IEEE P802.11
Wireless LANs

|  |
| --- |
| Security comments assigned to me |
| Date: 2016-05-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes resolutions to the remaining comments assigned to me from the recirc SB on P802.11-REVmc/D5.0: CID 7061, CID 7420, CID 7421, CID 7462, CID 7727, CID 7783.

# CID 7061

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Clause Number | Page | Line | Comment | Proposed Change | Proposed Resolution |
| 9.4.2.25.2 | 831 | 53 | "An AP may specify the selector 00-0F-AC:0 (Use group cipher suite) for a pairwise cipher suite if it does not support any pairwise cipher suites." - normative verb in clause 9 | Either change to "can specify" or "specifies" depending on whether this is truly optional behaviour and cite clause 10/11/12 location that defined this behaviour; or move this to clause 10/11/12. | REVISED. Apply changes proposed for CID 7061 in <this document>. |

**Discussion**

EDITOR: 2016-02-04 11:55:24Z - I reviewed uses of this selector, and didn’t find any that were obviously normative descriptions of when it can be used.

It looks like: “An AP may specify the selector 00-0F-AC:0 (Use group cipher suite) for a pairwise cipher suite if it does not support any pairwise cipher suites.”

could be moved into Clause 12, but didn’t find an obvious home. Transferring to GEN/Security.

Jouni: There is already a comment related to this with normative language for the non-AP STA in 12.6.3. That paragraph can have the “AP may” language in it while 9.4.2.25.2 should specify what the AP does in case it does not support any pairwise cipher suites using “AP specifies” language. Since there is not really any more detail in 12.6.3, I’m not sure there would be value in referencing that clause from 9.4.2.25.2.

## Proposed changes to address CID 7061

**9.4.2.25.2 Cipher suites**

*Change the following paragraphs in D5.4 page 846 lines 5-12 as shown:*

The cipher suite selector 00-0F-AC:0 (Use group cipher suite) is valid only as the pairwise cipher suite. An AP specifies the selector 00-0F-AC:0 (Use group cipher suite) for a pairwise cipher suite if it does not support any pairwise cipher suites. If an AP specifies 00-0F-AC:0 (Use group cipher suite) as the pairwise cipher selection, this is the only pairwise cipher selection the AP advertises.

If any cipher suite other than TKIP, WEP-104, or WEP-40 is enabled, then the AP supports pairwise keys, and thus the suite selector 00-0F-AC:0 (Use group cipher suite) is not a valid option.

**12.6.3 RSNA policy selection in an infrastructure BSS**

*Change the following paragraphs in D5.4 page 2011 lines 24-27 as shown:*

In order to accommodate local security policy, a STA may choose not to associate with an AP that does not support any pairwise cipher suites. An AP may indicate that it does not support any pairwise keys by advertising 00-0F-AC:0 (Use group cipher suite) as the pairwise cipher suite selector.

# CID 7420

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Clause Number | Page | Line | Comment | Proposed Change | Proposed Resolution |
| 12.5.3.3.6 | 1949 | 37 | It says "A CCMP protected individually addressed robust Management frame shall be protected with the TK." -- what about other CCMP-protected frames? Note for the recipient this is clearer: "A CCMP protected individually addressed robust Management frame shall use the same TK as a Data frame." | Change to "A CCMP protected frame shall be protected with the appropriate TK, where a CCMP protected individually addressed robust Management frame shall use the same TK as a Data frame." | REVISED. Apply changes proposed for CID 7420 in <this document>. |

**Discussion**

The comment seems to identify a missing detail since the pre-802.11w text did not describe any specific TK for Data frames and the matching TK between Data frames and individually addressed robust Management frames is also missing here on the originator side. The proposed change from the commenter looks fine and it would also look fine to simply accept the comment. The comment spreadsheet seemed to imply that a submission could be needed for CID 7420 or CID 7421, so here is that submission with a slightly different text, but I wouldn’t object to a simple “Accept” as the resolution either.

Note: CID 7421 below is identical comment for GCMP. These two comments should be addressed consistently.

