IEEE P802.11
Wireless LANs

|  |
| --- |
| WEP removal |
| Date: 2022-11-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes resolution to the LB270 (REVme/D2.0) comment CID 3134 (remove WEP as a standalone cipher).

r1: Removed one missed instance of “mixed environment” in 12.7.4.

**CID 3134**

P2787 L37 12.3.2

Comment:

WEP was marked obsolete in IEEE Std 802.11-2020 and it should not have been used for anything for years. Following the IEEE 802.11 maintenance steps, it would appropriate to remove WEP from the standard as a part of REVme. However, it should be noted that the definition of TKIP depends on the definition of WEP and since TKIP was marked only deprecated in IEEE Std 802.11-2020 (and now obsolete in REVme), it and the dependencies for it should be left in for one more round. The WEP as a standalone mechanism and anything using WEP could be removed, though.

Proposed Change:

Replace 12.3.2.1 (WEP overview) (i.e., leave other 12.3.2.\* subclauses as-is) with following:
"WEP is an obsolete cipher that has been removed from the standard as a standalone mechanism. The following subclauses are included for the definition of TKIP."

At P2885 L19, delete "The <TA,RA> identifies the pairwise key, which does not correspond to any WEP key identifier."
Delete P2885 L22-L58.

At P228 L19, delete " that the group cipher suite specified is not wired equivalent privacy (WEP)"
At P240 delete L56-58 (definition of WEP).
At P255 L20, delete the WEP entry.
At P343 L46, delete "WEP is obsolete. The WEP algorithm is unsuitable for the purposes of this standard."
At P491 L22, delete "WEP, "
At P493 L4, delete "WEP, "
At P925 L46, delete "WEPUndecryptableCount and "
At P1038 L58, delete "For WEP, the RSC field is reserved."
At P2797 L55, delete "The ExtIV bit shall be 0 for WEP frames."
At P2780 L28, delete "WEP is obsolete. The WEP algorithm is unsuitable for the purposes of this standard."
At P2780 L37, delete "WEP, described in 12.3.2 (Wired equivalent privacy (WEP))"
At P2835 L52, delete ", compared to the 4 octets added to the MPDU header when WEP is used"
At P2903 L26, delete "For WEP, the RSC field is reserved."
At P2943 delete L47-60 (subclauses 12.8.5 and 12.8.6)
At P4633 delete L16-28 (PICS entry PC2 for WEP)
At P5644 L39, delete all of J.6.2 (WEP test vector)
At P5679 L1, delete "8 (WEP) "

At P525 L15, delete "the contents of dot11WEPDefaultKeysTable and dot11WEPKeyMappingsTable and "
At P525 L18, delete "there are no entries in the dot11WEPDefaultKeysTable, no entry for the current AP in dot11WEPKeyMappingsTable, and "
At P525 L24, delete "there are entries in the dot11WEPDefaultKeysTable, or an entry for the current AP in dot11WEPKeyMappingsTable, or "
At P525 L28, delete "that a WEP key is available, or "
Delete P4941 L9 - P4943 L25 (i.e., all of dot11WEPDefaultKeys and dot11WEPKeyMappings in the MIB)
At P4891 delete L6-10 (WEPKeytype)
At P4896 delete L23-33 (dot11PrivacyOptionImplemented in MIB)
At P4944 L9, delete "For WEP-only clients, the security mechanism used is WEP."
At P4944 L14, delete "dot11RSNAActivated is false or the MIB attribute does not exist, the security mechanism invoked is WEP; if "
Delete P4944 L20 - P4945 L26 (more WEP MIB variables).

Remove Shared Key authentication:
- at P311 L49, delete "Shared Key authentication relies on WEP to demonstrate knowledge of a WEP encryption key."
- at P312 L14, delete "In an RSN, Shared Key IEEE 802.11 authentication is not used."
- at P312 L43, delete "Shared Key, "
- at P730 delete L34-39 ("Shared Key" rows in Table 9-69)
- at P747 L36, delete "Authenticatyion algorithm number = 1: Shared Key"
- at P2430 L30, delete "or Shared Key authentication" and "or 12.3.3.3 (Shared Key authentication), respectively"
- at P2430 L59, delete "or Shared Key authentication" and "or 12.3.3.3 (Shared Key authentication), respectively"
- at P2431 L25, delete "12.3.3.3 (Shared Key authentication), "
- at P2431 L30, delete "12.3.3.3 (Shared Key authentication), "
- at P2783 L47, delete "An RSNA STA shall not associate if Shared Key authentication was invoked prior to RSN association."
- at P2784 L62-63, delete "Authentication frames with Authentication Algorithm Number field equal to 1 (Shared Key) and Authentication Transaction Sequence Number field equal to 3."
- at P2790 L60-61 in 12.3.3.1, delete "Shared Key authentication is obsolete and support for this mode might be subject to removal in a future revision of the standard. Shared Key authentication is distinct from FILS Shared Key authentication."
- at P2791 L53, delete 12.3.3.3 (Shared Key authentication) including its subclauses
- at P4633 L9, delete PICS B4.4.4.1 item PC1.3 (Shared Key authentication)
- at P4642 L17, delete "12.3.3.3.5 (Shared Key authentication (first frame)), "
- at P4940 L44, delete "Value = 2: Shared key"

