IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID 6438, 6439, 6440 | | | | |
| 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 this section as indicated:***

* Key confirmation with FILS authentication

Key confirmation for FILS authentication is an (Re)Association Request followed by an (Re)Association Response. Components of the (Re)Association Request and (Re)Association Response shall be protected using KEK. [14/0341r5][CID 5020]

***Instruct the editor to modify this section as indicated:*** [14/0341r5]

* (Re)Association Request for FILS key confirmation [CID 4851]

The STA constructs an (Re)Association Request frame for FILS authentication per section 8.3.3.5 ((Re)Association Request frame format). Hash functions are used to generate the Key Confirmation element and the specific hash function depends on the AKM negotiated (8.4.2.24.3 (AKM suites)). [CID 4852, 4332][14/0824r2]

For FILS shared key authentication, the KeyAuth field of the Key Confirmation element is constructed by using the HMAC mode of the negotiated hash function with a key of KCK on a concatenation of the STA's nonce, the AP's nonce, the STA's MAC address, the AP's BSSID, and conditionally the STA's public Diffie-Hellman value and the AP's public Diffie-Hellman value, in that order:[13/1354r2] [14/0824r2]

Key-Auth = HMAC-Hash(KCK, NSTA | NAP | STA-MAC | AP-BSSID[ || gSTA || gAP]).. [14/0824r2]

Where:[14/0824r2]

* Hash is the hash function specific to the negotiated AKM
* NSTA is the STA's nonce, NAP is the AP's nonce
* STA-MAC is the MAC address of the STA and AP-BSSID is the BSSID of the AP
* gSTA is the STA's Diffie-Hellman public value and gAP is the AP's Diffie-Hellman public value
* The brackets indicate the optional inclusion of the Diffie-Hellman public values when doing PFS with FILS shared key authentication

For FILS public key authentication, the KeyAuth field of the Key Confirmation element is a digital signature using the STA's private key, of the negotiated hash function on a concatenation of the STA's public Diffie-Hellman value, the AP's public Diffie-Hellman value, the STA's nonce, the AP's nonce, the STA's MAC address, and the AP's BSSID, in that order. [13/1354r2]

Key-Auth = Sig-STA((gSTA | gAP | NSTA | NAP | STA-MAC | AP-BSSID). [14/0824r2]

Where Sig-STA( ) indicates a digital signature using the STA's private key, analog to the STA's trusted public key. The form of signature depends on the type of public key used by the STA (RFC 3447 for RSA; FIPS 184-4 for DSA; and, ISO/IEC 14888-3 for ECDSA). The data to be signed is first hashed and the hash algorithm used with the appropriate digital signature algorithm shall be specific to the negotiated AKM. [14/0824r2]

The (Re)Association Request frame shall be secured with KEK using the AEAD algorithm as defined in 11.11.2.5 (AEAD cipher mode for FILS). The AEAD algorithm takes AAD that is authenticated but not encrypted. The AAD for the (Re)Association Request is constructed by concatenating the following data together in order.

* The STA MAC
* The AP BSSID
* The STA's nonce
* The AP's nonce
* The contents of the (Re)Association Request frame from the capability (inclusive) to the FILS Session element (inclusive) [CID 4048]

[CID 2221]The plaintext passed to the AEAD encryption algorithm is the data that would follow the FILS session element in an unencrypted frame. If the AEAD cipher requires a unique counter, the current value of the AEAD counter from the PTKSA shall be passed to the AEAD encryption algorithm. The ciphertext output by the AEAD algorithm becomes the data that follows the FILS session element in the encrypted and authenticated (Re)Association Request frame. The resulting (Re)Association Request frame shall be transmitted to the AP. [14/0958r1 CID 5025]

The AP decrypts and verifies the received (Re)Association Request frame with KEK. The AAD is reconstructed as defined in this section above and is passed, along with the ciphertext of the received frame to the AEAD decrypt operation. If the AEAD cipher mode requires an AEAD counter, the AP implicitly uses the STA's initial AEAD counter of all zeros to decrypt and verify the received frame.