## Proposed changes to address CID 7420

**12.5.3.3.6 CCM originator processing**

*Change the following paragraphs in D5.4 page 1990 line 63 as shown:*

A CCMP protected frame shall be protected with the appropriate TK. A CCMP protected individually addressed robust Management frame shall be protected using the same TK as a Data frame.

# CID 7421

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Clause Number | Page | Line | Comment | Proposed Change | Proposed Resolution |
| 12.5.5.3.6 | 1957 | 62 | It says "A GCMP protected individually addressed robust Management frame shall be protected with the TK." -- what about other GCMP-protected frames? Note for the recipient this is clearer: "A GCMP protected individually addressed robust Management frame shall use the same TK as a Data frame." | Change to "A GCMP protected frame shall be protected with the appropriate TK, where a GCMP protected individually addressed robust Management frame shall use the same TK as a Data frame." | REVISED. Apply changes proposed for CID 7421 in <this document>. |

**Discussion**

Note: The comment points to incorrect page/line (the matching CCMP text). The table above shows the fixed location that this comments talks about (GCMP).

The comment seems to identify a missing detail since the pre-802.11w text did not describe any specific TK for Data frames and the matching TK between Data frames and individually addressed robust Management frames is also missing here on the originator side. The proposed change from the commenter looks fine and it would also look fine to simply accept the comment. The comment spreadsheet seemed to imply that a submission could be needed for CID 7420 or CID 7421, so here is that submission with a slightly different text, but I wouldn’t object to a simple “Accept” as the resolution either.

## Proposed changes to address CID 7421

**12.5.5.3.6 GCM originator processing**

*Change the following paragraph in D5.4 page 1998 line 24 as shown:*

A GCMP protected frame shall be protected with the appropriate TK. A GCMP protected individually addressed robust Management frame shall be protected using the same TK as a Data frame.

# CID 7462

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Clause Number | Page | Line | Comment | Proposed Change | Proposed Resolution |
| 12.6.1.3.2 | 1967 | 23 | ", or if the PMK in the cached PMKSA is no longer valid," -- how can this be determined? How is this even possible -- doesn't invalidation of a PMK also invalidate the whole PMKSA? | Delete the cited text. Also at 1975.45 | REVISED. Apply changes proposed for CID 7462 in <this document>. |

**Discussion**

The comment is correct in the expected a PMKSA cache invalidating a PMKSA entry when the associated PMK is “invalidated” which, in practice, mean when its lifetime expires. 12.6.1.1.2 (PMKSA) describes this constraint on caching: “PMKSAs are cached for up to their lifetimes.” That said, there does not seem to be a clear shall statement mandating STA (or Supplicant/Authenticator) to remove a PMKSA cache entry whose lifetime (which is identical to the lifetime of the PMK) expires.

## Proposed changes to address CID 7462

**12.6.1.3.2 Security association in an ESS**

*Change the following list item in D5.4 page 2008 lines 42-55 as shown:*

A STA (AP) can cache PMKSAs for APs (STAs) in the ESS to which it has previously performed a full IEEE Std 802.1X authentication or SAE authentication. If a STA wishes to roam to an AP for which it has cached one or more PMKSAs, it can include one or more PMKIDs in the RSNE of its (Re)Association Request frame. An AP that has retained the PMK for one or more of the PMKIDs can proceed with the 4-way handshake. The AP shall include the PMKID of the selected PMKSA in message 1 of the 4-way handshake. If none of the PMKIDs of the cached PMKSAs matches any of the supplied PMKIDs, or if the AKM of the cached PMKSA differs from that offered in the (Re)Association Request, then the Authenticator, in the case of Open System authentication, shall perform another IEEE Std 802.1X authentication and, in the case of SAE authentication, shall transmit a Deauthentication frame to the STA. Similarly, if the STA fails to send a PMKID, the STA and AP need to perform a full IEEE Std 802.1X authentication.