Remove TSN (= WEP as group cipher)
- at P234 delete L35-40 (definition of TSN)
- at P254 delete L32 (definition of TSN)
- at P969 delete L52-L55 (RSNE restrictions for WEP/TSN)
- at P977 replace L1-11 with "-- Bit 1: Reserved." (i.e., remove No Pairwise bit from RSN Capabilties)
- at P2787 L27, delete " and TSN security mechanisms"
- at P2787 L32, delete "TSN security mechanism are deprecated."
 (note: I have another comment that asks this "deprecated" to be changed to "obsolete")
- at P2867 delete L38-51 (all of 12.6.4)
- at P2869 delete L40-52 (all of 12.6.6)
- at P2885 delete L55-58
- at P4950 L14, replace "RSNA and TSN" with "RSNA"

Discussion:

See 1847r3 for an alternative approach that removes both WEP and TKIP. While those changes would not satisfy the intent of CID 3134, the changes in that document (with some additional cleanup and additions) could be used to address the comment if the group has sufficient support for that direction. The changes in redline below follow the direction proposed in CID 3134, but might not be an exact match.

Proposed Resolution:

REVISED. Remove WEP as a standalone cipher by incorporating changes under the “Changes for CID 3134” header in document <this document>.

**Changes for CID 3134**

**3.2 Definitions specific to IEEE Std 802.11**

*Modify the RSN definition in 3.2 (D2.0 P228 L19) as shown:*

robust security network (RSN): A security network that allows only the creation of robust security

network associations (RSNAs). An RSN can be identified by the indication in the RSN element (RSNE) of

Beacon frames.

*Delete the TSN definition in 3.2 (D2.0 P234 L35-40) as shown:*

*Delete the WEP definition in 3.2 (D2.0 P240 L56-58) as shown:*

**3.4 Acronyms and abbreviations**

*Delete the TSN acronym in 3.4 (D2.0 P254 L32) as shown:*

*Delete the WEP acronym in 3.4 (D2.0 P255 L20) as shown:*

**4.5.4 Access control and data confidentiality services**

**4.5.4.2 Authentication**

*Modify 4.5.4.2 (D2.0 P311 L49) as shown:*

…

IEEE Std 802.11 defines four IEEE 802.11 authentication methods: Open System authentication, FT authentication, simultaneous authentication of equals (SAE), and FILS authentication. Open System authentication admits any STA to the DS. FT authentication relies on keys derived during the initial mobility domain association to authenticate the stations as defined in Clause 13 (Fast BSS transition). SAE authentication uses finite field cryptography to prove knowledge of a shared password. FILS authentication allows for faster connection to the network for FILS non-AP STAs by providing authentication, association, and key confirmation information in an efficient number of frame exchanges (see 4.10.3.6 (AKM operations using FILS authentication)). The IEEE 802.11 authentication mechanism also allows definition of new authentication methods.

…

*Modify 4.5.4.2 (D2.0 P312 L14) as shown:*

…

SAE authentication and Open System IEEE 802.11 authentication are used by STAs in an RSN for an infrastructure BSS. FILS authentication can be used by FILS STAs in an RSN for an infrastructure BSS. SAE authentication, Open System IEEE 802.11 authentication, or no IEEE 802.11 authentication is used in an RSN for an IBSS. SAE authentication is used for an MBSS. In an RSN for DMG BSS, Open System IEEE 802.11 authentication is not used (12.2.4 (RSNA establishment)).

…

 **4.5.4.3 Deauthentication**

*Modify 4.5.4.2 (D2.0 P312 L14) as shown:*

The deauthentication service is invoked when an existing Open System, FT, SAE, or FILS authentication is to be terminated. Deauthentication is a station service.

…

**5.1.2 Security services**

*Modify 5.1.2 (D2.0 P343 L46) as shown:*

…

The use of TKIP is obsolete. 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 TKIP or “Use group cipher suite.”

