802.11bi Draft Specification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed spec texts for PMKID requirement follow up | | | | |
| Date: 2024-03-27 | | | | |
| 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 follow up spec text for FT 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

***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:**

We have concluded the recomputation of PMKID based on SNonce and ANonce.

For FT, the identifier becomes PMKR0Name while roaming.

A close-up of a document

Description automatically generated

We follow similar design principles to use ANonce and SNonce for the derivation for PMKR0Name as well.

A white paper with black text

Description automatically generated

Reference for current spec texts in revme D5.0.

A close-up of a computer code

Description automatically generated

A close-up of a document

Description automatically generated

A white background with black text

Description automatically generated

**Proposed Texts:**

**TGbi Editor: *Instruction: Modify 12.14.6 PMKSA caching privacy as shown below***

**12.14 Client Privacy Enhancement**

**12.14.6 PMKSA caching privacy**

**12.14.6.2 PMKR0Name privacy**

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 indicated PMKR0Name used by the target FTR to identify PMK-R1 (see 13.8.1 (Overview)), and a PTKSA is established using the identified PMK-R1,

* the R1KH of the target FTR shall contact R0KH to provide the latest S0KH-ID, and
* both the S0KH of the FTO and the R0KH contacted by the target FTR 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 (seeTable 9-190 (AKM suiteselectors)) 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, SPA address needs to be randomized in the frame indicating PMKR0Name to identify cached PMK-R0 security association. As a result, the tracking can not be done on MAC address.

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 due to encryption of Reassociation Request and Response frame.

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: *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 latest derived PMKR0Name of a PMK-R0 security association derived as part of an FT initial mobility domain association or recomputed as part of a fast BSS transition
* 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), ~~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.

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 12.6.1.1.3 as shown below***

* **PMK-R0 security association**

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
* (#1776)MDID
* PMK-R0
* R0KH-ID
* Latest derived PMKR0Name
* Latest S0KH-ID
* PMK-R0 lifetime
* Pairwise cipher suite selector
* All authorization parameters specified by the AS or local configuration

**TGbi Editor: *Instruction: Modify 12.6.1.1.4 as shown below***

* **PMK-R1 security association**

The PMK-R1 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 or
* A successful completion of the authentication phase in the fast BSS transition to the target AP

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

* SSID
* MDID
* PMK-R1
* PMK-R1 lifetime
* PMKR1Name
* R1KH-ID
* R0KH-ID
* Latest derived PMKR0Name
* Latest S0KH-ID
* Latest S1KH-ID
* Pairwise cipher suite selector
* All authorization parameters specified by the AS or local configuration

**TGbi Editor: *Instruction: Modify 13.5.2 as shown below***

* **Over-the-air FT protocol authentication in an RSN**

(…existing texts…)

If PMKSA caching privacy is not used, the R1KH of the target FTR uses the value of PMKR0Name and other information in the frame to calculate PMKR1Name and check if a PMK-R1 can be identified with the PMKR1Name. 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 retrieve that key from the R0KH identified by the FTO. See 13.2 (Key holders). Upon receiving a new PMK-R1 for a STA, the target AP shall delete the prior PMK-R1 security association and PTKSAs derived from the prior PMK-R1.

(…existing texts…)

**TGbi Editor: *Instruction: Modify 13.8.1 as shown below***

* **Overview**

(…existing texts…)

The first message is used by the FTO to initiate a fast BSS transition. When RSNA is enabled, the FTO shall include the R0KH-ID and the SNonce in the FTE and the PMKR0Name in the RSNE. If PMKSA caching privacy is not used, the target FTR can use the PMKR0Name to derive the PMKR1Name and check if a PMK-R1 can be identified. 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. See 13.2 (Key holders). The FTO includes a fresh SNonce as its contribution to the association instance identifier and to provide key separation of the derived PTK; it is selected randomly to serve as a challenge that demonstrates the liveness of the peer in the fourth message.

(…existing texts…)