IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIDs from 11.11.2.4.1 and 2 | | | | |
| 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

This submission proposes resolutions to CIDs 4336, 5023, 5156

***Instruct the editor to modify section 2 as indicated:***

**2. Normative references**

FIPS PUB 186-4-2013, Digital Signature Standard (DSS)

ISO/IEC 14888-3:2006, Information technology – Security techniques—Digital signatures with appendix—Part 3: Discrete logarithm based mechanisms

IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specification Version 2.1

***Instruct the editor to modify section 11.11.2.4.1 as indicated:***

**11.11.2.4.1 Association Request for FILS key confirmation**

The STA constructs an 802.11 Association request frame for FILS Authentication per section 8.3.3.5 (Association Request frame format). Hashing 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)).

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:

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

Where Hash is the hash function specific to the negotiated AKM and the bracketed information is included 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.

Key-Auth = Sig-STA (gSTA || gAP || NSTA || NAP || STA-MAC || AP-BSSID).

Where Sig-STA [ ] indicates a digital signature using the 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.

The Association Request frame shall be securedwith KEK using the AEAD algorithm as defined in 11.11.2.5 (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 exchangeshall 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.

For FILS shared key authentication, the AP constructs a verifier , Key-Auth', in an identical manner as the STA constructed its Key-Auth above.

cipiher mode for FILS). The AEAD algorithm takes AAD that is authenticated but not encrypted. The AAD for the 802.11 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 Association Request frame from the capability (inclusive) to the FILS Session element (inclusive)

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 encryption operation becomes the data that follows the FILS session element in the encrypted and authenticated 802.11 Association Request frame. The resulting Association Request frame shall be transmitted to the AP.

***Instruct the editor to modify section 11.11.2.4.2 as indicated:***

**11.11.2.4.2 Association response for FILS key confirmation**

The AP constructs an 802.11 Association response frame for FILS Authentication per section 8.3.3.6 (Association Response frame format). As with the Association request frame, hashing 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)).

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 FILS Key Delivery element(8.4.2.182 (Key Delivery element)) of the Association Response frame.

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-Helman value and the STA’s public Diffie-Hellman value, in that order.

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

Where Hash is the hash function specific to the negotiated AKM, and the bracketed information is included 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 concatentation 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:

Key-Auth = Sig-AP(gAP || gSTA || NAP || NSTA || AP-BSSID || STA-MAC ).

Where Sig-AP [] indicates a digital signature using the 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.

The Association Response frame shall be secured with KEK using the AEAD cipher mode as defined in 11.11.2.5 (AEAD cipiher mode for FILS). The AAD used with the AEAD algorithm for the 802.11 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 Association Response frame from the capability (inclusive) to the FILS Session element (inclusive)

**References:**