IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution for CID 63 “Remove pre-RSNA security”  |
| Date: 2017-09 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Davie, FL, USA. | 916 799 9563 | gsmith@srtrl.com |

Abstract

This submission proposes resolutions for CID 63

Green indicates material agreed to in the group,

yellow material to be discussed, red material rejected by the group and

cyan material not to be overlooked.

The “Final” view should be selected in Word.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Clause  | Page  | Line | Comment | Proposed |
| 63 | Graham Smith | 12.3.1 | 2062 | 6 | Time to remove all pre-RSNA security mechanisms other than Open System authentication? WEP | Remove |

CID 63 Pre-RSNA security methods

*2062.6 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.*

Hence delete WEP/TKIP and keep only the section on Open Authentication.

Discussion in Berlin:

* In practice WEP is deployed in many devices. TKIP relies on WEP things. (do not remove)
* WEP is broken and message needs to be sent to market (remove) Exists in the older versions if reference needed.
* Edits in obsolete clauses are not being corrected.
* Need to take legal advice. If WEP implemented and WEP removed, now “Non-compliant”. (IPR issue)
* 2001 first problems with WEP reported. Enough is enough after 16 years.
* Other Stds. announce a time period.
* Deprecate (11mb) – Obsolete (11mc) –
* TKIP is marked “Deprecated”.
* Could make announcement or liaison that 11md will remove WEP.

Straw Polls (Chicago rules):

1. Remove WEP as an independent cipher in TGmd 16/8
2. Remove WEP andTKIP in TGmd 15/6
3. Mark WEP and TKIP as Obsolete and will be removed 19/7
4. No change 0/25

So based on 4) change is needed. Obviously more discussion required but a ground swell to remove.

Point not brought up in Berlin:

* **“Certified” 11n and 11ac APs fail if they associate with WEP.**
* Hence, the market has made its decision, WEP and TKIP are gone. Why burden the Std. when older versions can still be used if information on WEP is required?

COMMENTER VIEWPOINT

Still worthwhile doing the work to remove (because it will happen sometime….)

So, after many hours, here are the removal instructions.

Note: After having carried out all changes, a search should be made for “WEP” and “TKIP” to check if I missed anything.

RESOLUTION

REVISED

***Note to Editor: 802.11REVmd\_D0.2 is the base.***

Make changes as per below:

P2058L15 12.2.1 Classes of security algorithm

“This standard defines one class of security algorithms for IEEE 802.11 networks:

— Algorithms for creating and using an RSNA, called *RSNA algorithms*

”

P2058L30 12.2.2 Security methods

P2063L1 Rename 12.3 “Open System authentication”

Delete 12.3.1 to 12.3.2.4, and heading 12.3.3.

Renumber 12.3.3.1 as 12.3.1

12.3.1 Overview

In an infrastructure BSS, a non-DMG STA shall complete an IEEE 802.11 authentication exchange prior to

association. A DMG STA not in an IBSS shall complete an IEEE 802.11 authentication exchange prior to

association when an authentication algorithm other than the Open System authentication algorithm is

requested. A DMG STA shall not perform an IEEE 802.11 authentication exchange using the Open System

authentication algorithm. A mesh STA shall not perform an IEEE 802.11 authentication exchange using the Open System. An IEEE 802.11 authentication exchange is optional in an IBSS.

All Authentication frames shall be individually addressed, as IEEE 802.11 authentication is performed

between pairs of STAs, i.e., group addressed authentication is not allowed. Deauthentication frames are

advisory and may be sent as group addressed frames.

Delete heading 12.3.3.2

Renumber 12.3.3.2 as 12.3.2 “General”

Renumber 12.3.3.2.2 as 12.3.3

Renumber 12.3.3.2.3 as 12.3.4

Delete 12.3.3.3 in its entirety

P2090L1 Delete 12.5.2 Temporal key integrity protocol (TKIP) in its entirety

12.6.3 RSNA policy selection in an infrastructure BSS

P2129L51 delete “.”

12.6.5 RSNA policy selection in an IBSS and for DLS

P2131L26 Delete “ .”

12.6.7 RSNA policy selection in an MBSS

P2132L60 Delete “.”

12.7.1.1. Key Hierachy

P2146L28 Delete

.

.

12.7.1.3 Pairwise key hierarchy

P2148L54 Delete NOTE 2

12.7.2 EAPOL-Key frames

P2159L47 delete as shown

“The value 1 shall be used for all EAPOL-Key frames to a STA when the negotiated AKM

is 00-0F-AC:1 or 00-0F-AC:2 and the pairwise cipher is "Use group cipher suite"

for Key Descriptor 1. This value indicates the following:

P2159L57 in ii) delete as shown

“and either the pairwise or the group cipher is an enhanced

data cryptographic encapsulation mechanism for Key Descriptor 2.

P2160L54 In 8) delete as shown

“Error (bit 10) is set by a Supplicant to report that a MIC failure occurred in an

SMK handshake failure.”

P2161L30 “Table 12-4—Cipher suite key lengths”

Delete first three rows – WEP-40, WEP-104, TKIP.

P2162L50 Just after “Table 12-5 Key RSC field”, delete “.”

