IEEE P802.11
Wireless LANs

|  |
| --- |
| Putting TKIP in Its Place |
| Date: 2022-02-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission resolves several CIDs—1076, 1077, and 1079—that all advise that references to TKIP be removed from RSN sections and be dealt with as a non-RSN mode.

**CID 1077**

Comment: put TKIP with WEP in a non-RSNA section.

Proposed Change: Title 12.3 as “Non-RSNA security methods” and then move 12.5.2 into that section.

Discussion: TKIP is really not an RSNA. It’s used in a TSN where the pairwise cipher is TKIP and the group cipher is WEP, so this CID is a bit more expansive than it proposes. WEP is deprecated, so we should probably not talk about TSNs in the RSN security association management section.

In addition to doing what the CID proposes, it is also proposed to move discussion of TSN policy selection from 12.6 into the newly revised 12.3.

Resolution:

*Instruct the editor to modify section 12.3 as indicated:*

**12.3 Non-RSNA security methods**

**12.3.1 Overview**

Non-RSNA security methods consist of pre-RSNA security mechanisms and TSN security mechanisms.

Except for Open System authentication, all pre-RSNA security mechanisms are obsolete. Support for them might be removed in a later revision of the standard. TSN security mechanisms are deprecated and may be obsoleted in a later revision of the standard.

Open System authentication shall not be used between mesh STAs.

*Further instruct the editor to move 12.5.2 to a new section 12.3.4, renumbering 12.5 as required.*

**CID 1076**

Comment: TKIP is not an RSNA protocol

Proposed Change: remove mention of TKIP as an RSNA, remove the paragraph on lines 15-18 too.

Discussion: TKIP is deprecated so the paragraph talking about it being optional for an RSNA is obviously dated.

Resolution: Accept

*Instruct the editor to further modify section 12.5 as indicated:*

**12.5 RSNA confidentiality and integrity protocols**

**12.5.1 Overview**

This standard defines the following RSNA data confidentiality and integrity protocols: CCMP, and GCMP. This standard defines the following integrity protocol for Management frames and for WUR Wake-up frames: BIP.

BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust Management frames and WUR Wake-up frames (see 29.10 (WUR frame protection)).

**CID 1079**

Comment: let's stop talking about how to use WEP and TKIP

Proposed Change: remove the paragraphs on the pages and lines this comment refers to.

Discussion: WEP is obsoleted, TKIP is deprecated. We should stop talking about how to use them because we are telling people they should not be used.

Resolution: Accept

**12.7.1 Key hierarchy**

**12.7.1.1 General**

An RSNA STA shall support at least one pairwise key for any <TA,RA> pair for use with enhanced data cryptographic encapsulation mechanisms. The <TA,RA> identifies the pairwise key, which does not correspond to any WEP key identifier.

**References:**