IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of CIDs 4773 and 4774 | | | | |
| Date: 2016-02-18 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 1322 Crossman ave, Sunnyvale, California, United States of America | 408-555-1212 | dharkins at arubanetworks dot com |
|  |  |  |  |  |

Abstract

This submission proposes resolution of CIDs 4773 and 4774.

CIDs 4773 and 4774 both have identical comments of “What is ‘ikm’?” with identical proposed changes of “Delete or define”

Discussion: Deletion is out of the question as that would leave a missing parameter in the random function. Therefore the term is referred to as “input keying material”, which is what it stands for. The submitter is taking the liberty of defining “salt” in 12.10.1 as well since that is not defined and would probably result in a similar “Delete or define” comment in the next ballot.

***Instruct the editor to modify section 12.4.2 as indicated:***

**12.4.2 Assumptions on SAE**

SAE uses various functions and data to accomplish its task and assumes certain properties about each

function. These are as follows:

* H is an “extractor” function (see IETF RFC 5869) that concentrates potentially dispersed entropy from an input to create an output that is a cryptographically strong, pseudorandom key. This function takes as input a non-secret “salt” and a secret input keying material “ikm” and produces a fixed-length output.
* CN is a confirmation function that takes a secret key and data to confirm and bind to the exchange.
* A finite cyclic group is negotiated for which solving the discrete logarithm problem is computationally infeasible.

When used with AKMs 00-0F-AC:8 or 00-0F-AC:9 from Table 9-132 (AKM suite selectors), H is

instantiated as HMAC-SHA-256:

H(salt, ikm) = HMAC-SHA-256(salt, ikm)

***Instruct the editor to modify section 12.10.1 as indicated:***

**12.10.1 AP PeerKey overview**

When used with AKM 10 from Table 9-132 (AKM suite selectors) to indicate AP PeerKey, H shall be instantiated as HMAC-SHA-256, taking as input a non-secret “salt” and a secret input keying material “ikm”:

H(salt, ikm) = HMAC-SHA-256(salt, ikm)

Other instantiations of function H require creation of a new AKM identifier.

**References:**