802.11bi Draft Specification

|  |
| --- |
| Proposed spec texts for PMKID requirement |
| Date: 2023-10-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  |  |  |
| Johannes Berg |  |  |  |  |
| Ilan Peer |  |  |  |  |
| Robert Stacey |  |  |  |  |

Abstract

This submission proposes spec text based on the following passed requirement.

* ***11bi shall define a mechanism to prevent an eavesdropper distinguishing whether reassociation exchanges between CPE Clients and CPE APs use identical PMK or distinct PMK***

Revision History:

* Rev 0: Initial version of the document
* Rev 1: Revision based on the comments received for PMKID privacy during Nov 2023 F2F. Changes related to PMKID privacy are marked with green. Also, tag all proposals related to FT as **<tag FT>. <tag FT>** is not part of the texts to be proposed for the 11bi draft. It is mainly to differentiate the proposal for FT.
* Rev 2: Revision based on the SP and discussion with Dan Harkins. Changes are marked with blue.
* Rev 3: Revision based on the suggestion from Jouni on ANonce and SNonce.
* Rev 4: Remove all <tag FT> change and revision based on the discussion in the meeting. Also update discussion.
* Rev 5: Revision for missing “)” and fixing spelling error.
* Rev 6: Align the clause number based on D0.1
* Rev 7: change during the teleconference call

***Editing instructions formatted like this are intended to be copied into the TGbi 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 or insert 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.***

**Discussion:**

Based on the SP in the 11bi meeting in Jan IEEE meeting, there is a strong support to have a compact formula of PMKID recomputation for all AKMs. Also, using ANonce and SNonce is the preferred route after offline discussion. As a result, the texts are now updated based on the latest discussions.

|  |
| --- |
|  |

**Proposed Texts:**

**TGbi Editor: *Instruction: Insert new rows in Table 9-363 in 9.4.2.241 RSNXE as shown below***

9.4.2.241 RSNXE

|  |
| --- |
| * **Extended RSN Capabilities field**
 |
| **Bit** | **Information** | **Notes** |
| <ANA> | PMKSA Caching Privacy Support | A EDP STA sets the PMKSA Caching Privacy Support subfield to 1 if dot11EDPPMKSACachingPrivacySupportActivated is true. Otherwise, this subfield is set to 0. See 12.14.x (PMKSA Caching Privacy Support). |

**TGbi Editor: *Instruction: Insert 12.14.x PMKSA caching privacy as shown below***

**12.14 Client Privacy Enhancement**

**12.14.x PMKSA caching privacy**

This subclause defines rules to have 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.

**12.14.x.1 PMKID privacy**

After the indicated PMKID 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 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, 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 suite selectors)) 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, SPA address needs to be randomized in the frame indicating PMKID to identify cached PMKSA. As a result, the tracking cannot be done on MAC address.

**TGbi Editor: *Instruction: Modify 9.4.2.23.5 as shown below***

* **PMKID**

The PMKID Count field indicates the number of PMKIDs that are contained in the PMKID List field. The PMKID List field contains a series (possibly empty) of PMKIDs.

When one or more PMKIDs are included in a (Re)Association Request frame or FILS Authentication frame to an AP, they identify PMKSAs that the STA believes to be valid for the destination AP. When a PMKID is included in a FILS Authentication frame to a STA, it identifies a PMKID that the AP has selected.

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 latest derived PMKID of a cached PMKSA from an EAP, FILS, or SAE authentication
* The latest derived PMKID of a PMKSA derived from a PSK for the target AP
* The PMKR0Name of a PMK-R0 security association derived as part of an FT initial mobility domain association
* 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.

See 12.7.1.3 (Pairwise key hierarchy), 12.7.1.6.3 (PMK-R0), and 12.14.x.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)

for the construction of PMKR0Name and PMKR1Name.

NOTE—A STA need not insert a PMKID in the PMKID List field if the STA (M118)is not using that PMKSA.

**TGbi Editor: *Instruction: Modify 12.6.1.1.2 PMKSA as shown below***

* **PMKSA**

The PMKSA is created by the Authenticator’s SME and Supplicant’s SME when EAP authentication, SAE authentication, (#1084)FILS authentication, or an OWE exchange completes successfully, or when the PSK is configured.

When the negotiated AKM uses PMKID derivation with (#3744)PTK-KCK as a parameter as defined in 12.7.1.3 (Pairwise key hierarchy), the PMKID derived from the PTK-KCK during the initial 4-way handshake is not changed during the lifetime of this PMKSA.

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:

* Latest derived PMKID, as defined in 12.7.1.3 (Pairwise key hierarchy) or 12.7.1.6.3 (PMK-R0) or 12.14.x.1 (PMKID privacy). The PMKID identifies the security association.
* Authenticator’s or peer’s MAC address. For multi-band RSNA, the MAC address is associated with the operating band in use when the PMKSA is established.
* PMK; or if the PMKSA was established with an (#3266)AKMP for which the Authentication type column includes FT authentication (see Table 9-188 (AKM suite selectors)), MPMK (see 12.7.1.6.3 (PMK-R0)).
* Lifetime, as defined in 12.7.1.3 (Pairwise key hierarchy) or 12.7.1.6 (FT key hierarchy).
* AKMP.
* All authorization parameters specified by the AS or local configuration. This might include parameters such as the STA’s authorized SSID.
* Cache Identifier, if advertised by the AP in FILS Indication element.