IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of CID 8017 |
| Date: 2015-06-30 |
| 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 aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission proposes a resolution to CID 8017.

***Instruct the editor to modify section 11.6.12.4.1 as indicated:***

**11.6.12.4.1 Initial provisioning for PKEX**

Prior to sending a PKEX message, both STAs shall be provisioned with a shared key/code/word/phrase, hereinafter a credential. It shall be interpreted as a UTF-8 string with no NULL termination. The credential shall be used to generate a password element, PWE per section 11.3.4.2.2 (for ECC groups) or 11.3.4.3.2 (for FFC groups), in the same group as the public key with the one minor change: the MAC addresses are removed from the pwd-seed value calculation in section 11.3.4.2.2 (for ECC groups) and 11.3.4.3.2 (for FFC groups) and the equation becomes:

pwd-seed = H(base || counter)

The password element, PWE, generated using the shared credential shall be used as function f() from 11.6.12.2 and the encryption and decryption operations become:

 Encrypt: C = elem-op(P, PWE)

 Decrypt: P = elem-op(C, -PWE)

**References:**