IEEE P802.11
Wireless LANs

|  |
| --- |
| mc SAE comments  |
| Date: 2012-09-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This document addresses some comments received during the call for comments on IEEE 802.11-2012.

***Instruct the editor to modify 11.3.3 as indicated:***

The binary representation of the password, after being transformed from a character representation or directly if it is already in binary form, is stored in the dot11RSNAConfigPasswordValueTable. When a “password” is called for in the description of SAE that follows, the credential from the dot11RSNAConfigPasswordValueTable is used.

***Instruct the editor to modify 11.3.5.4 as indicated:***

If the scalar value is greater than zero (0) and less than the order, *r*, of the negotiated group, scalar validation succeeds; otherwise, it fails. Element validation depends on the type of group. For FFC groups, the element shall be an integer greater than one (1) and less than the prime number *p*, and the scalar operation of the element and the order of the group, *r*, shall be equal to one (1) modulo the prime number *p*.

***Instruct the editor to add the following columns to table 11-9 in 11.6.3:***

|  |  |  |  |
| --- | --- | --- | --- |
|  AKM |  Integrity algorithm |  Size of MIC |  Key-wrap algorithm |
|  00-0F-AC:8 |  AES-128-CMAC |  16 |  NIST AES Key Wrap |
|  00-0F-AC:9 |  AES-128-CMAC |  16 |  NIST AES Key Wrap |

**References:**