IEEE P802.11
Wireless LANs

|  |
| --- |
| May or May Not? That is the Question |
| Date: 2019-05-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins  | HPE | 3333 Scott boulevardSanta Clara, California,United States of America |  |  |
|  |  |  |  |  |

Abstract

This submission proposes a clarifying change, with justification, for a comment based on some confusing language.

Discussion:

There are security implications in the action being discussed in this text. The implementers who read this standard will not have had the benefit of being in the room while this was being discussed and may not understand the factors involved in making the decision. Therefore it is necessary to add a short sentence discussing one reason why one may decide to retain the cached PMKSA.

***Instruct the editor to modify section 12.12.2.6.2 as indicated:***

**12.12.2.6.2 (Re)Association Request for FILS key confirmation**

If authentication is deemed a failure, ICK, KEK, TK, and the PTKSA shall be irretrievably deleted and the AP shall return an Authentication frame with a status code set to 112 (Authentication rejected due to FILS authentication failure). If PMKSA caching was not being employed for this failed authentication attempt, the PMKSA shall also be deleted. If PMKSA caching was being employed, the reason for failure might be an impersonation attack. Therefore, when FILS with PMKSA caching fails, the AP may decide to retain the cached PMKSA.

**References:**