IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution for WEP/TKIP removal CIDs  |
| Date: 2018-04 |
| 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 CIDs 1006, 1233, 1234, 1410, 1411, AND 1323

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.

R1 – Added 1323

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Clause  | Page  | Line | Comment | Proposed |
| 1006 | Graham Smith | 12.3.1 | 2310 | 51 | "Except for Open System authentication, all pre-RSNA security mechanisms are obsolete." This was considered on D0.1 CID 63 and rejected as "Known implementations.... in the market". 17/1504 details deletion changes. It was also noted that it should be re-considered in January 2018 (i.e. D1.0). Security is IMPORTANT and discouraging WEP and TKIP is IMPORTANT. Implementations using WEP are compliant to 802.11 - 2012 and maybe to 2016 so the reference and specification is available even though we are not keeping WEP and TKIP up to date by addressing comments for them. Latest developments in WFA on WPA3 are clear, DO NOT TEST WEP or TKIP and fail devices that allow WEP and TKIP. If vendors wish to support outdated security, that's fine, they can't be tested anyhow. Let's get rid of WEP and TKIP in our standard - why keep poor security in our Std. that is irresponsible. | Incorporate changes as described in 17/1504. Note Page and Line numbers will need to be checked to comply with D1.0 |
| 1233 | Guido Hiertz | 12.3.2 | 2311 | 1 | WEP provides no use as it is broken. | Remove WEP from the standard |
| 1234 | Guido Hiertz | 12.5.2 | 2338 | 1 | TKIP provides no use as it is insecure. | Remove TKIP from the standard |
| 1410 | Mark RISON | 12.3.3.3 | 2315 | 17 | WEP is obsolete and has not been maintained (comments on it in previous ballots were rejected on the basis it was obsolete and was going to be deleted), so implementations based on the current wording are likely to be erroneous | Delete Subclause 12.3.3.3 |
| 1411 | Mark RISON | 12.5.2 | 2338 | 19 | WEP is obsolete and has not been maintained (comments on it in previous ballots were rejected on the basis it was obsolete and was going to be deleted), so implementations based on the current wording are likely to be erroneous | Delete Subclause 12.5.2 |
| 1323 | Mark Rison | 12.3.3.3 | 2315 | 17 | It is confusing to have something called "FILS Shared Key authentication", as it sounds as if this is a special case of "Shared Key authentication" (a.k.a. WEP) | Delete Subclause 12.3.3.3 |

HISTORY

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 proposal was to 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.

Discussion in Orlando

* “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?
* This one gets complicated. Certified devices are not supposed to accept WEP connections, but we have a mixed mode WPA2/WPA mixed mode, then you have to do the group key using TKIP, but that would be hard because we still need TKIP. While this is the case, we cannot take TKIP out.
* We know that there known implementation of WEP and TKIP in the market. We should not remove at this time.
* The Group did not come to consensus on removal of these two features. Agreed to add a non-consensus sentence to the REJECT resolution.
* The need to make a decision by the close out in January, and so we could reject for now, and then bring it up at a later time if we feel it appropriate

POINTS

* WEP and TKIP are specified in 802.11-2007, 2012 and 2016 so any implementators can refer to those Standards – these past versions are readily available from IEEE (see over)
* Implementors will still be compliant (to previous Standards).
* WEP and TKIP are broken and insecure and are not being maintained. It is bad practice to keep these in the latest Standard.

It is therefore proposed to remove pre-RSNA from 802.11md

Note: After having carried out all changes, a search should be made for “WEP”, “TKIP” and “ARC4” to check if I missed anything.





RESOLUTION

REVISED

***Note to Editor: 802.11REVmd\_D1.0 is the base.***

Make changes as per below:

178. 41 delete “An RSN can be identified by the indication in the RSN element (RSNE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).”

182.53 delete “A TSN is identified by the indication in the robust security network element (RSNE) of Beacon frames that the group cipher suite in use is wired equivalent

privacy (WEP).”

