IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element Validation for Shared Key Authentication in FILS | | | | |
| Date: 2014-09-15 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman avenue, Sunnyval, California, United States of America | +1 408 227 4500 | dharkins at aruba networks, one word, dot com |
|  |  |  |  |  |

Abstract

This submission proposes resolution to CIDs 4078 and 4079.

***Instruct the editor to modify section 11.11.2.2.1 as indicated:***

**11.11.2.2.1 Key establishment with FILS shared key authentication**

If PFS is being used for the exchange, STA’s 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). Then the AP shall verify the STA’s public key in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56a-2013. If verification fails, the AP shall terminate the FILS authentication protocol. Otherwise, the AP shall perform the group's scalar-op (see 11.3.4.1 (General)) with the STA's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss.

1. If PFS is being used for the exchange, the AP’s 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). Then the STA shall verify the AP’s public key in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56a-2013. If verification fails, the STA shall terminate the FILS authentication protocol. Otherwise, the STA shall perform the group's scalar-op (see 11.3.4.1) with the AP's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, ss.

***Instruct the editor to modify section 11.11.2.2.2 as indicated:***

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

First, 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). Then 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-2013. If verification fails, the AP shall terminate the FILS authentication protocol.

**References:**