IEEE P802.11
Wireless LANs

|  |
| --- |
| Suggested resolution for CID #2222 |
| Date: 2014-01-22 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON | +1 415 690-7363+1 647 867-5658Skype: rstruik | rstruik.ext@gmail.com |

***Remove clause 11.11.2.8 in the current Draft D1.2 (in its entirety):***

*Editorial note: text making explicit the inclusion of the container objects will now be incorporatedin Clause 11.11.2.4 instead.*

**~~11.11.2.8 GTK Transfer~~**

~~In FILS Authentication, GTK is transferred in Association Response frame from AP to STA. After successful~~

~~authentication (11.11.2.2 (Key establishment with FILS authentication)), key derivation (11.11.2.3 (Key~~

~~derivation with FILS authentication)) and key confirmation (11.11.2.4 (Key confirmation with FILS authentication))~~

~~by the AP, the AP shall construct Key RSC TLV (8.4.2.181.5 (Key RSC TLV)) and GTK Transfer~~

~~TLV. The AP shall put these TLVs into FILS Secure Container (8.4.2.181 (FILS Secure Container element))~~

~~and shall encrypt it as described in 8.4.2.181 (FILS Secure Container element) and 11.11.2.6 (Encrypt and~~

~~authenticate operation for FILS association frames).~~

~~STA shall decrypt FILS Secure Container as described in 8.4.2.181 (FILS Secure Container element) and~~

~~11.11.2.7 (Decrypt and verify operation for FILS association frames). The STA install GTK and set key~~

~~RSC.~~

~~GTK rekeying shall be performed as described in 11.6.7 (Group Key Handshake).~~

***Change clause 8.4.2.181’s title as follows:***

**8.4.2.181 FILS ~~Secure~~ Container element**

*Editorial note: all other occurrences of “Secure Container element” in the draft should also be changed to “Container element”.*

***Change clause 11.11.2.4 as follows:***

**11.11.2.4 Key confirmation with FILS authentication**

Key confirmation for FILS Authentication is an Association Request followed by an Association Response.

The Association Request and Association Response shall be protected using the KEK2 according to

11.11.2.6 (Encrypt and authenticate operation for FILS association frames) and 11.11.2.7 (Decrypt and verify

operation for FILS association frames).

Upon the completion of key establishment (11.11.2.2) and key derivation (11.11.2.3) the STA shall construct

an 802.11 Association Request frame indicating its selected ciphersuite and the FILS AKM, and the

FILS Key Confirmation element. The content of the Key Auth field of the Key Confirmation element

depends on the type of FILS authentication.

The AP transfers any necessary KDEs to the STA in the Association Response frame. The AP may include

one or more KDEs using the FILS KDE container. The format and the rules for transferring the KDE shall

follow 11.6.2 (EAPOL Key Frames).

For FILS shared key authentication, the Key Auth field of the Key Confirmation element of the Association

Request shall be:

Key-Auth = HMAC-SHA256(KCK2, NSTA | NAP | STA-MAC | AP-BSSID).

For FILS public key authentication, the Key Auth field of the Key Confirmation element in the Association

Request shall contain a digital signature using the STA's private key, the specific construction of the digital

signature depends on the crypto-system of the public/private key pair:

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

Where Sig-STA indicates a digital signature using the STA's private key, gSTA is the octet-string representation

of the STA's public Diffie-Hellman value, gAP is the octet-string representation of the AP's public

Diffie-Hellman value, NSTA is the nonce selected by the STA, and NAP is the nonce selected by the AP.

The 802.11 Association Request frame shall be secured as follows:

The input key shall be the KEK2

— The input plaintext shall be the contents of the Association Request frame that follow the FILS Session

element

— The input AAD shall be:

a) The STA MAC

b) The AP BSSID

c) The STA's nonce

d) The AP's nonce

e) The contents of the Association Request frame from the capability (inclusive) to the FILS Session

element (inclusive)

— The input key, the plaintext, and the AAD shall be passed to the encrypt-and-authenticate operation

specified in 11.11.2.6.

— The output ciphertext shall become the remainder of the Association Request frame that follows the

FILS Session element.

The resulting 802.11 Association Request frame shall be transmitted to the AP.

The received 802.11 Association Request frame shall be processed as follows:

— The input key shall be the KEK2

— The input ciphertext shall be the contents of the Association Request frame that follow the FILS Session

element

— The input AAD shall be:

a) The STA MAC

b) The AP BSSID

c) The STA's nonce

d) The AP's nonce

e) The contents of the Association Request frame from the capability (inclusive) to the FILS Session

element (inclusive)

— The input keys, the ciphertext, and the AAD shall be passed to the decrypt-and-verify operation

specified in 11.11.2.6.