A mesh STA with dot11MeshSecurityActivated equal to true shall not use the pairwise cipher suite selector TKIP.

An S1G STA shall not use the pairwise cipher suite selectors TKIP or “Use group cipher suite”.

**6.5.14 SetKeys**

**6.5.14.1 MLME-SETKEYS.request**

**6.5.14.1.2 Semantics of the service primitive**

*Modify Valid range column for Key ID in 6.5.14.1.2 (D2.0 P491 L22) as shown:*

0–3 shall be used with TKIP, CCMP, and GCMP; 4–5 with BIP for IGTK; 6-7 with BIP for BIGTK; 8–9 with BIP for WIGTK; and 10–4095 are reserved

**6.5.15 DeleteKeys**

**6.5.15.1 MLME-DELETEKEYS.request**

**6.5.15.1.2 Semantics of the service primitive**

*Modify Valid range column for Key ID in 6.5.15.1.2 (D2.0 P493 L4) as shown:*

0–3 shall be used with TKIP, CCMP, and GCMP; 4–5 with BIP for IGTK; 6-7 with BIP for BIGTK; 8–9 with BIP for WIGTK; and 10–4095 are reserved

**6.6.7 ESS status reporting**

**6.6.7.1.3 When generated**

*Modify 6.6.7.1.3 (D2.0 P525 L10) as shown:*

This primitive is generated when the ESS link to a network of APs is available to exchange Data frames. The generation of this primitive may vary depending on the setting of dot11RSNAOptionImplemented.

If dot11RSNAOptionImplemented is false, then the network does not use encryption. This event is generated upon receipt of an MLME-ASSOCIATE.confirm primitive with a result code of success.

If dot11RSNAOptionImplemented is true, then the network requires the use of encryption on the link. Before declaring that the link is ready to exchange Data frames, the convergence function receives an MLME-ASSOCIATE.confirm primitive with a result code of success and the SME emits an MLME-SETKEYS.request primitive. The latter primitive is used to determine that the RSN 4-way handshake has completed.

**9.3.3.11 Authentication frame format**

*Modify Table 9-69 in 9.3.3.11 (D2.0 P730 L34-39) as shown:*

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**9.4.1.1 Authentication Algorithm Number field**

*Modify 9.4.1.1 (D2.0 P747 L36) as shown:*

The Authentication Algorithm Number field indicates a single authentication algorithm. The length of the Authentication Algorithm Number field is 2 octets. The Authentication Algorithm Number field is shown in Figure 9-129 (Authentication Algorithm Number field format). The following values are defined for authentication algorithm number:

Authentication algorithm number = 0: Open System

Authentication algorithm number = 2: Fast BSS Transition

Authentication algorithm number = 3: Simultaneous Authentication of Equals (SAE)

Authentication algorithm number = 4: FILS Shared Key authentication without PFS

Authentication algorithm number = 5: FILS Shared Key authentication with PFS

Authentication algorithm number = 6: FILS Public Key authentication

Authentication algorithm number = 65 535: vendor specific use

NOTE—The use of this value implies that a Vendor Specific element is included with more information.

All other values of authentication algorithm number are reserved.

**9.4.2.24 RSNE**

**9.4.2.24.1 General**

*Modify 9.4.2.24.1 (D2.0 P967 L15) as shown:*

…

NOTE—The following represent sample elements:

IEEE 802.1X authentication, CCMP-128 pairwise and group data cipher suites (

TKIP not allowed):

30, // Element id, i.e., 48 in decimal

14, // Length in octets, i.e., 20 in decimal

01 00, // Version 1

00 0F AC 04, // CCMP-128 as group data cipher suite

01 00, // Pairwise cipher suite count

00 0F AC 04, // CCMP-128 as pairwise cipher suite

01 00, // Authentication count

00 0F AC 01, // IEEE 802.1X authentication

00 00 // No capabilities

IEEE 802.1X authentication, CCMP-128 pairwise and group data cipher suites (TKIP

not allowed), preauthentication supported:

30, // Element id, i.e., 48 in decimal

14, // Length in octets, i.e., 20 in decimal

01 00, // Version 1

00 0F AC 04, // CCMP-128 as group data cipher suite

01 00, // Pairwise cipher suite count

00 0F AC 04, // CCMP-128 as pairwise cipher suite

01 00, // Authentication count

00 0F AC 01, // IEEE 802.1X authentication

01 00 // Preauthentication capabilities

IEEE 802.1X authentication, CCMP-128 pairwise and group data cipher suites, preauthentication and two

PMKIDs:

30, // Element id, i.e., 48 in decimal

36, // Length in octets, i.e., 54 in decimal

01 00, // Version 1

00 0F AC 04, // CCMP-128 as group data cipher suite

01 00, // Pairwise cipher suite count

00 0F AC 04, // CCMP-128 as pairwise cipher suite

01 00, // Authentication count

00 0F AC 01, // IEEE 802.1X authentication

01 00, // Preauthentication capabilities

02 00, // PMKID count

01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10, // PMKID

11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 // PMKID

 (FT-)PSK or (FT-)SAE authentication, CCMP-128 pairwise and group data cipher suites,

GCMP-128 alternative pairwise data cipher suite and management frame protection with BIP-CMAC-128 as

group management cipher suite.