187.36 delete WEP defininition.

200.8 Delete WEP line

242.12 delete “In a WLAN that does not support RSNA, two services, authentication and data confidentiality, are defined.

IEEE 802.11 authentication is used instead of the wired media physical connection. WEP encryption was

defined to provide the data confidentiality aspects of closed wired media.”

242.39 delete “Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key.”

244.17 edit as follows: “IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including: CCMP, and GCMP. CCMP and GCMP are based

on the advanced encryption standard (AES). A means is provided for STAs to select the algorithm(s) to be

used for a given association.”

244.65 delete footnote 20

270.52 delete “The use of WEP for confidentiality, authentication, or access control is deprecated. The WEP algorithm is unsuitable for the purposes of this standard.

The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard.

A STA that has associated with management frame protection enabled shall not use pairwise cipher suite selectors WEP-40, WEP-104, TKIP, or “Use group cipher suite.”

A mesh STA with dot11MeshSecurityActivated equal to true shall not use the pairwise cipher suite selectors WEP-40, WEP-104, or TKIP”

380.9 delete “WEP, TKIP,”

682.41 to 682.48 delete paragraph

1019.11 and 1019.22 delete “(WEP-40, WEP-104, and TKIP not allowed)”

1019.33 delete “WEP-40 group data cipher suites, optional RSN Capabilities field omitted:”

1019.38 delete “00 0F AC 01, // WEP-40 as group data cipher suite”

1019.56 delete “(WEP-40, WEP-104, and TKIP are not allowed)”

1020.52 replace “WEP-40” with “Reserved”

1020.53 replace “TKIP’ with “Reserved”

1020.59 replace “WEP-104” with “Reserved”

1021.40 to 1021.46 delete

1021.54 delete “other than TKIP, WEP-104, or WEP-40”

1022.8 Table 9-143—Cipher suite usage, delete rows for WEP-40, WEP-104, TKIP

1026.37 delete “If a STA supports WEP default key 0 simultaneously with a pairwise key (see 12.7.1 (Key hierarchy)), then the STA sets the No Pairwise subfield of the RSN Capabilities field to 0.

If a STA does not support WEP default key 0 simultaneously with a pairwise key (see 12.7.1 (Key hierarchy)), then the STA sets the No Pairwise subfield of the RSN Capabilities field to 1.”

1080.38 delete “For WEP, the RSC value is reserved.”

23.06 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*

”

2306.30 12.2.2 Security methods

2306.32

Pre-RSNA security comprises IEEE 802.11 entity authentication, described in 12.3.3 (Pre-RSNA authentication)

2306.39 delete” — TKIP, described in 12.5.2 (Temporal key integrity protocol (TKIP))”

2310.48 Rename 12.3 “Open System authentication”

Delete 12.3.1 to 12.3.2.4, and heading 12.3.3. in their entirety

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

2338.19 Delete 12.5.2 Temporal key integrity protocol (TKIP) in its entirety

2380.1 12.6.3 RSNA policy selection in an infrastructure BSS

delete “.”

2381.45 12.6.5 RSNA policy selection in an IBSS and for DLS

Delete “ .”

2383.12 12.6.7 RSNA policy selection in an MBSS

Delete “.”

2395.57 12.7.1.1. Key Hierachy, General

Delete

.

.

2398.47 Delete NOTE 2

2407.47 12.7.2 EAPOL-Key frames

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:

2407.57 in ii) delete as shown

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

data cryptographic encapsulation mechanism for Key Descriptor 2.

2408.54 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.”

2409.26 “Table 12-5—Cipher suite key lengths”

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

2410.41 Just after “Table 12-5 Key RSC field”, delete “.”

2414.51 12.7.3 EAPOL-Key frame construction and processing

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

2423.40 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

2424.22 Delete as shown in the lowest two boxes : “Set Temporal Encryption Key”

12.7.8.4.2 TPK handshake message 1

2432.14, 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..”

2432.57, 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.”

