IEEE P802.11
Wireless LANs

|  |
| --- |
| PMKSA Caching with SAE |
| Date: 2014-11-04 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  |  |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA, United States of America | +1 408 227 4500 | Dharkins at aruba networks dot com |

Abstract

The behaviour for performing PMKSA Caching with a PMKSA established by SAE is ambiguous. This submission clarifies the expected behaviour.

***Instruct the editor to modify section 11.5.10.3 as indicated:***

**11.5.10.3 Cached PMKSAs and RSNA key management**

If a STA in an ESS has determined it has a valid PMKSA with an AP to which it is about to (re)associate, it performs Open System authentication to the AP, and then it includes the PMKID for the PMKSA in the RSNE in the (Re)Association Request. When the PMKSA was not created using pre-authentication, the AKM indicated in the RSNE by the STA in the (Re)Association Request shall be identical to the AKM used to establish the cached PMKSA in the first place.

Upon receipt of a (Re)Association Request frame with one or more PMKIDs, an AP checks whether its Authenticator has retained a PMK for the PMKIDs, whether the AKM in the cached PMKSA matches the AKM in the (Re)Association Request, and whether the PMK is still valid; and if so, it shall assert possession of that PMK by beginning the 4-Way Handshake after association has completed. If the Authenticator does not have a PMK for the PMKIDs in the (Re)Association Request, its behavior depends on how thePMKSA was established. If SAE authentication was used to establish the PMKSA, then the AP STA shallreject (re)association by sending a (Re)Association Response frame with status code STATUS\_INVALID\_PMKID. Note—This allows the non-AP STA to fall back to full SAE authentication to establish another PMKSA. . IfIEEE Std 802.1X authentication was used to establish the PMKSA, the AP begins a full IEEE Std 802.1X authentication after association has completed.

If both sides assert possession of a cached PMKSA, but the 4-Way Handshake fails, both sides may delete the cached PMKSA for the selected PMKID.

**References:**