30, // Element id, i.e., 48 in decimal

2A, // Length in octets, i.e., 42 in decimal

01 00, // Version 1

00 0F AC 04, // CCMP-128 as group data cipher suite

02 00, // Pairwise cipher suite count

00 0F AC 04, // CCMP-128 as pairwise cipher suite

00 0F AC 08, // GCMP-128 as pairwise cipher suite

04 00, // Authentication count

00 0F AC 02, // PSK authentication

00 0F AC 04, // FT-PSK authentication

00 0F AC 08, // SAE authentication

00 0F AC 09, // FT-SAE authentication

80 00, // Management frame protection is enabled but not required

00 00, // PMKID count

00 0F AC 06 // BIP-CMAC-128 as group management cipher suite

**9.4.2.24.2 Cipher suites**

*Modify Table 9-189 (Cipher suite selectors) in 9.4.2.24.2 (D2.0 P968 L59) as shown:*

|  |  |  |
| --- | --- | --- |
| **OUI** | **Suite type** | **Meaning** |
| 00-0F-AC | 0 | Use group cipher suite |
| 00-0F-AC | 1 | Reserved |
| 00-0F-AC | 2 | TKIP |
| 00-0F-AC | 3 | Reserved |
| 00-0F-AC | 4 | CCMP-128 |
| 00-0F-AC | 5 | Reserved |

*Modify 9.4.2.24.2 (D2.0 P969 L52) as shown:*

…

Use of any group cipher suite other than TKIP with TKIP as the pairwise cipher suite is not supported.

*Modify 9.4.2.24.2 (D2.0 P970 L1) as shown:*

If an AP advertises a group cipher suite other than TKIP, then the AP supports pairwise keys, and thus the pairwise suite selector 00-0F-AC:0 (Use group cipher suite) is not a valid option.

*Delete Table 9-187 (Cipher suite usage) rows WEP-40 and WEP-104 (D2.0 P970 L20).*

**9.4.2.24.4 RSN capabilities**

*Replace “No Pairwise” with “Reserved” in Figure 9-350 B1 column (D2.0 P977 L43).*

*Modify 9.4.2.24.4 (D2.0 P978 L1-11) as shown:*

Bit 1: Reserved.

**9.4.2.21.9 STA Statistics report**

*Modify the Statistics Returned column for Group Identity Request 0 row in Table 9-168 (D2.0 P925 L46) as shown:*

dot11Counters Group for the Interface on which the STA Statistics request was received (with the exception of those counters listed in Group Identity 1):

**9.4.2.47 FTE**

*Modify 9.4.2.47 (D2.0 P1038 L58) as shown:*

…

…

**11.3.4.2 Authentication—originating STA**

*Modify item (b) (1) in 11.3.4.2 (D2.0 P2430 L30) as shown:*

For the Open System authentication algorithm, the authentication mechanism described in 12.3.3.2 (Open System authentication).

**11.3.4.3 Authentication—destination STA**

*Modify item (a) in 11.3.4.3 (D2.0 P2430 L59) as shown:*

If Open System authentication algorithm is being used, the STA shall execute the procedure described in 12.3.3.2 (Open System authentication). These result in the generation of an MLME-AUTHENTICATE.indication primitive to inform the SME of the authentication request.

*Modify item (f) in 11.3.4.3 (D2.0 P2431 L25) as shown:*

Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is not SUCCESS, the MLME shall transmit an Authentication frame with the corresponding status code, as defined in 9.4.1.9 (Status Code field), and the state for the originating STA shall be left unchanged. The Authentication frame is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 13.5 (FT protocol), or 13.6 (FT resource request protocol).

*Modify item (g) in 11.3.4.3 (D2.0 P2431 L25) as shown:*

Upon receipt of an MLME-AUTHENTICATE.response primitive, if the ResultCode is SUCCESS, the MLME shall transmit an Authentication frame that is constructed using the appropriate procedure in 12.3.3.2 (Open System authentication), 13.5 (FT protocol) or 13.6 (FT resource request protocol), with a status code of SUCCESS, and the state for the originating STA shall be set to State 2 if it was State 1; the state shall remain unchanged if it was other than State 1.

