IEEE P802.11
Wireless LANs

|  |
| --- |
| Suggested resolution for CID #2983 |
| 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 |

***Replace clause 11.11.2.2.2 in the current Draft by the following clause:***

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

When performing FILS public key authentication, the non-AP STA begins FILS Key Establishment by first selecting a finite cyclic group from the dot11RSNConfigDLCGroup table. It then chooses a random, ephemeral private key, uses the selected group's scalar-op (see 11.3.4.1) with its private key to generate its ephemeral public key, and chooses a random nonce.

The STA then constructs an 802.11 authentication frame (see 8.3.3.11) with the Authentication algorithm number set to <ANA-1> and the Authentication transaction sequence number set to one (1). The STA's FILS Identity shall be indicated using the FILS Identity element (see 8.4.2.180), the random nonce shall be encoded in the FILS nonce field (see 8.4.1.57), the FILS authentication type shall be set to indicate FILS public key authentication

(2), the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the STA's public key shall be encoded into the Element field (see 8.4.1.40) according to the element to octet string conversion in 11.3.7.2.4.

The STA shall transmit the 802.11 authentication frame to the AP.

Upon receipt, the AP processes the STA's 802.11 authentication frame. First, if the finite cyclic group indicated by the Finite Cyclic Group field is not acceptable, the AP shall respond with an 802.11 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. If the finite cyclic group is acceptable, the AP shall verify the validity of the STA's public key.

First, the public key shall be converted from an octet string to an element according to the conversion in

11.3.7.2.5. Then the public key, as a group element, shall be verified in a group-specific fashion as described in section 5.6.2.3 of NIST SP 800-56a-2013. If verification fails, the AP shall terminate the FILS authentication protocol.

Otherwise, the AP then shall choose a random nonce and random, ephemeral private key, and then use the agreed upon group's scalar-op (see 11.3.4.1) with its private key to generate its ephemeral public key. The AP then constructs an 802.11 authentication frame (see 8.3.3.11) with the Authentication algorithm number set to <ANA-1>, the Authentication transaction sequence number set to two (2), and the FILS authentication type to indicate FILS public key authentication (2). The AP's identity shall be indicated using the FILS Identity element (see 8.4.2.179), its random nonce shall be encoded in the FILS nonce field (see 8.4.1.55), the finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42), and the AP's public key shall be encoded in the Element field (see 8.4.1.40) according to the element to octet-string conversion in 11.3.7.2.4. The AP shall transmit the 802.11 authentication frame to the STA. The AP may choose to derive the Diffie-Hellman shared secret, ss, at this point or it may choose to delay those computations until Key Confirmation (see 11.11.2.4). Either way, it shall compute the Diffie-Hellman shares secret, ss, based on the STA's ephemeral public key and its own private key with the chosen group's scalar-op, and the AP shall then perform Key Derivation (see 11.11.2.3). If the AP chooses to delay these computations, it shall perform them just prior to Key Confirmation (see 11.11. 2.4).

Upon receipt, the STA processes the AP's 802.11 authentication frame. First it checks 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. Otherwise, the STA shall verify the validity of the AP's public key.

First, the public key shall be converted from an octet string to an element according to the conversion in

11.3.7.2.5. Then the public key, as a group element, shall be verified in a group-specific fashion according to section 5.6.2.3 of NIST SP 800-56a-2013. If public key validation fails, the STA shall terminate the authentication exchange. Otherwise, it shall 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. The STA then performs Key Derivation (see

11.11.2.3) and begins Key Confirmation (see 11.11.2.4).