IEEE P802.11
Wireless LANs

|  |
| --- |
| CID 1243 – LB258 802.11REVme  |
| Date: 2022-08-23 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Joseph LEVY | InterDigital, Inc. | 111 W 35th St., NY, New York | +1 631.622.4239 | joseph.levy@interdigital.com |
|  |  |  |  |  |

Abstract

This document provides a proposed resolution for CID 1243 from LB258.

This contribution addresses:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Page(C)** | **Line(C)** | **Clause** | **Comment** | **Proposed Change** |
| 1243 | Joseph Levy | 3221 | 14 | 12.7.6.4 | "The Supplicant also:" is not a required action for this requirement. | Change: "The Supplicant also:"To be: "The Supplicant shall also:" |

**Discussion:**

This CID was discussed at the Tuesday 23 Aug 2022 TGme ad hoc meeting in San Diego, where it was agreed in principle, but it was noted that the tense of the verbs in the following bullets need to be changed.

**Resolution:**

Revised

Agree that a “shall” should be added, but to do so the tense of the verbs in the following bullets need to be modified. The modifications are provided in [11-22/1378r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1378-00-000m-cid-1243---lb258-802-11revme.docx).

**Proposed text changes (redlined):**

The Supplicant shall also:

* Verify the RSNE and, if present, the RSNXE. If this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the Supplicant verifies that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and verifies that all other fields of the RSNE are identical to the fields in the RSNE present in the Beacon or Probe Response frames and verifies that the FTE and MDE are the same as in the (Re)Association Response frame. Otherwise, the Supplicant verifies that the RSNE is identical to that the STA received in the Beacon or Probe Response frame. If the RSNXE is present, the Supplicant verifies that the RSNXE is identical to that the STA received in the Beacon or Probe Response frame. If any of these verification steps indicates a mismatch, the STA shall disassociate or deauthenticate. If a second RSNE is provided in the message, the Supplicant uses the pairwise cipher suite specified in the second RSNE or deauthenticates.
* Verify the message 3 MIC or AEAD decryption operation result. If the calculated MIC does not match the MIC that the Authenticator included in the EAPOL-Key frame or AEAD decryption operation returns failure, the Supplicant silently discards message 3.
* Update the last-seen value of the Key Replay Counter field.
* If the Extended Key ID for Individually Addressed Frames subfield of the RSN Capabilities field is 1 for both the Authenticator and Supplicant: Use the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to receive individually addressed MPDUs protected by the PTK with the assigned Key ID.
* Construct message 4.
* Send message 4 to the Authenticator.
* Use the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to send and, if the receive key has not yet been installed, to receive individually addressed MPDUs protected by the PTK. The GTK is also configured by MLME-SETKEYS primitive. (11ba)If WUR frame protection is negotiated, the WTK, and if applicable the WIGTK, is also configured by using the MLME-SETKEYS primitive.

**References:**