**12.2 Framework**

**12.2.1 Classes of security algorithm**

*Modify 12.2.1 (D2.0 P2780 L28) as shown:*

This standard defines two classes of security algorithms for IEEE 802.11 networks:

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

— Pre-RSNA algorithms

NOTE—This standard does not prohibit STAs from simultaneously operating pre-RSNA and RSNA algorithms.

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

**12.2.2 Security methods**

*Modify 12.2.2 (D2.0 P2780 L37) as shown:*

Pre-RSNA security comprises the following algorithms and procedures:

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

RSNA security comprises the following algorithms and procedures:

— TKIP, described in 12.5.2 (CTR with CBC-MAC protocol (CCMP))

 NOTE—TKIP is not however considered a robust security network mechanism.

— CCMP, described in 12.5.2 (CTR with CBC-MAC protocol (CCMP))

**12.2.4 RSNA establishment**

*Modify 12.2.4 (D2.0 P2783 L47) as shown:*

**12.2.6 Requirements for the Protected Frame field**

*Modify 12.2.6 (D2.0 P2784 L62-63) as shown:*

The Protected Frame field shall be set to 1 in the following:

— Data frames that are protected using the mechanisms specified in Clause 12 (Security).

— Individually addressed protected robust Management frames.

**12.3 Non-RSNA security methods**

**12.3.1 Overview**

*Modify 12.3.1 (D2.0 P2774 L27) as shown:*

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

Open System authentication shall not be used between mesh STAs.

**12.3.2 Wired equivalent privacy (WEP)**

**12.3.2.1 WEP overview**

*Modify 12.3.2.1 (D2.0 P2787 L41-47) as shown:*

WEP is an obsolete cipher that has been removed from the standard as a standalone mechanism. The following subclauses are included for the definition of TKIP.

**12.3.3 Pre-RSNA authentication**

**12.3.3.1 Overview**

*Modify 12.3.3.1 (D2.0 P2790 L60-61) as shown:*

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. 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.

**12.3.3.3 Shared Key authentication**

*Delete 12.3.3.3 including its subclauses (D2.0 P2791 L53 – P2794 L60)*

**12.3.4.2 TKIP MPDU formats**

*Modify 12.3.4.2 (D2.0 P2797 L55) as shown:*

…

The ExtIV bit in the Key ID octet indicates the presence or absence of an extended IV. If the ExtIV bit is 0,

only the nonextended IV is transferred. If the ExtIV bit is 1, an extended IV of 4 octets follows the original IV.

For TKIP the ExtIV bit shall be set to 1, and the Extended IV field shall be supplied. The Key ID field shall be set to the key index supplied by the MLME-SETKEYS.request

primitive for the key used in cryptographic encapsulation of the frame.

**12.5.2.2 CCMP MPDU format**

*Modify 12.5.2.2 (D2.0 P2835 L52) as shown:*

…

The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP Header field extends the MPDU header by a total of 8 octets. The ExtIV subfield is always set to 1 for CCMP.

*Delete 12.6.4 (D2.0 P2867 L38-51) as shown:*

*Delete 12.6.6 (D2.0 P2869 L40-52) as shown:*

**12.7 Keys and key distribution**

**12.7.1 Key hierarchy**

**12.7.1.1 General**

*Modify 12.7.1.1 (D2.0 P2885 L19) as shown:*

…

An RSNA STA shall support at least one pairwise key for any <TA,RA> pair for use with RSNA mechanisms.

**12.7.2 EAPOL-Key frames**

*Modify item (g) in 12.7.2 (D2.0 P2903 L26) as shown:*

**RSC**. This field contains the current receive sequence counter (RSC) for the GTK being installed. It is used in message 3 of the 4-way handshake and message 1 of the group key handshake, where it is used to synchronize the IEEE 802.11 replay state. It may also be used in the Michael MIC Failure Report frame, to report the TSC field value of the frame experiencing a MIC failure. It shall contain 0 in other messages. If the RSC is less than 8 octets in length, it is stored in the first octets and the remaining octets are set to 0. The least significant octet of the RSC is in the first octet of the RSC field. The RSC for TKIP is the TKIP sequence number (TSC); for CCMP and GCMP it is the packet number (PN); see Table 12-9 (RSC field).

