IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed resolutions to some LB270 comments | | | | |
| Date: 2022-11-18 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses and proposes resolutions to the following LB270 (REVme/D2.0) comments: 3135, 3255, 3422, 3489, 3635

r1: CID 3135 updates based on 2022-11-14 PM2 discussion

r2: CID 3135 update in Clause 13 language to set the new MIC Length subfield as appropriate

r3: added CID 3255, 3422, 3489, 3635

**CID 3135**

P2910 L24 12.7.3

Comment:

The recently added AKM 00-0F-AC:25 (FT/SAE with variable key length) made parsing of the first Authentication frame in the FT protocol case inconvenient since the AP receiving this frame may not have been part of the SAE authentication exchange with the non-AP STA and as such, it does not yet know which finite cyclic group was used with SAE and as such, does not know the length of the MIC field. However, this AP needs to be able to parse the FTE in this frame and, in particular, find the subelements from the FTE after the variable length MIC field. This cannot be done robustly without knowing the length of the MIC field (and the 8 octet length of the likely first subelement makes this even more inconvenient since that happens to be the difference between possible MIC field lengths).

Proposed Change:

Specify the length of the MIC field in the FTE for the new AKM:  
- at P1037 L8 (Figure 9-418), add a new subfield "MIC Length" for B1..B3 (3 bits), leaving B4..B7 (4 bits) as the new size for Reserved  
- at P1037 (was 1036) L18 add a new paragraph:  
 "The MIC Length subfield defines the length of the MIC field when using AKM 00-0F-AC:25. The value of this subfield is not applicable for other AKMs. Table 9-<new> defines the available values for this."  
- at P1037 (was 1036) L18 add a new table "Table 9-<new>--MIC length" with columns "Value" and "MIC field length in octets" and values "0 = 16 or not applicable", "1 = 24", "2 = 32", "3-7 = Reserved".

Discussion:

The comment is on the last row of this table:



The identified issue has been identified in an early implementation of the new AKM and the proposed change addresses the identified parsing issue, but has couple of editorial issues that are addressed in the following redline version.

Proposed Resolution:

REVISED. Add the proposed subfield with some editorial cleanup by incorporating changes under the “Changes for CID 3135” header in document <this document>.

**Changes for CID 3135**

*Modify 9.4.2.47 (D2.0 P1037 L8-18) as shown:*

**9.4.2.47 FTE**

The fast BSS transition element (FTE) includes information needed to perform the FT authentication

sequence or FILS authentication during a fast BSS transition in an RSN. This element is shown in Figure 9-

417 (FTE format).



The Element ID and Length fields are defined in 9.4.2.1 (General).

The MIC Control field is 2 octets and is defined in Figure 9-418 (MIC Control field format).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0 | B1 B3 | B4 B7 | B8 B15 |
|  | RSNXE Used | MIC Length | Reserved | Element Count |
| Bits: | 1 | 3 | 4 | 8 |

**Figure 9-418—MIC Control field format**

The RSNXE Used subfield of the MIC Control field is used in the third and fourth messages of the FT

authentication sequence to indicate whether the STA transmitting the frame containing the FTE includes an

RSNXE in other frames. This subfield is set to 0 in other frames.

When using AKM 00-0F-AC:25, the MIC Length subfield defines the length of the MIC field, as defined in Table 9-<new>. This subfield is reserved for other AKMs.

**Table 9-<new>—MIC Length subfield values**

|  |  |
| --- | --- |
| **Value** | **MIC field length in octets** |
| 0 | 16 |
| 1 | 24 |
| 2 | 32 |
| 3-7 | Reserved |

The Element Count subfield of the MIC Control field contains the number of elements that are included in

the message integrity code (MIC) calculation.

When the Element Count subfield has a value greater than 0, the MIC field contains a MIC. Otherwise, the

MIC field is set to 0.

The length of the MIC field depends on the negotiated AKM selector and the value of the MIC Length subfield, when not reserved, and is specified in Table 12-11 (Integrity and key wrap algorithms) and Table 9-<new>.

The ANonce field contains a value chosen by the R1KH.

The SNonce field contains a value chosen by the S1KH.

**13.4.2 FT initial mobility domain association in an RSN**

*Modify 13.4.2 (D2.0 P2969 L11) as shown:*

…

The (Re)Association Response frame from the AP shall contain an MDE, with contents as presented in Beacon and Probe Response frames. The FTE shall include the key holder identities of the AP, the R0KH-ID and R1KH-ID, set to the values of dot11FTR0KeyHolderID and dot11FTR1KeyHolderID, respectively. The FTE shall have a MIC element count of zero (i.e., no MIC present) and have ANonce, SNonce, and MIC fields set to 0. The RSNXE Used subfield of the MIC Control field shall be set to 0. When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.

**13.8.2 FT authentication sequence: contents of first message**

*Modify 13.8.2 (D2.0 P2990 L32) as shown:*

…

If present, the FTE shall be set as follows:

* R0KH-ID shall be the value of R0KH-ID obtained by the FTO during its FT initial mobility domain association exchange.
* SNonce shall be set to a value chosen randomly by the FTO, see 12.7.5 (Nonce generation) for a recommended procedure.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* All other fields shall be set to 0.

