IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| SB1 Proposed text for PMKSA from PASN for PMKSA caching |
| Date: 2023-11-28 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

 |

Abstract

This submission proposes texts for PMKSA from PASN for PMKSA caching on P802.11-REVme D4.1:

**Revision History:**

R0: Initial version.

## Discussion:

PMKSA generated through PASN currently cannot be used as part of the PMK caching to be used later and can only be used to generated PTKSA of PASN. Conceptually, PMKSA generated through PASN goes through similar authentication procedure using tunneling, and as a result, the PMKSA generated through PASN should be able to be used as part of the PMKSA caching without further limitation if the only modification of the authenticatino procedure is just tunneling.

This document proposes change to enable PMKSA generated by PASN to be used as PMK caching.

Note that to use PMKSA caching and go to association, a non-PASN authentication like open authentication is required to change the state from 1a to 2, then follow by (re)association request with PMKID carried in the RSNE. This is already covered by the existing texts and can be used after removing the restriction of using the PMKSA derived during PASN only for the PTK derivation of PASN.

## Proposed Text Update:

*Instruction to TGme Editor: Update REVme D4.1 12.13.1 as shown below (track change on).*

**12.13 Preassociation security negotiation**

**12.13.1 General**

(…existing texts…)

PASN is primarily intended for use in infrastructure networks for a STA and an AP to establish a PTKSA using a three-message authentication frame exchange. Some salient aspects of this protocol are:

* Where available, it leverages a cached PMK for a Base AKMP or already specified mechanisms for a Base AKMP to establish the PMKSA from which the PASN PTKSA is derived. Such a PTKSA provides mutual authentication.
* It leverages a cached PMK for a Base AKMP or already specified mechanisms for a Base AKMP to establish the PMKSA from which the PASN PTKSA is derived.
* It exchanges ephemeral public keys to provide PFS and derive the PTKSA keys, using a PMKSA if one exists. The PASN AKMP shall not be used in the RSNE of an (re)association request.

(…existing texts…)

*Instruction to TGme Editor: Update REVme D4.1 12.13.4 as shown below (track change on).*

**12.13.4 PASN authentication with FILS shared key**

(…existing texts…)

The PMKSA is then used in PTKSA derivation for PASN authentication. The PMKID of the PMKSA is derived as defined in 12.11.2.5.2 (PMKSA key derivation with FILS authentication) and the AKMP of the PMKSA is the corresponding Base AKMP.

*Instruction to TGme Editor: Update REVme D4.1 12.13.5 as shown below (track change on).*

**12.13.5 PASN authentication with SAE**

(…existing texts…)

The PMKSA is then used in PTKSA derivation for PASN authentication. The PMKID of the PMKSA is derived as defined in 12.4.5.4 (Processing of a peer’s SAE Commit message) and the AKMP of the PMKSA is the corresponding Base AKMP. If establishment of SAE PMKSA fails, PASN authentication shall be abandoned.