If the output from the AEAD decryption operation returns a failure, the authentication exchange shall be deemed a failure. If the output does not return failure, the returned plaintext replaces the ciphertext as portion of the frame that follows the FILS session element and processing of the received frame continues by checking the value of the Key Confirmation element. [CID 4071]

For FILS shared key authentication, the AP constructs a verifier, Key-Auth, in an identical manner as the STA constructed its Key-Auth above. [13/1354r2]

The AP compares Key-Auth' with the Key-Auth field in the Key Confirmation element of the received frame. If they differ, authentication shall be deemed a failure.

For FILS public key authentication, the AP uses the STA's (certified) public key from the FILS Public Key element to verify that the signature contained in the Key-Auth field corresponds to the purported signature by the STA over the concatenation of the following:

* the STA's public Diffie-Hellman value gSTA,
* the AP's public Diffie-Hellman value gAP,
* the STA's nonce NSTA, the AP's nonce NAP,
* the STA's MAC address STA-MAC, and
* the AP's BSSID AP-BSSID

in that order, according to the signature scheme used. Furthermore, the AP checks all certificates in the certificate chain, both cryptographically and from a security policy perspective, according to the procedures for checking certificates and certificate chains in RFC 5280. If any of these verifications fail, authentication shall be deemed a failure. [13/1354r2][14/0958r1 CID 5029]

If authentication is deemed a failure, KCK, KEK, TK and the PTKSA shall be irretrievably destroyed and the AP shall return an 802.11 Authentication frame with a status code set to <ANA> (Authentication rejected due to FILS authentication failure). If PMKSA caching was not being employed for this failed authentication attempt, the nascent PMKSA shall also be deleted. If PMKSA caching was being used, the cached PMKSA shall not be deleted in this case. [CID 4072][CID 4978]

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

* (Re)Association response for FILS key confirmation

The AP constructs an (Re)Association Response frame for FILS authentication per section 8.3.3.6 ((Re)Association Response frame format). As with the (Re)Association Request frame, hash functions are used to generate the Key Confirmation element and the specific hash function depends on the AKM negotiated (see 8.4.2.24.3 (AKM suites)). [ CID 4332]

The AP constructs a Key Delivery element indicating the current GTK for the BSS and the current RSC for the GTK. The AP puts this element into the FILS Key Delivery element (8.4.2.182 (Key Delivery element)) of the (Re)Association Response frame. [CID 4512][14/0824r2]

For FILS shared key authentication, the Key Auth field of the Key Confirmation element is constructed by using the HMAC mode of the negotiated hash function with a key of KCK on a concatenation of the AP's nonce, the STA's nonce, the AP's BSSID, the STA's MAC address, and conditionally the AP's public Diffie-Hellman value and the STA's public Diffie-Hellman value, in that order. [13/1354r2][CID 4512][14/0824r2]

Key-Auth = HMAC-Hash(KCK, NAP | NSTA | AP-BSSID | STA-MAC[ || gAP || gSTA]). [14/0824r2]

Where: [13/1354r2][CID 4512][14/0824r2]

* Hash is the hash function specific to the negotiated AKM
* NAP is the AP's nonce and NSTA is the STA's nonce
* AP-BSSID is the BSSID of the AP and STA-MAC is the MAC address of the STA
* gAP is the AP's Diffie-Hellman public value and gSTA is the STA's Diffie-Hellman public value
* The brackets indicate the optional inclusion of the Diffie-Hellman public values when doing PFS with FILS shared key authentication.

