IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 802.11 REVmd LB236 comment resolutions | | | | | |
| Date: 2019-05-31 | | | | | |
| Author(s): | | | | | |
| Name | Company | Address | Phone | email |
| Michael Montemurro | BlackBerry Ltd | 4701 Tahoe Blvd, Mississauga, ON. CANADA. L4W 0B4 | +1-289-261-4183 | [mmontemurro@blackberry.com](mailto:mmontemurro@blackberry.com) |

**Abstract**

This document contains some proposed resolutions to REVmd LB236 comments.

## 

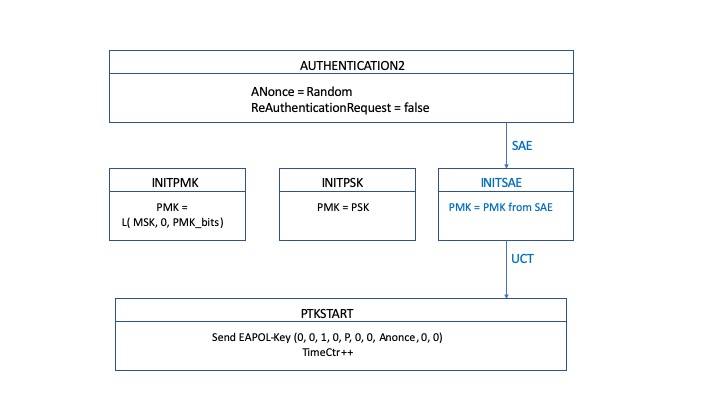
# Comments

### CID 2207

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2207 | 2650.00 | 12.7.10.1 |  |  | Authenticator state machine does not include possibility of getting PMK from SAE. There is only INITPMK and INITPSK states for setting PMK. The SAE case (PMK derived as part of Authentication frame exchange) does not seem to be covered. | Add INITSAE state next to the INITPSK state with "PMK = PMK from SAE" contents and UCT transition to PTKSTART. AUTHENTICATION2 state to INITSAE state transition condition set to "SAE". On page 2653 line 42, replace "INITPMK or INITPSK" with "INITPMK, INITPSK, or INITSAE". On page 2653 line 26, add "INITSAE: This state is entered when SAE authentication is completed successfully." |

#### Discussion:

* The changes would look like this:



* The text changes look like:
  + 2653.26:

— INITPMK : This state is entered when the IEEE 802.1X backend AS completes successfully. If a

PMK is supplied, it goes to the PTKSTART state; otherwise, it goes to the DISCONNECTED state.

— INITPSK: This state is entered when a PSK is configured.

— INITSAE : This state is entered when SAE authentication is completed successfully.

* + 2653.42:

— PTKSTART: This state is entered from INITPMK, INITPSK or INITSAE to start the 4-way handshake or if no response to the 4-way handshake occurs.

#### Proposed Resolution:

Accepted.

### CID 2499

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2499 | 667.00 | 6.3.94.2.2 |  |  | "N/A" does not make sense as a valid range for the Key ID | Copy the Valid range cell from the table in 6.3.19.1.2 |

#### Discussion:

* From 12.5.5.3.2

“The PN is incremented by a positive number for each MPDU. The PN shall be incremented in steps of 1 for

constituent MPDUs of fragmented MSDUs and MMPDUs. The PN shall never repeat for a series of

encrypted MPDUs using the same temporal key.

If the PN is larger than dot11PNExhaustionThreshold, an MLME-PN-EXHAUSTION.indication primitive

shall be generated.”

* The valid range of the Key ID from 6.3.19.1.2 is:

“0–3 shall be used with WEP, TKIP, CCMP, and GCMP; 4–5 with BIP; and 6–4095 are reserved”

* However, the primitive MLME-PN-EXHAUSTION is only specified form CCM, GCM and BIPencapsulation, so the valid range would be 0-3 based on 6.3.19.1.2.

#### Proposed Resolution:

Revised. At the cited location replace “N/A” with “0-3 shall be used with CCMP and GCMP; 4-5 with BIP for IGTK; 6-7 with BIP for BIGTK; and 8-4095 are reserved”

### CID 2500

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2500 | 668.00 | 6.3.94.3.2 |  |  | "N/A" does not make sense as a valid range for the Key ID | Copy the Valid range cell from the table in 6.3.19.1.2 |

#### Discussion:

* The MLME-PN-WARNING was added between 802.11-2012 and 802.11-2016. However the behavioral text was removed in CID 59 (removal of DLS-STSL) inadvertently. See <https://mentor.ieee.org/802.11/dcn/17/11-17-1518-03-000m-resolution-cids-59-62-remove-dls-stsl.docx>
* PNs only apply to CCMP and GCMP encapsulation so the text in 6.3.19.1.2 should not be copied.
* Feedback from Jouni: “it should be noted that MLME-PN-WARNING.indication and MLME-PN-EXHAUSTION.indication primitives apply to Group (GTK), Pairwise (TK), and Group Management (IGTK) keys. The current standard is somewhat inconsistent on that and the proposed resolution for CID 2500 is bringing back the previously deleted text that does not seem to cover the IGTK case. In other words, IGTKSA should be added to this text just like GTKSA is handled now. Furthermore, 12.6.18 should cover IGTKSA (REVmd/D2.0 P2599 L25). In addition to that, only GCMP is currently documented to issue MLME-PN-EXHAUSTION.indication (12.5.5.3.2). That should cover MLME-PN-WARNING.indication and CCMP (12.5.3.4.2) and BIP (12.5.4.5) description should cover both.”