**13.8.3 FT authentication sequence: contents of second message**

*Modify 13.8.3 (D2.0 P2990 L61) as shown:*

…

If present, the FTE shall be set as follows:

* R0KH-ID shall be identical to the R0KH-ID provided by the FTO in the first message.
* R1KH-ID shall be set to the R1KH-ID of the target AP, from dot11FTR1KeyHolderID.
* ANonce shall be set to a value chosen randomly by the target AP, see 12.7.5 (Nonce generation) for a recommended procedure.
* SNonce shall be set to the value contained in the first message of this sequence.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* All other fields shall be set to 0.

**13.8.4 FT authentication sequence: contents of third message**

*Modify 13.8.4 (D2.0 P2991 L27) as shown:*

…

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
* The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).
* The RSNXE Used subfield of the MIC Control field shall be set to 1 if the FTO set to 1 any subfield, except the Field Length subfield, of the Extended RSN Capabilities field in the RSNXE; otherwise this subfield shall be set to 0.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* When the negotiated AKM is 00-0F-AC:3, 00-0F-AC:4, or 00-0F-AC:9, the MIC shall be calculated using the KCK and the AES-128-CMAC algorithm. The output of the AES-128-CMAC shall be 128 bits.

…

* All other fields shall be set to 0.

**13.8.5 FT authentication sequence: contents of fourth message**

*Modify 13.8.5 (D2.0 P2992 L36) as shown:*

…

If present, the FTE shall be set as follows:

* ANonce, SNonce, R0KH-ID, and R1KH-ID shall be set to the values contained in the second message of this sequence.
* The Element Count subfield of the MIC Control field shall be set to the number of elements protected in this frame (variable).
* The RSNXE Used subfield of the MIC Control field shall be set to 1 if the target AP includes an RSNXE in its Beacon and Probe Response frames; otherwise this subfield shall be set to 0.
* When the negotiated AKM is 00-0F-AC:25, the MIC Length subfield of the MIC Control field shall be set to indicate the length of the MIC field.
* If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC capability, the Authenticator shall include FT OCI subelement in FTE.

…

* All other fields shall be set to 0.

**CID 3255**

P234 L1 3.2 (note comment identified incorrect Clause 23 without specifying page/line)

Comment:

Jouni: "temporal encryption key" feels inconvenient at best nowadays and it does not seem ideal even in the context of 802.11i-2004. IGTK and BIGTK are temporal keys, but they do not encrypt frames and as such, are not temporal encryption keys. Since "temporal key" refers "temporal encryption key" as the definition, that should really work for IGTK and BIGTK as well, but it doesn't.. I think I'd prefer to get rid of that "temporal encryption key" terms completely and just call all keys that are used directly with any of the defined ciphers suites as "temporal keys". This would then include TK (from PTK), GTK, IGTK, BIGTK, and I guess even WIGTK nowadays. This would get rid of the need for the TKIP exception, too, since TK for TKIP would not need to be "split" into encryption and non-encryption parts in the definition section.  
  
Figure 12-31 is only an informative example, so I would not consider it to normatively define GTK or how it is derived. In 802.11i-2004, this was described with "The GTK is partitioned into temporal keys" (of which only one is defined), but it looks like we've dropped that language at some point. I guess one could claim that that empty box depicts the "portion of GTK" that is not a temporal key.. ;-) One could even define group transient key as the container for a group temporal key in the model of PTK/TK, but I don't recall whether that was ever the point during P802.11i work. And if it was, 802.11w did not follow that concept by extending group transient key to contain group temporal key and integrity group temporal key.

Proposed Change:

As it says in the comment

Discussion:

The comment is not exactly clear on the location and changes that would satisfy it. However, since the “temporal encryption key” language exists only in two definitions in 3.2, the intent of the comment seems clear. There is no need to define a separate term just to be able to use it in the definition of “temporal key”, so the best approach here seems to be to reword the definition of “temporal key” in a manner that is independent of whether the cipher suite uses encryption.

Proposed Resolution:

REVISED. Incorporate changes under the “Changes for CID 3255” header in document <this document>. This modifies the definitions along the direction proposed in the comment.

**Changes for CID 3255**

**3.2 Definitions specific to IEEE Std 802.11**

*Modify 3.2 (D2.0 P234 L1-17) as shown:*

temporal key (TK): A key that is used to protect data in medium access control (MAC) protocol data units (MPDUs) using a cipher. When abbreviated this is, unless explicitly shown otherwise, specifically the key used to protect individually addressed frames, as distinct from e.g., the TK that is the group temporal key (GTK).

NOTE—A temporal key is a session key.

**CID 3442**

P313 L26 4.5.4.4

Comment:

"IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including TKIP,  
CCMP, and GCMP." -- what about BIP/GMAC/CMAC?

Proposed Change:

After the cited text add "IEEE Std 802.11 provides several cryptographic algorithms to protect management traffic, including BIP-CMAC and BIP-GMAC."

