IEEE P802.11
Wireless LANs

|  |
| --- |
| 11bi D0.4 CR for 12.14.6 |
| Date: 2024-07-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |

Abstract

This submission proposes resolutions for the following CIDs:

1465, 1466, 1467, 1468, 1469, 1470, 1472, 1473, 1225, 1496,

1392,

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Revision based on the discussion during the teleconference call
* Rev 2: Revision for 1225 and 1392
* Rev 3: Revision based on the discussion during the teleconference call

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbi D0.4 Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGbi D0.4 Draft. (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents). TGbi Editor: Editing instructions preceded by “TGbi Editor” are instructions to the TGbi editor to modify existing material in the TGbi draft. As a result of adopting the changes, the TGbi editor will execute the instructions rather than copy them to the TGbi Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **P.L** | **Comment** | **Proposed Change** | **Resolution** |
| 1465 | Mark RISON | 12.14.6 | 78.36 | "to have PMKSA caching privacy" would be better as "for PMKSA caching privacy" | As it says in the comment | Revised – Agree in principle with the commenter. TGbi editor to make the changes shown in 11-24/1181r1 under all headings that include CID 1465 |
| 1466 | Mark RISON | 12.14.6.1 | 78.47 | "After the indicated PMKID identifies a cached PMKSA " -- indicated where? | As it says in the comment | Revised – PMKID is indicated in an RSNE. TGbi editor to make the changes shown in 11-24/1181r1 under all headings that include CID 1466 |
| 1467 | Mark RISON | 12.14.6.1 | 78.54 | " For MLO, if any EDP non-AP STA affiliated with an EDP non-AP MLD and any EDP AP affiliated with an EDP AP MLD set the PMKSA Caching Privacy Support subfield in the RSNXE to 1" reads as if they could differ | Change to " For MLO, if the EDP non-AP STAs affiliated with an EDP non-AP MLD and the EDP APs affiliated with an EDP AP MLD set the PMKSA Caching Privacy Support subfield in the RSNXE to 1" | Accepted -  |
| 1468 | Mark RISON | 12.14.6.1 | 79.17 | "SPA address needs to be randomized in the frame indicating PMKID to identify cached PMKSA" -- articles missing. Also next subclause | As it says in the comment | Revised – Agree in principle with the commenter.TGbi editor to make the changes shown in 11-24/1181r1 under all headings that include CID 1468 |
| 1469 | Mark RISON | 12.14.6.2 | 79.29 | "If both a FTO and target FTR set the PMKSA Caching Privacy Support subfield in the RSNXE to 1, after the indicated PMKR0Name used by the target FTR to identify PMK-R1" -- I don't understand the after bit. After in time? After in some frame/element? | As it says in the comment | Revised– It means after the action “the indicated PMKR0Name used by the target FTR to identify PMK-R1”.We revise to make it read better.TGbi editor to make the changes shown in 11-24/1181r1 under all headings that include CID 1469 |
| 1470 | Mark RISON | 12.14.6.2 | 79.33 | "shall contact R0KH" -- what does "contact" mean here? Also missing article | Clarify | Revised – Agree in principle with the commenter. We use “send”.TGbi editor to make the changes shown in 11-24/1181r1 under all headings that include CID 1470 |
| 1472 | Mark RISON | 12.14.6.2 | 79.64 | "is not recomputed due to encryption of Reassociation Request and Response frame." is not clear: "is not recomputed, because the frames are encrypted", or "is not recomputed because the frames are encrypted, but might be recomputed for some other reason"? | Clarify | Revised – Agree in principle with the commenter. We use “because”TGbi editor to make the changes shown in 11-24/1181r1 under all headings that include CID 1472 |
| 1473 | Mark RISON | 12.14.6.2 | 80.01 | "The R0KH may then deliver the latest PMKR0Name to other R1KHs with corresponding PMK-R1 SA in the same mobility domain. The R1KH of the target FTR may also retrieve the latest PMKR0Name from the R0KH." -- shouldn't these be shalls? | As it says in the comment | Rejected – This does not need to be “shall” right away after recomputation because we also have the following procedure if PMK-R1 can not be eventually identified using PMKR0Name during FT protocol. *If PMKSA caching privacy is used, then the R1KH of the target FTR uses the**value of PMKR0Name to check if a PMK-R1 and corresponding PMKR1Name can be identified (see**12.6.1.1.4 (PMK-R1 security association)). If the target FTR does not identify a PMK-R1, it may attempt to retrieve that key from the R0KH identified by R0KH-ID.* |
| 1225 | Mark RISON |   | 0.00 | "latest derived" has been inserted in some places, but not all, and it's not clear why those locations need this to be stated explicitly but not the others | Revert the insertion | Revised – We revise to clarify that recomputation only happens if PMKSA caching privacy is used.TGbi editor to make the changes shown in 11-24/1181r3 under all headings that include CID 1225 |
| 1496 | Mark RISON | 13.8.1 | 87.31 | "If PMKSA caching privacy is not used, tThe target FTR can use the PMKR0Name to derive the PMKR1Name and check if a PMK-R1 can be identified." -- why is this not "uses ... checks" (or even shalls). Other locatinos in this and previous subclause do not use "can" | As it says in the comment | Rejected –The referred sentence is a baseline sentence. *“the target FTR can use the PMKR0Name to derive the PMKR1Name”* |
| 1392 | Mark RISON | 12.6.1.1 | 0.00 | I'm not sure about adding those "Latest derived"s. I think that by default everything is always the latest derived already | As it says in the comment | Revised – We revise to clarify that recomputation only happens if PMKSA caching privacy is used.TGbi editor to make the changes shown in 11-24/1181r3 under all headings that include CID 1225 |

