IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA2 Security comment resolutions | | | | |
| Date: 2024-04-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |

Background

This contribution proposes comment resolutions to selected REVme SEC adhoc comments from the SA Ballot recirculation on D5.0.

R0 – Initial version.

R1 –

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 7231 | 3029.00 | 12.5.2.4.4 |  |  | "The number indicated by the TDLS responder STA (if a TDLS Discovery Response frame is sent) is ignored, as is the GTKSA Replay Counter field in the TDLS Setup Request frame and any TDLS Discovery Response frame." -- also potentially other fields, e.g. Joint Multi-Band RSNA (note 12.6.20.4 Multi-band RSNA with TDLS in a non-DMG BSS), EKIDIAF, OCVC. But maybe only EKIDIAF is relevant to TDLS | Change to "… as are the GTKSA Replay Counter and Extended Key ID For Individually Addressed Frames fields …". Ditto at 3043.21 |

### Discussion:

* The cited text in context is as follows:

A close-up of a document

Description automatically generated

* The proposed change is

Change

“NOTE 1—The number indicated by the TDLS responder STA (if a TDLS Discovery Response frame is sent) is ignored, as is the GTKSA Replay Counter field in the TDLS Setup Request frame and any TDLS Discovery Response frame.”

to

“NOTE 1—The number indicated by the TDLS responder STA (if a TDLS Discovery Response frame is sent) is ignored, as are the GTKSA Replay Counter and Extended Key ID For Individually Addressed Frames fields in the TDLS Setup Request frame and any TDLS Discovery Response frame.”

* The proposed change is adding additional fields to the note. However, the proposed change references a field that has nothing to do with replay counters. It would be better to change the cited text to:

“NOTE 1—The number of replay counters indicated by the TDLS responder STA (if a TDLS Discovery Response frame is sent) is ignored, …”

* The text in the note could be structured better

### Proposed Resolution: (7231)

REVISED. Modified the note at 3029.40 and 3043.21, changing:

“NOTE 1—The number indicated by the TDLS responder STA (if a TDLS Discovery Response frame is sent) is ignored, as is the GTKSA Replay Counter field in the TDLS Setup Request frame and any TDLS Discovery Response frame.”

to

“NOTE 1— The number of replay counters, the GTKSA Replay Counter, and Extended Key ID For Individually Addressed Frames fields indicated by the TDLS responder STA are ignored in the TDLS Setup Request frame and any TDLS Discovery Response frame.”

Note To Editor: Number the notes appropriately at the cited locations.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 7191 | 3107.00 | 12.7.6.4 |  |  | "the Supplicant verifies that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and verifies that" should be "the Supplicant shall verifiy that the PMKR1Name in the PMKID List field of the RSNE is identical to the value it sent in message 2 and shall verify that" (maybe other bullets) | As it says in the comment |

### Discussion:

* The cited text is shown as follows:A close-up of a computer screen

  Description automatically generated
* After looking at the text in context, the shall on line 26 applies to the enumerated list. There are other “shall” requirements in the list, but they apply to exceptions for example “if any of these verification steps indicate a mismatch, the STA shall disassociate…”

### Proposed Resolution: (7191)

REJECTED. The “shall” (3107.26) at the beginning of the list applies to all steps indicated in the list.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 7232 | 3119.00 | 12.7.8.4.2 |  |  | "If security is not required on the TDLS direct link (see 12.7.8.1 (General)) (#6149)and the request includes an RSNE" -- or FTE or TIE | Change to "… an RSNE, FTE or TIE" |
| 7233 | 3119.00 | 12.7.8.4.2 |  |  | "If security is required on the TDLS direct link (see 12.7.8.1 (General)) (#6149)and the request does not include both an RSNE and an FTE" -- and TIE | Change to "… include an RSNE, an FTE and a TIE" |
| 7234 | 3119.00 | 12.7.8.4.2 |  |  | "If the version field of the RSNE is 0, (#6149)the TDLS responder STA shall reject the request with status code UNSUPPORTED\_RSNE\_VERSION." -- also if >1 | Change to "… is not 1, …" |
| 7235 | 3119.00 | 12.7.8.4.2 |  |  | "If none of the pairwise cipher suites are acceptable, or pairwise ciphers include (#3056)TKIP" -- only one suite is (now) allowed | Change to "If the pairwise cipher suite is not acceptable (including if it is TKIP)" |
| 7236 | 3119.00 | 12.7.8.4.2 |  |  | "If the RSN Capabilities field has not been set the subfields according to the described rules for this message" is both grammatically broken and semantically opaque | Change to "If the PeerKey Enabled subfield is not set to 1 in the RSN Capabilities field" |
| 7237 | 3120.00 | 12.7.8.4.2 |  |  | "If the contents of the FTE are not as per specified for this message" not clear | Change to "If the FTE is not set as described above" |

### Discussion:

* The cited text for the comments in context is:

A screenshot of a computer

Description automatically generatedA close up of text

Description automatically generated

### Proposed Resolution: (7232, 7233, 7234, 7235, 7236, 7237)

REVISED. Make the changes proposed by the commenter as shown in <this> document under “Proposed Resolution: (7232, 7233, 7234, 7235, 7236, 7237)”

On reception of message 1, the TDLS responder STA (#6149)proceeds as follows:

If security is not required on the TDLS direct link (see 12.7.8.1 (General)) (#6149)and the request includes an RSNE, FTE, or TIE, the TDLS response STA shall reject the request with status code SECURITY\_DISABLED.

If security is required on the TDLS direct link (see 12.7.8.1 (General)) (#6149)and the request does not include an RSNE, an FTE and TIE, the TDLS responder STA shall reject the request with status code INVALID\_PARAMETERS.