12.7.9.3 Supplicant state machine variables

2441.26 Delete NOTE

“.”

2448.4 Delete “12.8.1 Mapping PTK to TKIP keys”

2448.19 Delete “12.8.2 Mapping GTK to TKIP keys”

2448.49 Delete “12.8.5 Mapping GTK to WEP-40 keys”

2448.56 Delete “12.8.6 Mapping GTK to WEP-104 keys”

2449.27 Delete “12.9.1 WEP frame pseudocode” in its entirety

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

2451.44 delete:

2451.60 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

2452.12 delete

12.9.2.4 Per-MPDU Tx pseudocode

2454.18, delete

12.9.2.6 Per-MPDU Rx pseudocode

2454.61 delete “**and** increment dot11WEPExcludedCount”

2455.15 delete as shown

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

discard the frame body

2455.22, edit as follows:

**endif**

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

2459.63, delete:

2460.31 delete:

14.5.2.1 Instance Pairwise Cipher Suite selection

2544.33 Delete “”.

14.5.2.2 Group cipher suite selection

2545.10 Delete “”

B.4.4.1 MAC protocol capabilities

3226.6 Delete PC2 PC2.1 and PC2.2 entry

3234.6 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

3237.20 to 26 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

3446.43

Change “WEPKeytype ::= TEXTUAL-CONVENTION” STATUS to “Deprecated”

DESCRIPTION "Represents the type of WEP key."

SYNTAX OCTET STRING (SIZE (5))”

3451.11 Change STATUS “dot11PrivacyOptionImplemented” to “Deprecated”

3488.41 Change STATUS “dot11WEPDefaultKeysTable” to Deprecated

3488.54 Change STATUS “dot11WEPDefaultKeysEntry” to Deprecated

3489.6 Change STATUS “dot11WEPDefaultKeysIndex” to Deprecated

3489.16 Change STATUS “dot11WEPDefaultKeyValue” to Deprecated

3489.37 Change STATUS “dot11WEPKEYMappingsTable” to Deprecated

3489.52 Change STATUS “dot11WEPKEYMappingsEntry” to Deprecated

3490.7 Change STATUS “dot11WEPKEYMappingsIndex” to Deprecated

3490.16 Change STATUS “dot11WEPKEYMappingsAddress” to Deprecated

3490.25 Change STATUS “dot11WEPKEYMappingsWEPOn” to Deprecated

3490.34 Change STATUS “dot11WEPKEYMappingValue” to Deprecated

3490.42 Change STATUS “dot11WEPKEYMappingStatus” to Deprecated

3491.19 edit as shown

dot11PrivacyInvoked TruthValue,

,

dot11ExcludeUnencrypted TruthValue,

,

3491.39 edit as shown

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

invoked for transmitting Data frames..

For 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.

3491.50 Change STATUS “WEPDefaultKeyID” to Deprecated

3492.1 Change STATUS “WEPKeyMappingLengthImplemented” to Deprecated

3492.30 Change STATUS “WEPICVErrorCount” to Deprecated

3492.46 Change STATUS “WEPExcludeCount” to Deprecated

3503.38 Change STATUS “RSNATKIPCounterMeasuresInvoked” to Deprecated

3506.2 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."

3507.38 delete from list the following

dot11RSNAStatsTKIPICVErrors

dot11RSNAStatsTKIPLocalMICFailures

dot11RSNAStatsTKIPRemoteMICFailures

dot11RSNAStatsTKIPReplays

Annex J

4079 Delete “J.1 TKIP temporal key mixing function reference implementation and test vector” in its entirety.

4104.38 Delete “J.6.2 WEP cryptographic encapsulation”

4105.41 Delete “J.6.3 TKIP test vector”

4111.28 Delete as shown J.7.1 “The test vectors in this subclause provide an example of PTK derivation for CCMP-128.

4111.53 Delete J.7.3 TKIP pairwise key derivation”

K2.2 Deriving Medium Time

4134.63 edit as shown

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