**12.6.10.3 Cached PMKSAs and RSNA key management**

*Change D5.4 page 2017 lines 20-52 as shown:*

In a non-FT environment, a STA might cache PMKSAs it establishes as a result of previous authentication. The PMKSA cannot be changed while cached. The PMKSA in the PMKSA is used with the 4-way handshake to establish fresh PTKs.

If a STA in an infrastructure BSS has determined it has a valid PMKSA with an AP to which it is about to (re)associate, it performs Open System authentication to the AP, and then it includes the PMKID for the PMKSA in the RSNE in the (Re)Association Request. When the PMKSA was not created using pre-authentication, the AKM indicated in the RSNE by the STA in the (Re)Association Request shall be identical to the AKM used to establish the cached PMKSA in the first place.

Upon receipt of a (Re)Association Request frame with one or more PMKIDs, an AP checks whether its Authenticator has cached a PMKSA for the PMKIDs and whether the AKM in the cached PMKSA matches the AKM in the (Re)Association Request; and if so, it shall assert possession of that PMKSA by beginning the 4-way handshake after association has completed. If the Authenticator does not have a PMKSA for the PMKIDs in the (Re)Association Request, its behavior depends on how the PMKSA was established. If SAE authentication was used to establish the PMKSA, then the AP shall reject (re)association by sending a (Re)Association Response frame with status code STATUS\_INVALID\_PMKID. Note that this allows the non-AP STA to fall back to full SAE authentication to establish another PMKSA. If IEEE Std 802.1X authentication was used to establish the PMKSA, the AP begins a full IEEE Std 802.1X authentication after association has completed.

If both sides assert possession of a cached PMKSA, but the 4-way handshake fails, both sides may delete the cached PMKSA for the selected PMKID.

If the lifetime of a cached PMKSA expires, the STA shall delete the expired PMKSA.

If a STA roams to an AP with which it is preauthenticating and the STA does not have a PMKSA for that AP, the STA needs to initiate a full IEEE Std 802.1X EAP authentication.

# CID 7727

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Clause Number | Page | Line | Comment | Proposed Change | Proposed Resolution |
| 3.2 | 42 | 1 | The definition of an RSNA assumes a 4WH, but for FT the non-initial, a.k.a. "FT Protocol authentication" (13.5.2/3), as distinct from the initial, a.k.a. "FT association" (13.4.2) procedure does not include a 4WH | Extend the definition to cover "FT Protocol authentication" | REVISED. Apply changes proposed for CID 7727 in <this document>. |

**Discussion**

Note: The page number in the comment is incorrect. The table above shows the correct location.

The comment is correct in identifying a missing case in ghe definition of RSNA. In fact, P802.11ai/D7.0 has already fixed this when adding FILS authentication. Since the FT protocol change is applicable to the base standard even before P802.11ai gets merged in, it sounds reasonable to fix this in REVmc even though that will result in some extra work for the P802.11ai editor to synchronize the draft with the updated REVmc draft.

## Proposed changes to address CID 7727

**3.2 Definitions specific to IEEE Std 802.11**

*Change the following definition in D5.4 page 43 lines 8-12 as shown:*

**robust security network association (RSNA):** The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-way handshake or FT protocol. Note that existence of an RSNA between two STAs does not of itself provide robust security. Robust security is provided when all STAs in the network use RSNAs.

# CID 7783

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Clause Number | Page | Line | Comment | Proposed Change | Proposed Resolution |
| 11.14 | 1720 | 1 | Since SA Query frames are robust, and receipt of any protected frame will do for SA Query, SA Query frames don't need a transaction identifier | Delete " and with a matching TransactionIdentifier" at 1625.6 and 1629.16Delete " with a TransactionIdentifier matching a TransactionIdentifier in an MLME-SA-QUERY.request issued in this SA Query procedure" at 1625.12 and 1629.22Delete " that has a matching transaction identifier" at 1720.1 | REVISED. Apply changes proposed for CID 7783 in <this document>. |

**Discussion**

From April 15 telecon: Action item #3: More Work needed – Reassign CID to Jouni, and have Mark, Jouni, and Adrian work out the details

Jouni: I went through more detailed analysis after that call and convinced myself of the proposed change being safe to do at high level. A bit modified version of the changes was prepared and discussed with Mark (cc’ing Adrian). Adrian recorded this in 273r9:

Note, in subsequent thread, **Jouni and Mark R agreed to the following resolution**:

Revised.

