IEEE P802.11
Wireless LANs

|  |
| --- |
| Security Requirements for Specification Framework |
| Date: 2012-03-08 |
| 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 submission specifies security requirements for the Specification Framework.

## 3. Security Framework

R.3.A The draft specification shall define a protocol for mutual authentication that is key generating and provides explicit key confirmation. The credential used for authentication shall be pre-existing.

R.3.B The mutual authentication protocol in the draft shall be resistant to active and passive attack. If the pre-existing credential is a shared secret, then either: 1) the protocol shall be defined to require that the probability of guessing the secret shall be no less than 2-80 ; or, 2) the protocol shall be resistant to dictionary attack.

R.3.C The mutual authentication protocol in the draft shall optionally support the feature that compromise of the pre-existing credential does not reveal data from past sessions.

**References:**