If the output from 11.11.2.6 returns a failure, authentication shall be deemed a failure. If the output returns

plaintext, the Key-Auth from the decrypted Association Response frame shall be checked. If it is incorrect,

authentication shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK,

KEK, and TK shall be irretrievably destroyed. If authentication is not deemed a failure, the AP shall check

the Key-Auth field in the Key Confirmation element.

For FILS shared key authentication, the AP shall construct a verifier as follows:

Key-Auth' = HMAC-SHA256(KCK, NSTA | NAP | STA-MAC | AP-BSSID)

If Key-Auth' differs from the Key-Auth field in the Key Confirmation element, authentication shall be

deemed a failure.

For FILS public key authentication, the AP shall use the STA's (certified) public key from the FILS Public

Key element in the Association frame to verify the contents of the Key-Auth field of the Key Confirmation

element. The specific technique for verification depends on the crypto-system used by the public key. If verification

fails, authentication shall be deemed a failure.

If authentication is a failure, the KCK2, KEK2, KCK, KEK, and TK shall be irretrievably destroyed. Otherwise,

the AP shall then construct an 802.11 associate response frame confirming the selected ciphersuite and

the FILS AKM, and containing the FILS KDE Container, and its own Key-Auth.

For FILS shared key authentication, the Key Auth field of the Key Confirmation element in the Association

Response shall be:

Key-Auth = HMAC-SHA256(KCK2, NAP | NSTA | AP-BSSID | STA-MAC).

For FILS public key authentication, the Key Auth field of the Key Confirmation element in the Association

Response shall contain a digital signature using the AP's private key, 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 AP's private key, and where gSTA, gAP, NSTA, and

NAP are the same as in the construction of the Association Request.

The AP shall construct Key RSC TLV (8.4.2.181.5 (Key RSC TLV)) and GTK Transfer

TLV. The AP shall put these TLVs into FILS Secure Container (8.4.2.181 (FILS Secure Container element)) and include these with the construction of the Association Response frame.

The 802.11 Association Response frame shall be protected as follows:

— The input keys shall be the KEK2

— The input plaintext shall be the contents of the Association Request frame that follow the FILS Session

element

— The input AAD shall be:

a) The AP BSSID

b) The STA MAC

c) The AP's nonce

d) The STA's nonce

e) The contents of the Association Response frame from the capability (inclusive) to the FILS

Session element (inclusive)

— The input keys, the plaintext, and the AAD shall be passed to the encrypt-and-authentication operation

specified in 11.11.2.5.

— The output ciphertext shall become the remainder of the Association Response frame that follows the

FILS Session element.

The resulting 802.11 Association Response frame shall be transmitted to the STA.

The STA shall process the received 802.11 Association Response frame as follows:

— The input key shall be the KEK2

— The input ciphertext shall be the contents of the Association Response frame that follow the FILS

Session element

— The input AAD shall be:

a) The AP BSSID

b) The STA MAC

c) The AP's nonce

d) The STA's nonce

e) The contents of the Association Response frame from the capability (inclusive) to the FILS

Session element (inclusive)

The input keys, the tag, the ciphertext, and the AAD shall be passed to the decrypt-and-verify operation

specified in 11.11.2.6.

If the output from 11.11.2.6 returns failure, authentication shall be deemed a failure. If the output returns

plaintext, the Key-Auth from the decrypted Authentication frame shall be checked. If it is incorrect, authentication

shall be deemed a failure. If authentication is deemed a failure, the KCK2, KEK2, KCK, KEK, and

TK shall be irretrievably destroyed. If authentication is not deemed a failure, the AP shall check the Key-

Auth field in the Key Confirmation element.

For FILS shared key authentication, the STA shall construct a verifier as follows:

Key-Auth' = HMAC-SHA256(KCK2, NAP | NSTA | AP-BSSID | STA-MAC).

If Key-Auth' differs from the Key-Auth field in the Key Confirmation element, authentication shall be

deemed a failure.

For FILS public key authentication, the STA shall use the AP's (certified) public key from the FILS Public

Key element in the Association frame to verify the contents of the Key-Auth field of the Key Confirmation

element. The specific technique for verification depends on the crypto-system used by the public key. If verification

fails, authentication shall be deemed a failure.

If authentication is a failure, the KCK2, KEK2, KCK, KEK, PMK, and TK shall be irretrievably destroyed.

Otherwise authentication succeeds. In that case, STA and AP shall irretrievably destroy the temporary keys

KCK2 and KEK2 and both shall use the TK with the cipher indicated by the negotiated. The KCK, KEK,

and PMK shall be used for subsequent key management as specified in clause 11.5. The STA and AP shall

set the lifetime of the PMKSA to the value dot11RSNAConfigPMKLifetime.

Upon successful completion of the FILS Authentication procedure, the STA shall process the Secure Container elements as described in 8.4.2.181 (FILS Secure Container element). The STA install GTK and set key

RSC. GTK rekeying shall be performed as described in 11.6.7 (Group Key Handshake).