IEEE P802.11
Wireless LANs

|  |
| --- |
| RSNXE validation in FILS association |
| Date: 2024-11-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

IEEE Std 802.11ai-2016 was developed at around the same time when the RSNXE was added, and while the validation of the AP’s RSNE was covered as a step in FILS association (key confirmation), no rules were defined for validating the AP’s RSNXE, and such rules were not added when incorporating IEEE Std 802.11ai-2016 into IEEE Std 802.11-2020 either (or for -2024).

While IEEE Std 802.11-2020 did define the RSNXE to be included in the (Re)Association Response frames, that rule was not in place when IEEE Std 802.11ai-2016 was published. There has been at least one known implementation of FILS authentication where the AP might have included the RSNXE in the Beacon and Probe Response frames, but not in the (Re)Association Response frame if the non-AP STA did not include an RSNXE in the (Re)Association Request frame. Strict validation of consistent RSNXE use might result in interoperability issues with such an AP implementation. Deployment of such an implementation with the RSNXE getting included in the Beacon and Probe Response frames and the non-AP STA not including the RSNXE in the (Re)Association Request frame might be unlikely, but nevertheless, it might be justifiable to note this possible interoperability issue when adding a new expectation for validating the RSNXE.

## Proposed changes

### 12.11.2.6.3 (Re)Association Response for FILS key confirmation

*Modify 12.11.2.6.3 (REVme/D7.0 page 3160 lines 19-22) as follows:*

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. Additionally, the STA verifies that the AP included the RSNXE consistently in the Beacon, Probe Response, and (Re)Association Response frames it received from the AP. If the AP included an RSNXE in any of those frames, but not in all those frames, or if the RSNXE is not identical in those frames, authentication fails.

NOTE—A known AP implementation does not include an RSNXE in the (Re)Association Response frame despite including an RSNXE in Beacon frames if a non-AP STA does not include an RSNXE in the (Re)Association Request frame. The non-AP STA might allow authentication to succeed in such a case.