**Discussion:**

**Proposal:**

*TGbi editor: Modify Clause 12.14.6 as follows (track change on):*

* PMKSA caching privacy(#1664r7)

This subclause defines rules for(#1465) PMKSA caching privacy such that the identifier related to PMKSA caching can be recomputed after using the identifier to establish PTKSA, thus, cannot be used for tracking.

A STA that sets the PMKSA Caching Privacy Support subfield in the RSNXE to 1 shall set the Encryption of the Frame Body Field of the (Re)Association Request/Response Frame Support subfield in the RSNXE to 1.

* PMKID privacy(#1664r7)

After the indicated PMKID in an RSNE(#1466) identifies a cached PMKSA (see 12.6.8.3 (Cached PMKSAs and RSNA key management)), and a PTKSA is established using the identified PMKSA,

* For non-MLO, if the EDP non-AP STA and the EDP AP set the PMKSA Caching Privacy Support subfield in the RSNXE to 1, both the EDP non-AP STA and the EDP AP shall recompute the PMKID for the identified PMKSA to be used next time.
* For MLO, if the EDP non-AP STA affiliated with an EDP non-AP MLD and the(#1467) EDP AP affiliated with an EDP AP MLD set the PMKSA Caching Privacy Support subfield in the RSNXE to 1, both the EDP non-AP MLD and the EDP AP MLD shall recompute the PMKID for the identified PMKSA to be used next time.

NOTE—For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

The PMKID shall be recomputed as:

 PMKID = Truncate-128(HMAC-Hash(Keyname, "PMK Name" || ANonce || SNonce))

where:

 Hash is the hash algorithm from the key derivation type (see

 Table 9-190 (AKM suiteselec tors)) for each AKM

 Keyname is the key stored as PMK or MPMK in the PMKSA (see 12.6.1.1.2 (PMKSA))

 ANonce is the Authenticator nonce used when the current PTKSA was established

 SNonce is the Supplicant nonce used when the current PTKSA was established

TBD for recalculating the PMKID for Suite B AKMs.

NOTE—For a different PMKID to ensure privacy, the SPA needs to be randomized in the frame indicating the PMKID to identify the cached PMKSA. As a result, tracking cannot be done on the MAC address. (#1468)

* PMKR0Name privacy(#637r1)

APs in the same mobility domain shall set the PMKSA Caching Privacy Support subfield in the RSNXE to the same value.

If both a FTO and target FTR set the PMKSA Caching Privacy Support subfield in the RSNXE to 1, after the target FTR uses the indicated PMKR0Name to identify the (#1469)PMK-R1 (see 13.8.1 (Overview)), and a PTKSA is established using the identified PMK-R1,

* the R1KH of the target FTR shall send the latest ANonce and SNonce to the R0KH, and (#1470)
* both the S0KH of the FTO and the R0KH (#1470)shall recompute the PMKR0Name.

NOTE—For MLO, all STAs affiliated with an MLD set the RSNXE to the same value.