Delete " and with a matching TransactionIdentifier" at 1625.6 and 1629.16

Delete " that has a matching transaction identifier" at 1720.1

At 1625.12 and 1629.22 replace:

"If no MLME-SA-QUERY.confirm primitive with a TransactionIdentifier matching a TransactionIdentifier in an MLME-SA-QUERY.request issued in this SA Query procedure is received within the dot11AssociationSAQueryMaximumTimeout period"

with:

"If no MLME-SA-QUERY.confirm primitive for the STA is received within the dot11AssociationSAQueryMaximumTimeout period"

## Proposed changes to address CID 7783

**11.3.5.3 AP or PCP association receipt procedures**

*Change the (e) (3) and (4) items in D5.4 page 1660 lines 1-20 as shown:*

3) Following this, if the SME is not in an ongoing SA Query with the STA, the SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA every dot11AssociationSAQueryRetryTimeout TUs until an MLME-SA-QUERY.confirm primitive for the STA is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. The SME shall increment the TransactionIdentifier by 1 for each MLME-SA-QUERY.request primitive, rolling it over the value to 0 after the maximum allowed value is reached.

4) If no MLME-SA-QUERY.confirm primitive for the STA is received within the dot11AssociationSAQueryMaximumTimeout period, the SME shall allow a subsequent association process with the STA to be started without starting an additional SA Query procedure, except that the SME may deny a subsequent association process with the STA if an MSDU was received from the STA within this period.

NOTE 1—Reception of an MSDU implies reception of a valid protected frame, which obviates the need for the SA Query procedure.

**11.3.5.3 AP or PCP reassociation receipt procedures**

*Change the (e) (3) and (4) items in D5.4 page 1664 lines 10-29 as shown:*

3)  Following this, if the SME is not in an ongoing SA Query with the STA, the SME shall issue one MLME-SA-QUERY.request primitive addressed to the STA every dot11AssociationSAQueryRetryTimeout TUs until an MLME-SA-QUERY.confirm primitive for the STA is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure have passed. The SME shall increment the TransactionIdentifier by 1 for each MLME-SA-QUERY.request primitive, rolling it over to 0 after the maximum allowed value is reached.

4)  If no MLME-SA-QUERY.confirm primitive for the STA is received within the dot11AssociationSAQueryMaximumTimeout period, the SME shall allow a subsequent reassociation process to be started without starting an additional SA Query procedure, except that the SME may deny a subsequent reassociation process with the STA if an MSDU was received from the STA within this period.

 NOTE 1—Reception of an MSDU implies reception of a valid protected frame, which obviates the need for the SA Query procedure.

**11.14 SA Query procedures**

*Change the last paragraph of 11.14 in D5.4 page 1757 line 2 as shown:*

If a non-AP and non-PCP STA that has an SA with its AP or PCP for an association that negotiated management frame protection receives an unprotected Deauthentication or Disassociation frame with reason code INVALID\_CLASS2\_FRAME or INVALID\_CLASS3\_FRAME from the AP or PCP, the non-AP and non-PCP STA may use this as an indication that there might be a mismatch in the association state between itself and the AP or PCP. In such a case, the non-AP and non-PCP STA’s SME may initiate the SA Query procedure with the AP or PCP to verify the validity of the SA by issuing one MLME-SA-QUERY.request primitive every dot11AssociationSAQueryRetryTimeout TUs until a matching MLME-SA-QUERY.confirm primitive is received or dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure has passed. If the AP or PCP responds to the SA Query request with a valid SA Query response, the non-AP STA should continue to use the SA. If no valid SA Query response is received, the non-AP and non-PCP STA’s SME may delete the SA and temporal keys held for communication with the STA by issuing an MLME-DELETEKEYS.request primitive and the non-AP and non-PCP STA may move into State 1 (or State 2, for a DMG STA) with the AP.