IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution to CID 7457 |
| Date: 2015-05-11 |
| R1 Author: |
| Name | Affiliation | Address | Phone | email |
| Ping FANG | Huawei Technologies | Vision Business Park, Nanshan, Shenzhen, China | 0086 755 36835832 | ping.fang@huawei.com |

Abstract

This document provides proposed changes to resolve CID 7457.

CID 7457

"the procedure described in 11.11.2.3 reads as a long stream-of-consciousness and is hard to follow"

**Instructions for Editor: please modify the text of clause 11.11.2.3 with the following changes:**

**11.11.2.3 Key establishment with FILS public key authentication**

This subclause defines the procedure for establishing a shared key between a FILS capable STA and AP using public key.

FILS public key authentication performs key establishment with a Diffie-Hellman exchange.

Prior to beginning the exchange, the non-AP STA:

1. Selects a finite cyclic group from the dot11RSNConfigDLCGroup table in which to perform the Diffie-Hellman exchange.
2. Generates a random nonce, generates an ephemeral private key, and uses the selected group’s scalar-op (see 11.3.4.1 (General)) with its private key to generate its ephemeral public key.
3. Constructs an Authentication frame (see 8.3.3.11 (Authentication frame format)) as follows:
4. The Authentication algorithm number shall be set to 4 and the Authentication transaction sequence number shall be set to one (1).
5. The random nonce shall be encoded in the FILS Nonce field (see 8.4.1.59 (FILS Nonce field)).
6. The FILS Authentication Type field shall be set to indicate FILS public key authentication (2).
7. The chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)).
8. The STA’s public key shall be encoded into 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 then transmit the Authentication frame to the AP.

Upon receipt, the AP processes the STA’s Authentication frame as follows:

1. If the finite cyclic group indicated by the Finite Cyclic Group field is not acceptable, the AP shall respond with an Authentication frame with the status code of 77 (“Authentication is rejected because the offered finite cyclic group is not supported”) and terminate the FILS authentication protocol.
2. If the finite cyclic group is acceptable, the AP verifies the validity of the STA’s public key.
3. The 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).
4. The public key, as a group element, shall be verified in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56a-R23. If verification fails, the AP shall terminate the FILS authentication protocol.
5. The STA’s nonce and validated public key shall be extracted from the Authentication frame.

Next, the AP then shall:

1. Generate a random nonce, generate a random, ephemeral private key, and then use the agreed-upon group’s scalar-op (see 11.3.4.1 (General)) with its private key to generate its ephemeral public key.
2. Construct an Authentication frame (see 8.3.3.11 (Authentication frame format)) as follows:
3. The Authentication algorithm number set to 4, and the Authentication transaction sequence number set to two (2).
4. The FILS Authentication Type field to indicate FILS public key authentication (2).
5. The random nonce shall be encoded in the FILS Nonce field (see 8.4.1.59 (FILS Nonce field)).
6. The finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)).
7. The AP’s 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).
8. Transmit the Authentication frame to the STA.
9. Compute the Diffie-Hellman shared secret, ss, based on the STA’s ephemeral public key and its own private key with the chosen group’s scalar-op.
10. Perform key derivation (see 11.11.2.4 (PTKSA establishment with FILS authentication)).

Upon receipt, the STA:

1. Verifies that the finite cyclic group in the AP’s response is equal to the group selected by the STA. If these differ, the STA shall terminate the authentication exchange.
2. Verifies the validity of the AP’s public key.
3. The 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).
4. The public key, as a group element, shall be verified in a group-specific fashion according to 5.6.2.3 of NIST SP 800-56a-R2. If public key validation fails the STA shall terminate the authentication exchange.
5. Extracts the AP’s nonce and verified public key from the Authentication frame.
6. Compute the Diffie-Hellman shared secret, ss, based on the AP’s ephemeral public key and its own private key with the chosen group’s scalar-op to derive ss.
7. Performs key derivation (see 11.11.2.4 (PTKSA establishment with FILS authentication)) and begins key confirmation (see 11.11.2.5 (Key confirmation with FILS authentication)).

**References:**

1. **IEEE P802.11ai™/D4.0, 2015**