12.7.3 EAPOL-Key frame construction and processing

P2167L20, edit as shown

“Table 12-8 (Integrity and key-wrap algorithms) indicates the particular algorithms to use when constructing

and processing EAPOL-Key frames. The AKM of “Deprecated” indicates an AKM of 00-0F-AC:1 or 00-

0F-AC:2 when “Use group cipher suite” is the negotiated pairwise cipher. For all other

AKMs the negotiated pairwise cipher suite does not influence the algorithms used to process EAPOL-Key

frames.”

12.7.6.6 4-way handshake implementation considerations

P2178L29 edit as shown

“An implementation should save the KCK and KEK beyond the 4-way handshake, as they are needed for

group key handshakes, and STK Rekeying.”

Figure 12-46 Sample 4-way handshake

P2179L23 Delete as shown in the lowest two boxes : “Set Temporal Encryption Key”

12.7.9.4.2 TPK handshake message 1

P2196L34, edit as shown

“The pairwise cipher suite list field indicating the pairwise cipher suites the TDLS initiator STA

is willing to use with the TPKSA..”

P2197L13, edit as follows:

“If none of the pairwise cipher suites are acceptable then the TDLS responder STA shall reject the TDLS Setup Request frame with

status code STATUS\_INVALID\_PAIRWISE\_CIPHER.”

12.7.10.3 Supplicant state machine variables

P2205L39 Delete NOTE

“.”

P2212L27 Delete “12.8.1 Mapping PTK to TKIP keys”

P2212L43 Delete “12.8.2 Mapping GTK to TKIP keys”

P2213L8 Delete “12.8.5 Mapping GTK to WEP-40 keys”

P2213L15 Delete “12.8.6 Mapping GTK to WEP-104 keys”

P2213L47 Delete “12.9.1 WEP frame pseudocode” in its entirety

12.9.2.2 Per-MSDU/Per-A-MSDU Tx pseudocode

P2215L62 delete:

P2216L16 delete as shown:

**else if** GTK entry for Key ID is not null **then**

Set the Key ID subfield of the IV field to the Key ID.

**if** MPDU has an individual RA **then**

discard the entire MSDU or A-MSDU and generate one or more MAUNITDATA-

STATUS.indication primitives to notify the LLC that the

MSDUs were undeliverable due to a null key

P2216L28 delete

12.9.2.4 Per-MPDU Tx pseudocode

P2218L36, delete

12.9.2.6 Per-MPDU Rx pseudocode

P2219L28 delete as shown

**if** key is null **then**

discard the frame body

P2219L39, edit as follows:

**endif**

12.9.2.8 Per-MSDU/Per-A-MSDU Rx pseudocode

P2224L14, delete:

P2224L47 delete:

14.5.2.1 Instance Pairwise Cipher Suite selection

P2309L33 Delete “”.

14.5.2.2 Group cipher suite selection

P2310L10 Delete “”

B.4.4.1 MAC protocol capabilities

P2871L36 Delete PC2 PC2.1 and PC2.2 entry

Delete PC34.1.2.2, PC34.1.2.2.1, PC34.1.2.2.2, PC34.1.2.2.3, PC34.1.2.2.4 rows.

Item PC 34.1.10

P2882L20-27 Delete

“12.5.2.1.2 (TKIP cryptographic encapsulation),

12.5.2.1.3 (TKIP decapsulation),

12.5.2.2 (TKIP MPDU formats),”

C.3 MIB detail

P3061L45 delete

“WEPKeytype ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION "Represents the type of WEP key."

SYNTAX OCTET STRING (SIZE (5))”

P3066L26

Delete “dot11PrivacyOptionImplemented” entirely

P3104 delete lines 10 to 65

P3105 delete lines 1 to 65

P3106 dlete lines 1 to 30

P3106 L58 edit as shown

dot11PrivacyInvoked TruthValue,

,

dot11ExcludeUnencrypted TruthValue,

,

dot11RSNAActivated TruthValue,

P3107L14 edit as shown

When this attribute is true, it indicates that some level of security is

invoked for transmitting Data frames..

For (#136)RSNA capable clients, an additional variable dot11RSNAActivated

indicates whether RSNA is enabled. If

dot11RSNAActivated is true, RSNA security mechanisms invoked are

configured in the dot11RSNAConfigTable.

P3107 delete Lines 24 to 51

P3108 delete lines 5 to 31

P3119 delete lines 22 to 35 “dot11RSNATKIPCounterMeasuresInvoked”

P3123L60 edit as shown “This object indicates the length of the pairwise cipher key. This should

be 128 or 256 for CCMP and 128 or 256 for GCMP."

P3126 delete lines 22 to 33 “dot11RSNAStatsTKIPICVErrors”

P2127 delete lines 16 to 26 “dot11RSNAStatsTKIPReplays”

Annex J

Delete “J.1 TKIP temporal key mixing function reference implementation and test vector” in its entirety.

Delete “J.6.2 WEP cryptographic encapsulation”

Delete “J.6.3 TKIP test vector”

J.7.1 General P3714L19 Delete as shown “The test vectors in this subclause provide an example of PTK derivation for CCMP-128.

Delete J.7.3 TKIP pairwise key derivation”

K2.2 Deriving Medium Time

P3737L63 edit as shown

Security Encapsulation Size = 16 (CCMP), 20 (GCMP), or 0 (open system)