**12.7.4 EAPOL-Key PDU notation**

*Modify the Key Data item in EAPOL-Key() in 12.7.2 (D2.0 P2911 L24) as shown:*

GTK[N] is the GTK, with the key identifier field set to N (The key identifier specifies

which index is used for this GTK. Indexes 0 and 3 shall not be used for GTKs.)

**12.7.8 TDLS PeerKey (TPK) security protocol**

**12.7.8.1 General**

*Modify 12.7.8.1 (D2.0 P2926 L45) as shown:*

The TPK security protocol is executed between the two non-AP STAs that intend to establish an RSNA for TDLS direct link communication. If any security method (pre-RSNA or RSNA) is enabled on the connection between a STA and the AP, the STA shall require that the TPK security protocol complete successfully before using a TDLS direct link. If no security method is enabled on the connection between a STA and the AP, the STA shall not use the TPK security protocol on the TDLS direct link.

NOTE—A STA might refuse to set up a TDLS direct link when the STA link to the AP is secured with TKIP or is unsecured.

**12.7.8.2 TPK handshake**

*Modify 12.7.8.2 (D2.0 P2926 L62) as shown:*

The TPK handshake occurs as part of the TDLS direct link setup procedure. The TPKSA is the result of the successful completion of the TPK handshake protocol, which derives keys for providing confidentiality and data origin authentication.

In order to maintain TPK confidentiality, both the TDLS initiator STA and the TDLS responder STAs establish an RSNA with their common AP prior to executing the TPK handshake. To meet this criterion, a STA may refuse to initiate the TDLS direct link if:

a) The AP does not include an RSNE in its Beacon and Probe Response frames to advertise the availability of security;

b) The AP’s RSNE indicates that TKIP (00-0F-AC:2) is enabled as either pairwise or group cipher suites; or

c) The AP’s RSNE indicates that Use group cipher suite (00-0F-AC:0) is used as the pairwise cipher suite.

**12.7.8.4.2 TPK handshake message 1**

*Modify 12.7.8.4.2 (D2.0 P2929 L10) as shown:*

The pairwise cipher suite list field shall indicate the pairwise cipher suites the TDLS initiator STA is willing to use with the TPKSA. TKIP shall not be included in this list.

*Modify 12.7.8.4.2 (D2.0 P2929 L52) as shown:*

If none of the pairwise cipher suites are acceptable, or pairwise ciphers include TKIP, then the TDLS responder STA shall reject the TDLS Setup Request frame with status code STATUS\_INVALID\_PAIRWISE\_CIPHER.

**12.8 Mapping EAPOL keys to IEEE 802.11 keys**

*Modify 12.8 by removing subclauses 12.8.5 and 12.8.6 (D2.0 P2943 L47-60) as shown:*

**12.12.2 Security constraints in the 6 GHz band**

*Modify 12.12.2 (D2.0 P2963 L32) as shown:*

The following apply to a STA operating in the 6 GHz band:

— The STA shall not use the following pre-RSNA security methods:

— Open System authentication without encryption

— The STA shall not use the following cipher suite selectors:

— 00-0F-AC:0 (Use group cipher suite)

— 00-0F-AC:2 (TKIP)

**14.5.2.1 Instance Pairwise Cipher Suite selection**

*Modify 14.5.2.1 (D2.0 P3032 L41) as shown:*

Pairwise cipher suite selector TKIP shall not be used as the pairwise cipher suite when dot11MeshSecurityActivated, dot11ProtectedTXOPNegotiationActivated, or dot11ProtectedQLoadReportActivated is true.

**14.5.2.2 Group cipher suite selection**

*Modify 14.5.2.2 (D2.0 P3033 L18) as shown:*

Group cipher suite selector TKIP shall not be used as the group cipher suite when

dot11MeshSecurityActivated is true.

**B.4.4.1 MAC protocol capabilities**

*Modify B.4.4.1 by removing PICS entry PC1.3 (D2.0 P4633 L8-15) as shown:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PC1.2 | Open System authentication | 12.2.2 (Securitymethods) | PC1 AND notCFDMG:M | Yes  No  |
|  |  |  |  |  |

*Modify B.4.4.1 by removing PICS entry PC2 (D2.0 P4633 L16-28) as shown:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*Modify the References column for the B.4.4.1 item PC34.1.10 (Management frame protection) (D2.0 P4642 L17) as shown:*

9.2.4.1.10 (+HTC subfield), 9.4.1.11 (Action field), 9.4.2.24.4 (RSN capabilities), 9.6.3 (QoS Action frame details), 12.3.4.1.2 (TKIP Cryptographic encapsulation), 12.3.4.1.3 (TKIP decapsulation), 12.3.4.2 (TKIP MPDU formats), 12.5.2.3.3 (Construct AAD), 12.5.2.3.7 (CCM originator processing), 12.5.2.4.2 (CCM recipient processing), 12.5.2.4.4 (PN and replay detection), 12.6.3 (RSNA policy selection in an infrastructure BSS)

**C.3 MIB detail**

*Modify C.3 (D2.0 P4891 L6-10) as shown*

WEPKeytype ::= TEXTUAL-CONVENTION

STATUS deprecated

DESCRIPTION "Deprecated because WEP has been removed from IEEE 802.11. Represents the type of WEP key."

