IEEE P802.11
Wireless LANs

|  |
| --- |
| [place document subject title text here] |
| Date: 2017-07-01 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Gabor Bajko | Mediatek | 2840 Junction Rd |  | Gabor.bajko@mediatek.com |
|  |  |  |  |  |

Abstract

[802.11-2016 spec defines the use of SAE authentication and key establishment protocol.

One could read the text in a way that key generation has to happen within dot11RSNASAERetransPeriod (timer t0), otherwise SAE messages are retransmitted.

Here it is proposed to add two minor clarifications to prevent misinterpretation.

Editor: add the following text to section 12.4.8.4:

12.4.8.4 Timers

The parent SAE process does not use timers. Each protocol instance can set timers that result in fire() events

to be sent to itself. The following timers can be set:

— t0—A retransmission timer (this timer is not used when STAs operate in infrastructure mode)

— t1—A PMK expiration timer.

Editor: add the following text to the description of the MIB variable:

dot11RSNASAERetransPeriod OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a control variable.

It is written by the SME when establishing or becoming a member of a BSS.

Changes take effect for the next MLME-START.request primitive.

This object specifies the initial retry timeout, in millisecond units,

used by the SAE authentication and key establishment protocol."

DEFVAL { 40 }

::= { dot11RSNAConfigEntry 40 }

Note, this variable is not used when STAs operate in infrastructure mode.

**References:**