modify section 11.11.2.2.4:***

**11.11.2.2.4 AP Construction of Authentication frame**

If the AP is not connected to, or does not recognize the Authentication Server identified by the STA using the realm in the key Name-NAI field of the EAP-Initiate/Re-auth message, then the AP shall send Authentication frame with Status set to 115, “Authentication rejected due to unknown Authentication Server” to the non-AP STA.

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, 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-R2. 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.

The AP transmits the Authentication frame to the STA. Upon transmission of the FILS Authentication frame, the AP shall proceed to key establishment per 11.11.2.4 (Key establishment with FILS authentication).

***Instruct the editor to modify section 11.11.2.2.5 as indicated:***

**11.11.2.2.5 Non-AP STA Processing of Authenticaton frame**

The STA processes the received Authentication frame as follows.

1. If the received Authentication frame does not include the Authentication algorithm number equal to 4 (“FILS authentication) (see 8.4.1.1 (Authentication Algorithm Number field)). If PMKSA caching was attempted and the received Authentication frame includes a PMKID that does not match a PMKID in the Authentication frame sent by the STA; or if the received Authentication frame doesn’t include either a PMKID or an EAP-Finish/Re-auth packet, the STA shall abandon FILS authentication.
2. 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.
3. 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).
4. 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.
5. 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.
6. If applicable, the STA processes the EAP-Finish/Re-auth packet as per IETF RFC6696.
7. If the ‘R’ flag = 0, indicating success, then the STA shall derive rMSK.
8. If the ‘R’ flag = 1, indicating failure, then the STA shall abandon the FILS authentication.
9. 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-R2. 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.
10. The STA shall perform key derivation per 11.11.2.4 (PTKSA establishment with FILS authentication) and key confirmation per 11.11.2.5 (Key confirmation with FILS authentication) .

If the STA doesn’t successfully receive an Authentication frame 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.

Upon successful processing of the Authentication frame, the STA shall proceed with key estsablishment per 11.11.2.4 (Key establishment with FILS authentication).

***Instruct the editor to modify section 11.11.2.4 as indicated:***

**11.11.2.4 Key establishment with FILS authentication**

When not using PMKSA caching, a PMK is created using the Extract function of IETF RFC 5869. When using PMKSA caching, a new PMKSA is not created. Instead, the PMKSA used for PMKSA caching remains and continues to be identified by the appropriate PMKID. Regardless of whether PMKSA caching is used or not, a PTKSA shall be generated with each FILS authentication exchange.

PTKSA creation uses the KDF from 11.6.1.7.2 (Key derivation function (KDF)) to derive the following keys from the PMK: -a key confirmation key (KCK); a key encryption key (KEK); and a temporal key (TK).

When the AKM negotiated is 00-0F-AC:14 or 00-0F-AC:16 the hash algorithm used for the PMKSA and PTKSA creation shall be SHA-256 and when the AKM negotiated is 00-0F-AC:15 or 00-0F-AC:17 the hash algorithm used for the PMKSA and PTKSA creation shall be SHA-384.

PTKSA key establishment shall immediately be followed by key confirmation per 11.11.2.5 (Key confirmation with FILS authentication)

**References:**