For FILS public key authentication, the Key Auth field of the Key Confirmation element is a digital signature using the AP's private key of the output from the negotiated hash function on a concatenation of the AP's public Diffie-Hellman value, the STA's public Diffie-Hellman value, the AP's nonce, the STA's nonce, AP's BSSID, and the STA's MAC address, in that order. The specific construction of the digital signature depends on the crypto-system of the public/private keypair: [13/1354r2]

Key-Auth = Sig-AP(gAP | gSTA | NAP | NSTA | AP-BSSID | STA-MAC ). [13/1354r2][CID 4512][14/0824r2]

Where Sig-AP() indicates a digital signature using the AP's private key analog to the AP's trusted public key. The form of signature depends on the type of public key used by the AP (RFC 3447 for RSA; FIPS 184-4 for DSA; and, ISO/IEC 14888-3 for ECDSA). The data to be signed is first hashed and the hash algorithm used with the appropriate digital signature algorithm shall be specific to the negotiated AKM. [13/1354r2][CID 4512][14/0824r2 CID 5029]

[14/183r0]The (Re)Association Response frame shall be secured with KEK using the AEAD cipher mode as defined in 11.11.2.5 (AEAD cipher mode for FILS). The AAD used with the AEAD algorithm for the (Re)Association Response is constructed by concatenating the following data together in order.

* The AP BSSID
* The STA MAC
* The AP's nonce
* The STA's nonce
* The contents of the (Re)Association Response frame from the capability (inclusive) to the FILS Session element (inclusive) [CID 4085]

The plaintext passed to the AEAD encryption algorithm is the data that would follow the FILS session element in an unencrypted frame. If the AEAD cipher requires a unique counter, the current value of the AEAD counter from the PTKSA shall passed to the AEAD encryption algorithm.The ciphertext output by the AEAD algorithm becomes the data that follows the FILS session element in the encrypted and authenticated (Re)Association Response frame. The resulting (Re)Association Response frame shall be transmitted to the STA. [14/0958r1 CID 5025]

The STA decrypts and verifies the received (Re)Association Response frame with KEK. The AAD is reconstructed as defined in this section above and is passed with the ciphertext of the received frame to the AEAD decrypt operation. If the AEAD cipher mode requires an AEAD counter, the STA implicitly uses the AP's initial AEAD counter of the value 128 followed by 12 octets of zero to decrypt and verify the received frame.

If the output from the AEAD decrypt operation returns failure, the authentication exchange shall be deemed a failure. If the output does not return failure, the output plaintext replaces the ciphertext as portion of the frame that follows the FILS session element and processing of the received frame continues by checking the value of the Key Confirmation element.

For FILS shared key authentication, the STA constructs a verifier, Key-Auth, in an identical manner as the AP constructed its Key-Auth above. [13/1354r2]

The STA compares Key-Auth' with the Key-Auth field in the Key Confirmation element of the received frame. If they differ, authentication shall be deemed a failure.

For FILS public key authentication, the STA uses the AP's (certified) public key from the FILS Public Key element to verify that the signature contained in the Key-Auth field corresponds to the purported signature by the AP over the concatenation of the following:

* AP's public Diffie-Hellman value gAP,
* the STA's public Diffie-Hellman value gSTA,
* the AP's nonce NAP,
* the STA's nonce NSTA,
* the AP's BSSID AP-BSSID, and
* the STA's MAC address STA-MAC

in that order, according to the signature scheme used. Furthermore, the AP checks all certificates in the certificate chain, both cryptographically and from a security policy perspective, according to the procedures for checking certificates and certificate chains in RFC 5280. If any of these verifications fail, authentication shall be deemed a failure. [13/1354r2][13/1354r2]13/1354r2][14/0958r1 CID 5029]

If authentication is deemed a failure, the KCK, KEK, PMK, and TK shall be irretrievably destroyed and the STA shall abandon the exchange. Otherwise authentication succeeds and the STA and AP shall irretrievably destroy the temporary keys and both shall use the TK with the cipher indicated by the negotiated cipher suite. The KCK, KEK, and PMK shall be used for subsequent key management as specified in 11.5 (RSNA security association management). The STA and AP shall set the lifetime of the PMKSA to the value dot11RSNAConfigPMKLifetime. [CID 4333] [CID 4953]

Upon successful completion of the FILS authentication procedure, the STA shall process the Key Delivery element as described in 8.4.2.182 (Key Delivery element). The STA shall install the GTK and shall set the key RSC. GTK rekeying shall be performed as described in 11.6.7 (Group Key Handshake).[14/183r0] [14/0423r0] [CID 4500] [CID 5157]