Discussion:

It seems reasonable to add the proposed text, but it should be added a bit later in the subclause to keep the sentence talking about TKIP/CCMP/GCMP together and to avoid claiming that the group management cipher suite would be “selected” (which might be interpreted as a reference to pairwise cipher negotiation). Furthermore, this could be more specific on the BIP examples applying only to group addressed management traffic.

Proposed Resolution:

REVISED. Incorporate changes under the “Changes for CID 3442” header in document <this document>. This adds a slightly modified text to a different location within the cited subclause.

**Changes for CID 3442**

**4.5.4.4 Data confidentiality**

*Modify 4.5.4.4 (D2.0 P313 L26) as shown:*

IEEE Std 802.11 provides several cryptographic algorithms to protect data traffic, including TKIP, CCMP, and GCMP. TKIP is based on the ARC420 algorithm, and 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.

IEEE Std 802.11 provides the following security protocols for protection of individually addressed robust Management frames: CCMP and GCMP. This standard provides data confidentiality for certain Action frames as indicated in Table 9-79 (Category values).

IEEE Std 802.11 provides several cryptographic algorithms to protect group addressed management traffic, including BIP-CMAC and BIP-GMAC."

IEEE Std 802.11 provides one security protocol, CCMP, for protection of individually addressed and group addressed Data frames between mesh STAs.

**CID 3489**

P2915 L9 12.7.6.3

Comment:

"OCI FTE subelement" -- what's that?

Proposed Change:

At 2915.9, 2917.34 change to "OCI KDE or FTE OCI subelement is missing in the message" to "OCI KDE or OCI subelement is missing in the message or FTE respectively". At 4648.49 change "OCI FTE subelement" to "OCI subelement"

Discussion:

The “OCI FTE subelement” variant is in PICS (P4648 L50) while other locations use “FTE OCI subelement” or “FT OCI subelement”. The comment did not propose those “FT OCI subelement” cases to be modified, but it would seem reasonable to address them as well. As far as the “OCI KDE or FTE OCI subelement” cases are concerned, they are for EAPOL-Key messages 2 and 3 which do not include FTE. As such, the proposed change is not the correct fix.

Proposed Resolution:

REVISED. Incorporate changes under the “Changes for CID 3489” header in document <this document>. This addresses the identified issue, including a couple of additional instances, with somewhat different changes.

**Changes for CID 3489**

**12.7.6.3 4-way handshake message 2**

*Modify 12.7.6.3 (D2.0 P2915 L10) as shown:*

If dot11RSNAOperatingChannelValidationActivated is true and the Supplicant RSNE indicates

OCVC capability, the Authenticator shall silently discard message 2 if any of the following are true:

— OCI KDE is missing in the message

— Channel information in the OCI does not match current operating channel parameters (see 12.2.9 (Requirements for Operating Channel Validation))

**12.7.6.4 4-way handshake message 3**

*Modify 12.7.6.4 (D2.0 P2917 L35) as shown:*

If dot11RSNAOperatingChannelValidationActivated is true and Authenticator RSNE indicates OCVC

capability, the Supplicant shall silently discard message 3 if any of the following are true:

— OCI KDE is missing in the message

— Channel information in the OCI does not match current operating channel parameters (see 12.2.9

(Requirements for Operating Channel Validation))

**13.8.4 FT authentication sequence: contents of third message**

*Modify 13.8.4 (D2.0 P2991 L46) as shown:*

If dot11RSNAOperatingChannelValidationActivated is true and Authenticator indicates OCVC

capability, the Supplicant shall include OCI subelement in FTE.

**13.8.5 FT authentication sequence: contents of fourth message**

*Modify 13.8.5 (D2.0 P2992 L38) as shown:*

If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC

capability, the Authenticator shall include OCI subelement in FTE.

**Annex B**

*Modify PICS (D2.0 P4648 L50) as shown:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PC45.2 | OCI KDE | 12.7.2 (EAPOL-Key frames) | PC45:M | Yes  No  N/A  |
| PC45.3 | OCI subelement | 9.4.2.47 (FTE) | PC45:M | Yes  No  N/A  |

**CID 3635**

Comment:

It is not clear whether EAPOL-Key request frames can be sent before the completion of the initial 4WH (e.g. because the Supplicant perceives that the Authenticator has abandoned the initial 4WH)

Proposed Change:

Specify that EAPOL-Key request frames may be sent at any point, but that the Secure bit is always 1

Discussion:

EAPOL-Key request frames are explicitly specified to require Secure=1 to indicate that a shared PTKSA has to exists to be able to protect them. The proposed change would open a security vulnerability since an attacker could inject EAPOL-Key request frames without protection between the association and completion of the initial 4-way handshake.

Proposed Resolution:

REJECTED. EAPOL-Key request frames need to be protected to prevent their misuse. That is why they are required to use Secure=1 and MIC=1 (with the AEAD exception). It would not be appropriate to send these frames “at any point” and the requirement of Secure=1 indicates that.