If the version field of the RSNE is not 1, (#6149)the TDLS responder STA shall reject the request with status code UNSUPPORTED\_RSNE\_VERSION.

(#6149)If (#3488)the RSNE does not indicate (#4225)the single (#3266)AKM 00-0F-AC:7(TPK handshake), the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_AKMP.

(#6149)If the pairwise cipher suite is not acceptable (include if it is (#3056)TKIP), then the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_PAIRWISE\_CIPHER.

(#6149) If the PeerKey Enabled subfield is not set to 1 in the RSN Capabilities field, the TDLS responder STA shall reject the request with status code INVALID\_RSNE\_CAPABILITIES.

(#6149)If the number of replay counters indicated by the TDLS initiator STA is not acceptable to the TDLS responder STA at both the TDLS initiator STA and the TDLS responder STA (see 12.5.2.4.4 (PN and replay detection) and 12.5.4.4.4 (PN and replay detection)), the TDLS responder STA shall reject the request with status code INVALID\_RSNE\_CAPABILITIES.

(#6149)If the suggested lifetime is unacceptable or below the default value, the TDLS responder STA shall reject the request with status code UNACCEPTABLE\_LIFETIME.

shall reject the request with status code STATUS\_INVALID\_FTE.

(#6149) If the FTE is not set as described above", the TDLS responder STA shall reject the request with status code STATUS\_INVALID\_FTE.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 7152 | 3154.00 | 12.12.2 |  |  | "The STA shall use management frame protection (MFPR=1) when using RSN." -- there is no need for a non-AP STA to set MFPR, only MFPC | Change the cited text to "A STA shall support management frame protection (MFPC=1) when using RSN. An AP shall require management frame protection (MFPR=1) when using RSN." |

### Discussion:

* The cited text in context (see last sentence)

A screenshot of a computer

Description automatically generated

* If a STA sets MFPR=1 it must be MFP capable so MFPC is set to 1. It’s also true in an infrastructure network that an AP is required to set MFPR =1 in the 6 GHz band. The commenter is adding the explicit requirement for an AP to set MFPR=1 for an infrastructure network.

### Proposed Resolution: (7152)

ACCEPTED

### Comment:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 7163 |  | 12.7.8.2 |  |  | "TPK" here is sometimes used not to mean "TDLS PeerKey" but to refer to some kind of key: "A TPK is a transient key". Also in 12.6.20.4 "the TPK-TK of the TPK" and "the TPK creation method". Also 12.7.8.3 "to derive the TPK" and 12.7.8.4 "to generate the TPK" and "compute the TPK" | Replace with "TPK transient key" |

### Discussion:

* The cited text in the comment is:

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

* Note on line 21, “The TPK transient key (TPK-TK) shall be computed”. The TPK-TK is the “TPK transient key”.
* Note that the PTK is defined (see 3078.17) to have the components PTK-KCK, PTK-KEK, and TK, where the TK is the temporal key.
* The TPK-TK should really be the TPK temporal key.
* The cited text in 12.6.20.4:

A close-up of a text

Description automatically generated

* The first paragraph should be:

“When two multi-band capable devices operate in a non-DMG BSS and set up a TDLS direct link in the BSS, the TPK handshake protocol can be used to create a TPK temporal key for use in another supported band/channel that is supported by both STAs and that was indicated in the Multi-band element in each of the STAs. The temporal key used in supported band/channel shall be set to the TPK-TK of the TPK transient key.”

* In the second paragraph the “TPK creation method” appears to refer to TPK transient key derivation, so

“In this case, the TPK creation method shall be used to calculate a different PTKSA in

the supported band/channel:”

should be changed to

“In this case, the TPK transient key derivation shall be used to calculate a different TPKSA in the supported band/channel:”

A screenshot of a computer

Description automatically generated

* For 12.7.8.3, “derive the TPK and attack …” should be “derive the TPK transient key and attack …”
* For 12.7.8.4.1, “generate the TPK” should be “generate the TPK transient key”
* The remainder of 12.7.8.4 has no additional issues with the use of TPK.

### Proposed Resolution: (7163)

REVISED. The TPK transient key is composed of the TPK-KCK and the TPK-TK, where the TPK-TK is the TPK temporal key. This is consistent terminology with the PTK.

At 3118.21, change

“The TPK transient key (TPK-TK) shall be computed”

to

“The TPK temporal key (TPK-TK) shall be computed”

At 3073.32, change

“When two multi-band capable devices operate in a non-DMG BSS and set up a TDLS direct link in the BSS, the TPK handshake protocol can be used to create a PTKSA for use in another supported band/channel that is supported by both STAs and that was indicated in the Multi-band element in each of the STAs. Only TK in PTKSA is required for the supported band/channel and it shall be equal to the TPK-TK of the TPK.”

to

“When two multi-band capable devices operate in a non-DMG BSS and set up a TDLS direct link in the BSS, the TPK handshake protocol can be used to create a TPK temporal key for use in another supported band/channel that is supported by both STAs and that was indicated in the Multi-band element in each of the STAs. The temporal key used in supported band/channel shall be set to the TPK-TK of the TPK transient key.”

At 3073.34, change

“In this case, the TPK creation method shall be used to calculate a different PTKSA in

the supported band/channel:”

to

“In this case, the TPK transient key derivation shall be used to calculate a different TPKSA in the supported band/channel:”

At 3118.43, change

“derive the TPK and attack …”

to

“derive the TPK transient key and attack …”

At 3118.63, change

“… generate the TPK.”

to

“… generate the TPK transient key”