IEEE P802.11
Wireless LANs

|  |
| --- |
| FILS Association Response RSNE |
| Date: 2019-05-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

Review of the proposed ways of extending RSNE discovered an issue in how IEEE Std 802.11ai-2016 described the mechanism for a non-AP STA to verify that that RSNE in unprotected frames (Beacon, Probe Response, Authentication frame) from the AP matches a protected version (which was supposed to be in (Re)Association Response frame when FILS authentication is used). The rules for the non-AP STA were included, but the (Re)Association Response frame construction was not updated to match this. If one were to implement a FILS AP following the current standard, a FILS STA compliant with the current standard would reject the (Re)Association Response frame from that AP. This contribution discusses this issue and proposed changes to address the missing details in the standard.

**Discussion**

FILS authentication does not use 4-way handshake and as such, cannot use EAPOL-Key msg 3/4 as the protected location for verifying AP’s RSNE. Instead, (Re)Association Response frame is used for this since those frames are protected using AES-SIV (RSNE being in the unencrypted, but integrity protected, AAD). P802.11ai described construction of (Re)Association Response frames as follows:

**12.12.2.6.3 (Re)Association Response for FILS key confirmation**

The AP constructs a (Re)Association Response frame for FILS authentication per 9.3.3.6 (Association

Response frame format) and 9.3.3.8 (Reassociation Response frame format).

This subclause also describes the non-AP STA steps for validating RSNE:

The STA verifies that the RSNE received in the (Re)Association Response frame has identical AKM suites

and cipher suites and RSN capabilities as were included in the RSNE in the Beacon, Probe Response, and

Authentication frames from the AP. If these fields differ, authentication fails.

However, P802.11ai missed changes in the frame format subclauses 9.3.3.6 and 9.3.3.8 to include the RSNE in FILS authentication cases. This results in inconsistent behavior between AP and non-AP STA that would result in (Re)Association Response frame being rejected by the non-AP STA.

**Proposed changes**

*Add a new row immediately before the Order=10 Information=Mobility Domain row in Table 9-37—Association Response frame body (REVmd/D2.2 P858 L11) and increment the Reorder column value by one for all the following rows:*

Order: 10

Information: RSN

Notes: The RSNE is present if dot11FILSActivated is true; otherwise not present.

*Change the Order=10 Information=RSN row in Table 9-39—Reassociation Response frame body (REVmd/D2.2 P864 L6:*

Order: 10

Information: RSN

Notes: An RSNE is present in a Reassociation Response frame if dot11FastBSSTransitionActivated is true, dot11RSNAActivated is true, and this frame is a response to a Reassociation Request frame that contained an FTE (i.e., part of a fast BSS transition in an RSN); or if dot11FILSActivated is true. Otherwise, not present.