#### Proposed Resolution:

Revised. Relative to D2.0, at the cited location replace “N/A” with “0-3 shall be used with CCMP and GCMP; 4-5 with BIP for IGTK; 6-7 with BIP for BIGTK; and 8–4095 are reserved”

In Clause 12.5.3.4.2 insert the following paragraph at 2564.39, insert the following paragraph:

“If the PN is larger than dot11PNExhaustionThreshold, an MLME-PN-EXHAUSTION.indication primitive

shall be generated.”

In Clause 12.5.4.4 (p2572.8), insert the following text before the NOTE:

“If the PN is larger than dot11PNExhaustionThreshold, an MLME-PN-EXHAUSTION.indication primitive

shall be generated.”

In Clause 12.6.18 (p.2599.25) insert the following paragraph:

“When a STA’s SME receives an MLME-PN-EXHAUSTION.indication primitive and the PN is associated with an IGTKSA, the STA’s SME shall delete the IGTKSA.”

At the end of Clause 12.6.21, add the following text (to reinstate the behavioral text that was inadvertently deleted):

“An Authenticator may initiate a 4-way handshake for the purpose of renewing the key associated with a PTKSA. A supplicant may send an EAPOL request message to the authenticator to request rekeying. In addition, if both the Authenticator and the Supplicant support multiple keys for individually addressed traffic, a smooth switchover to the new key is possible using the following procedure.

The IEEE 802.11 MAC shall issue an MLME-PN-WARNING.indication primitive when the packet number assignment for a particular PTKSA, IGTKSA, GTKSA or BIGTKSA reaches or exceeds the threshold that is defined in dot11PNWarningThresholdLow and dot11PNWarningThresholdHigh for the first time. The indication shall be issued only once for a given PTKSA, IGTKSA, GTKSA or BIGTKSA. The SME may use the indication as a trigger to establish a new PTKSA, IGTKSA, GTKSA or BIGTKSA before the Packet Number space is exhausted.

A PTKSA has a limited lifetime, either in absolute time or due to exhausting the PN space. To maintain an uninterrupted security association, a STA should establish a new PTKSA prior to the expiration of the old PTKSA.

When both ends of the link support extended Key IDs for individually addressed frames, it is possible to install the new PTKSA without data loss, provided the new PTKSA uses a different Key ID from the old PTKSA. Data loss might occur if the same Key ID is used because it is not possible to precisely coordinate (due to software processing delays) when the new key is used for transmit at one end and when it is applied to receive at the other end. If a different Key ID is used for the new PTKSA, then provided the new key is installed at the receive side prior to its first use at the transmit side there is no need for precise coordination. During the transition, received packets are unambiguously identified using the Key ID as belonging to either the old or new PTKSA.”

### CID 2507

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2507 |  |  |  |  | "into its IEEE 802.11 MAC" is weird. It looks from other cases that "STA" is intended, i.e. Supplicant/MGTK recipient is considered to be part of the SME | Change "MAC" to "STA" in "into its IEEE 802.11 MAC" in 12.7.7.2 and 14.6.3. After the change in 14.6.3 add a "NOTE---The MGTK recipient is part of the SME." |

#### Discussion:

* See 12.2.4 a) 6) - It protects the data link by programming the negotiated cipher suites and the established temporal key into the MAC…
* Encryption keys are stored in the MAC.
* A GTKSA would be created by the SME, but the keys would be stored in the MAC. Therefore the note in the proposed resolution is not required.

#### Proposed Resolution:

Revised. Relative to D2.0,

At 2637.31, change “into its IEEE 802.11 MAC” to “into the MAC”

At 2764.44, change “into its IEEE 802.11 MAC” to “into the MAC”

Relative to D2.2

Change “IEEE 802.11 STA” to “IEEE 802.11 MAC” at 2632.3/6 and 2635.53/56

### CID 2550

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2550 | 417.00 | 6.3.19.1.4 |  |  | "When the Key Type is Group or IGTK, and the key matches the existing GTK or IGTK installed as a result of exiting WNM sleep mode (see 11.2.3.16.1 (WNM sleep mode capability)), if any, or matches the existing GTK or IGTK installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation considerations))" -- missing an "if any" for the second case. Also not clear what "existing" means here | Change the cited text at the referenced location to "When the Key Type is Group or IGTK, and the key matches the GTK or IGTK, if any, installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation considerations)) or of exiting WNM sleep mode (see 11.2.3.16.1 (WNM sleep mode capability))" |

#### Discussion:

* Modified Text: “When the Key Type is Group or IGTK, and the key matches the ~~existing~~ GTK or IGTK, if any, installed as  
  a result ~~of exiting WNM sleep mode (see 11.2.3.16.1 (WNM sleep mode capability)~~), if any, or matches the  
  ~~existing~~ GTK or IGTK, if any, installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key  
  handshake implementation considerations)) or of existing WNM sleep mode (see 11.2.3.16.1 (WNM sleep mode capability))”
* The change looks to be correct.

#### Proposed Resolution:

Accepted.

### CID 2573

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 2573 |  |  |  |  | There are references to a "PMKID field" but no such field exists | Change "PMKID field" to "PMKID List field" throughout |

#### Discussion:

* This is a duplicate of CID 2205, which has already been accepted.

#### Proposed Resolution:

Accepted. Duplicate of CID 2205.