SYNTAX OCTET STRING (SIZE (5))

*Modify C.3 (D2.0 P4896 L23-33) as shown*

dot11PrivacyOptionImplemented OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

This is a capability variable. Its value is determined by device capabilities.

This attribute, when true, indicates that the IEEE 802.11 WEP option is implemented."

::= { dot11StationConfigEntry 7 }

*Modify DESCRIPTION of dot11AuthenticationAlgorithm in C.3 (D2.0 P4940 L44) as shown:*

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute is the authentication algorithm described by this entry in the table. The following values can be used here

Value = 1: Open system

Value = 3: Fast BSS transition (FT)

Value = 4: Simultaneous authentication of equals (SAE)

Value = 5: FILS Shared Key authentication without PFS

Value = 6: FILS Shared Key authentication with PFS

Value = 7: FILS Public Key authentication

A given value shall not be used more than once."

*Modify C.3 (D2.0 P4941 L9 – P4943 L25) as shown*

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11WEPDefaultKeys TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dot11WEPDefaultKeysTable OBJECT-TYPE

SYNTAX SEQUENCE OF Dot11WEPDefaultKeysEntry

MAX-ACCESS not-accessible

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

Conceptual table for WEP default keys. This table contains the four WEP default secret key values corresponding to the four possible Key ID values. The WEP default secret keys are logically WRITE-ONLY. Attempts to read the entries in this table return unsuccessful status and values of null or 0. The default value of each WEP default key is null."

::= { dot11smt 3 }

dot11WEPDefaultKeysEntry OBJECT-TYPE

SYNTAX Dot11WEPDefaultKeysEntry

MAX-ACCESS not-accessible

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

An Entry (conceptual row) in the WEP Default Keys Table.

ifIndex - Each IEEE 802.11 interface is represented by an ifEntry. Interface tables in this MIB module are indexed by ifIndex."

INDEX { ifIndex, dot11WEPDefaultKeyIndex }

::= { dot11WEPDefaultKeysTable 1 }

Dot11WEPDefaultKeysEntry ::=

 SEQUENCE {

dot11WEPDefaultKeyIndex Unsigned32,

dot11WEPDefaultKeyValue WEPKeytype }

dot11WEPDefaultKeyIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..4)

MAX-ACCESS not-accessible

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

The auxiliary variable used to identify instances of the columnar objects in the WEP Default Keys Table. The value of this variable is equal to the WEPDefaultKeyID + 1"

::= { dot11WEPDefaultKeysEntry 1 }

dot11WEPDefaultKeyValue OBJECT-TYPE

SYNTAX WEPKeytype

MAX-ACCESS read-write

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

This is a control variable. It is written by an external management entity. Changes take effect as soon as practical in the implementation.

A WEP default secret key value."

::= { dot11WEPDefaultKeysEntry 2 }

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* End of dot11WEPDefaultKeys TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11WEPKeyMappings TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

dot11WEPKeyMappingsTable OBJECT-TYPE

SYNTAX SEQUENCE OF Dot11WEPKeyMappingsEntry

MAX-ACCESS not-accessible

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

Conceptual table for WEP Key Mappings. The MIB supports the ability to share a separate WEP key for each RA/TA pair. The Key Mappings Table contains zero or one entries for each MAC address and contains two fields for each entry: WEPOn and the corresponding WEP key. The WEP key mappings are logically WRITE-ONLY. Attempts to read the entries in this table return unsuccessful status and values of null or 0. The default value for all WEPOn fields is false."

::= { dot11smt 4 }

dot11WEPKeyMappingsEntry OBJECT-TYPE

SYNTAX Dot11WEPKeyMappingsEntry

MAX-ACCESS not-accessible

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

An Entry (conceptual row) in the WEP Key Mappings Table.

ifIndex - Each IEEE 802.11 interface is represented by an ifEntry. Interface tables in this MIB module are indexed by ifIndex."

