IEEE P802.11
Wireless LANs

|  |
| --- |
| A Few More DNH Comments |
| Date: 2015-03-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission addresses CIDs 7406 and 7222

***Instruct the editor to modify section 8.4.2.185 as indicated:***

**8.4.2.185 Fragment element**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element ID |  Length | Element ID Extension | PMKID Count | Sequence of PMKIDs |

Octets: 1 1 1 1 1

 **Figure -575ad—PMKID list element format**

***Instruct the editor to modify section 11.5.1.1.6 as indicated:***

**11.5.1.1.6 PTKSA**

The PTKSA consists of the following elements:

— PTK

— Pairwise cipher suite selector

— Supplicant MAC address or STA’s MAC address

— Authenticator MAC address or BSSID

— Key ID

— If FT key hierarchy is used,

* R1KH-ID
* PTKName

— If FILS is used,

* Non-AP STA’s AEAD counter
* AP’s AEAD counter

***[Editorial comment: if we used AES-SIV we would not need to make such modifications to the PTKSA]***

**References:**