IEEE P802.11
Wireless LANs

|  |
| --- |
| Editorial resolution of cross reference issue |
| Date: 2015-06-09 |
| 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 editorial resolution of cross reference issue.

**Discussion:**

In clause 11.11.2.3.2 of D4.5, there is a paragraph as below:

The STA then constructs an Authentication frame with the Authentication algorithm number set to 4 (FILS authentication) (see 8.4.1.1 (Authentication Algorithm Number field)) and the Authentication transaction sequence number set to 1. The random nonce shall be encoded in the FILS Nonce field (see 8.4.1.58 (FILS Nonce field)), and the FILS Authentication Type field shall be set to FILS shared key authentication as defined in Table 8-257c (Key Type). If a list of PMKSA identifiers was generated, it shall be used to construct the PMKID List elements. The EAP-Initiate/Re-auth packet, if generated, shall be copied into the FILS Wrapped Data field (see 8.4.2.183 (FILS Wrapped Data element)). If PFS is desired, the chosen finite cyclic group shall be encoded in the Finite Cyclic Group field (see 8.4.1.42 (Finite Cyclic Group field)) and the ephemeral 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).

There is a reference to Table 8-257c (Key Type) which is right. After offline discussion with George and Dan, it is confirmed that the reference is supposed to be Table 8-73a (Values of FILS Authentication Type Field). And “depending on whether PFS is used” is recommended by Dan giving the fact that there are two values for FILS shared key authentication in the table.

**Instructions for Editor: please modify the text in 11.11.2.3.2 as below (P141L15):**

**Change the sentence**

“The random nonce shall be encoded in the FILS Nonce field (see 8.4.1.58 (FILS Nonce field)), and the FILS Authentication Type field shall be set to FILS shared key authentication as defined in Table 8-257c (Key Type).”

**to**

“The random nonce shall be encoded in the FILS Nonce field (see 8.4.1.58 (FILS Nonce field)), and the FILS Authentication Type field shall be set to one of the FILS shared key authentication values as defined in Table 8-73a (Values of FILS Authentication Type field) depending on whether PFS is used.”

**References:**

1. **IEEE P802.11ai™/D4.3, May 2015**