INDEX { ifIndex, dot11WEPKeyMappingIndex }

::= { dot11WEPKeyMappingsTable 1 }

Dot11WEPKeyMappingsEntry ::=

 SEQUENCE {

dot11WEPKeyMappingIndex Unsigned32,

dot11WEPKeyMappingAddress MacAddress,

dot11WEPKeyMappingWEPOn TruthValue,

dot11WEPKeyMappingValue WEPKeytype,

dot11WEPKeyMappingStatus RowStatus }

dot11WEPKeyMappingIndex OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS not-accessible

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

The auxiliary variable used to identify instances of the columnar objects in the WEP Key Mappings Table."

::= { dot11WEPKeyMappingsEntry 1 }

dot11WEPKeyMappingAddress OBJECT-TYPE

SYNTAX MacAddress

MAX-ACCESS read-create

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

The MAC address of the STA for which the values from this key mapping entry are to be used."

::= { dot11WEPKeyMappingsEntry 2 }

dot11WEPKeyMappingWEPOn OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

Boolean as to whether WEP is to be used when communicating with the dot11WEPKeyMappingAddress STA."

::= { dot11WEPKeyMappingsEntry 3 }

dot11WEPKeyMappingValue OBJECT-TYPE

SYNTAX WEPKeytype

MAX-ACCESS read-create

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

A WEP secret key value."

::= { dot11WEPKeyMappingsEntry 4 }

dot11WEPKeyMappingStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

The status column used for creating, modifying, and deleting instances of the columnar objects in the WEP key mapping Table."

DEFVAL { active }

::= { dot11WEPKeyMappingsEntry 5 }

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* End of dot11WEPKeyMappings TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

*Modify C.3 (D2.0 P4944 L9) as shown:*

dot11PrivacyInvoked OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

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

invoked for transmitting Data frames.

For RSNA non-AP STAs, an additional variable dot11RSNAActivated indicates

whether RSNA is enabled. If

dot11RSNAActivated is true, RSNA security mechanisms invoked are

configured in the dot11RSNAConfigTable."

DEFVAL { false }

::= { dot11PrivacyEntry 1 }

dot11WEPDefaultKeyID OBJECT-TYPE

SYNTAX Unsigned32 (0..3)

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This attribute indicates the use of the first, second, third, or fourth

element of the WEPDefaultKeys array when equal to values of zero, one,

two, or three."

DEFVAL { 0 }

::= { dot11PrivacyEntry 2 }

dot11WEPKeyMappingLengthImplemented OBJECT-TYPE

SYNTAX Unsigned32 (10..4294967295)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a capability variable.

Its value is determined by device capabilities.

The maximum number of tuples that dot11WEPKeyMappings can hold."

::= { dot11PrivacyEntry 3 }

dot11ExcludeUnencrypted OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

When this attribute is true, the STA does not indicate at the MAC service

interface received MSDUs that have the Protected Frame subfield of the

Frame Control field equal to 0. When this attribute is false, the STA may

accept MSDUs that have the Protected Frame subfield of the Frame Control

field equal to 0."

DEFVAL { false }

::= { dot11PrivacyEntry 4 }

dot11WEPICVErrorCount OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the MAC when an ICV error is detected.

This counter increments when a frame is received with the Protected Frame

subfield of the Frame Control field equal to 1 and the value of the ICV as

received in the frame does not match the ICV value that is calculated for

the contents of the received frame. ICV errors for TKIP are not counted in

this variable but in dot11RSNAStatsTKIPICVErrors."

::= { dot11PrivacyEntry 5 }

dot11WEPExcludedCount OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"Deprecated because WEP has been removed from IEEE 802.11.

This is a status variable.

It is written by the MAC when a bad frame is received.

This counter increments when a frame is received with the Protected Frame

subfield of the Frame Control field equal to 0 and the value of

dot11ExcludeUnencrypted causes that frame to be discarded."

::= { dot11PrivacyEntry 6 }

dot11RSNAActivated OBJECT-TYPE

…

*Modify C.3 (D2.0 P4950 L14) as shown:*

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11RSNAConfig TABLE (RSNA)

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**J.6 Additional test vectors**

*Modify J.6 by removing subclause J.6.2 (D2.0 P5644 L38 – P5645 L37) as shown:*

|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

**K.2 Recommendation for implementation of contention based admission control**

**K.2.2 Deriving medium time**

*Modify K.2.2 (D2.0 P5679 L1) as shown:*

…

and where

Sizes are in octets; Rates are in b/s; durations and Times are in μs; Surplus Bandwidth Allowance is the

unsigned integer value passed

MAC Header Size = 26

MPDU Delimiter Size = 4

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

Ack Size = 14

BlockAck Size = 32

FCS Size = 4

…