IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 802.11 TGbh  CID resolutions on D2.0 | | | | |
| Date: 2024-01-17 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Stephen Orr | Cisco | New York | 8458634028 | sorr@cisco.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions to the following comments:

CIDs 48,181,183,184, 236

# Revision History

R0 – Iinitial version

# Draft version

Changes are relative to TGbh D2.0.

# Ready for Discussion

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/**  **Line** | **Comment** | **Proposed Change** |
| 48 | Michael Montemurro | 12.3.7 | 39.41 | In 802.11, protocol data is referred to as "elements" not "information elements" | at the cited location, change "information elements" to "elements" |

**Discussion:**

**Current text:**

*KEK is used to provide encryption for certain Information Elements in PASN frames, as defined in*

*12.13.3.2 PASN frame construction and processing. Its length is defined in Table 12-11 (Integrity*

*and key wrap algorithms)*

Suggested new text (changes shown):

*KEK is used to provide encryption for certain elements in PASN frames, as defined in*

*12.13.3.2 PASN frame construction and processing. Its length is defined in Table 12-11 (Integrity*

*and key wrap algorithms)*

In IEEE Std 802.11 there are currently 10 references to Information Elements (specifically FTM Synchronization information element), however “elements” is the more consistent term used throughout the standard.

**Proposed Resolution:**

Accept

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/**  **Line** | **Comment** | **Proposed Change** |
| 181 | Mark RISON | 12.13.7 | 39.37 | "KCK is the first 256 bits of the PTK" is duplication of the previous line | Delete the cited text |

**Current text:**

****

**Discussion:**

The text on line 37 is a description of line 36.

This is consistent with the text from 802.11-REVme/D4.1 (page 3097.41)).

**12.13.7 PTKSA derivation with PASN authentication**

**….**

Text

Description automatically generated with low confidence

…

However to be consistent with the rest of 802.11 this is redundant should be removed.

**Proposed Resolution:**

Accept

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/**  **Line** | **Comment** | **Proposed Change** |
| 183 | Mark RISON | 12.13.7 | 39.49 | "This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets." -- at best this duplicates the previous sentence "length is the same as a key for the pairwise cipher in RSNE provided  by the AP in the second PASN frame", at worst it contradicts it | Delete the first cited text |

**Current text:**

TK is the transient key whose length is the same as a key for the pairwise cipher in RSNE provided by the AP in the second PASN frame. This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets.

**Discussion:**

Current text is consistent with 802.11-REVme/D4.1 (3097.46).

**12.13.7 PTKSA derivation with PASN authentication**

**…**

TK is the transient key whose length is the same as a key for the pairwise cipher in RSNE provided by the AP in the second PASN frame. This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets.

**…**

Suggested new text (changes shown):

TK is the transient key whose length is the same as a key for the pairwise cipher in RSNE provided by the AP in the second PASN frame. ~~This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets.~~

Removing the text "This length is 16 octets for all ciphers, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which it is 32 octets." would make this more extensible if there are any future changes in cipher suites selectors.

**Proposed Resolution:**

Accept

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/**  **Line** | **Comment** | **Proposed Change** |
| 184 | Mark RISON | 12.13.17 | 39.60 | "The Key ID in the PTKSA (see 12.6.1.1.6 (PTKSA)) resulting from PASN authentication shall be 3 0." -- not clear. Shall be 30? Does that fit? Why 30? | Clarify |

**Current text:**

The Key ID in the PTKSA (see 12.6.1.1.6) resulting from PASN authentication shall be 3 0.

**Discussion:**

The text in this CID is consistent with what is currently in 802.11REVme/D4.1 (3097.60):

**12.13.7 PTKSA derivation with PASN authentication**

**…**

The Key ID in the PTKSA (see 12.6.1.1.6) resulting from PASN authentication shall be 3 0.

**…**

The current REVme D4.2 (12.13.7) is not clear onwhat the Key ID value will be in the PTKSA resulting from PASN authentication. 12.6.11.6 PTKSA is also not clear on what the Key ID will be.

**Proposed Resolutions:**

Request a contribution/input from a PASN expert.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/**  **Line** | **Comment** | **Proposed Change** |
| 236 | Okan Mutgan | 12.7.3 | 35.44 | Modify the note in Table 12-11--Integrity and key wrap algorithms (used for PASN) | As in comment. |

**Discussion:**

There is a question about the “Note” in Table 12-11

Current TGbhD2.0 additions to table 12-11

Table

Description automatically generated

**Table 12-11 from 802.11REVme/D4.1**

**Table

Description automatically generated**

The “Note” already exists in current REVme D4.1

**Proposed Resolutions:**

Reject

The “Note” already exists in current REVme D4.1 and Clause 12.2.12.3 Encryption of Device ID IE and IRM IE in PASN explicitly mentions how to use KEK for PASN frame protection.