The PMKR0Name shall be recomputed as follows:

 PMKR0Name = Truncate-128(HMAC-Hash( XXKey, "FT-R0N" || ANonce || SNonce))

where:

 Hash is the hash algorithm from the key derivation type (see Table 9-190 (AKM suite selectors)) for each AKM

 "FT-R0N" is treated as an ASCII string

 XXKey is defined in 12.7.1.6.3 PMK-R0

 ANonce is the Authenticator nonce used when the current PTKSA was established

 SNonce is the Supplicant nonce used when the current PTKSA was established

NOTE—For a different PMKR0Name to ensure privacy, the SPA needs to be randomized in the frame indicating the PMKR0Name to identify the cached PMK-R0 security association. As a result, tracking can not be done on the MAC address. (#1468)

NOTE—PMKR1Name is still derived based on the indicated PMKR0Name with the same formula defined in 12.7.1.6.4 (PMK-R1) for the first time and PMKR1Name once derived is not recomputed because the Reassociation Request and Response frame that carry PMKR1Name are encrypted(#1472).

The R0KH may then deliver the latest PMKR0Name to other R1KHs with corresponding PMK-R1 SA in the same mobility domain. The R1KH of the target FTR may also retrieve the latest PMKR0Name from the R0KH.

*TGbi editor: Modify Clause 9.4.2.23.5 as follows (track change on):*

* PMKID(#1664r7)

***Change third and fourth paragraph (not all shown) as follows:***

A PMKID in the PMKID List field can refer to

* The PMKID of a cached PMKSA that has been obtained through preauthentication with the target AP
* The PMKID of a cached PMKSA from an EAP, FILS, or SAE authentication
* The PMKID of a PMKSA derived from a PSK for the target AP

d) If PMKSA caching privacy is used, the recomputed PMKID

e) The PMKR0Name of a PMK-R0 security association derived as part of an FT initial mobility domain association

f) If PMKSA caching privacy is used, the recomputed PMKR0Name as part of a fast BSS transition(#637r1)

g) The PMKR1Name of a PMK-R1 security association derived as part of an FT initial mobility domain association or as part of a fast BSS transition.(#1225)

See 12.7.1.3 (Pairwise key hierarchy), ~~and~~ 12.7.1.6.3 (PMK-R0), and 12.14.6.1 (PMKID privacy) for the construction of the PMKID, 13.8 (FT authentication sequence) for the population of PMKID List for fast BSS transitions, 12.6.8.3 (Cached PMKSAs and RSNA key management) for the population of PMKID List when using PMKSA caching, 13.4 (FT initial mobility domain association) for the population of PMKID List for FT initial mobility domain association, 12.11.2 (FILS authentication protocol) for the population of PMKID List with FILS authentication, ~~and~~ 12.7.1.6 (FT key hierarchy), and 12.14.6.2 (PMKR0Name privacy) for the construction of PMKR0Name and PMKR1Name.(#637r1)

* PMKSA(#1664r7)

***Change first bullet of the third paragraph (not all shown) as follows:***

A PMKSA association is bidirectional. In other words, both parties use the information in the security association for both sending and receiving. The PMKSA is used to create the PTKSA. PMKSAs have a certain lifetime. The PMKSA consists of the following:

PMKID, as defined in 12.7.1.3 (Pairwise key hierarchy) or 12.7.1.6.3 (PMK-R0). The PMKID identifies the security association.

* If PMKSA caching privacy is used, recomputed PMKID as defined in(#1225) 12.14.6.1 (PMKID privacy). (#1225)
* PMK-R0 security association(#637r1)

***Change fifth bullet of the first paragraph (not all shown) as follows:***

The PMK-R0 security association is the result of a successful completion of the IEEE 802.1X authentication, SAE authentication, or use of PSK during the FT initial mobility domain association. This security association is bidirectional. It has a certain lifetime. It consists of the following:

* SSID
* MDID
* PMK-R0
* R0KH-ID
* PMKR0Name
* If PMKSA caching privacy is used, recomputed PMKR0Name (#1225)
* PMK-R1 security association(#637r1)

***Change eighth bullet of the second paragraph (not all shown) as follows:***

This security association is bidirectional. It has a certain lifetime. It consists of the following:Latest derived

* SSID
* MDID
* PMK-R1
* PMK-R1 lifetime
* PMKR1Name
* R1KH-ID
* R0KH-ID
* PMKR0Name
* If PMKSA caching privacy is used, recomputed PMKR0Name (#1225)