Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	PMK and AK switch time definition
Date Submitted	**2005-06-09**

Source(s)	Avishay Shraga	Avishay.shraga@intel.com
	Yigal Eliaspur	Voice: +972-54-5551063
	Intel corp.	Yigal.Eliaspur@intel.com
		Voice: +972-54-7884877

Re:	IEEE P802.16e/D8
Abstract	Sync the switch time of PMK following re-authentication
Purpose	Sync the switch time of PMK following re-authentication
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

PMK and AK switch time definition

Avishay Shraga

1. Motivation

In PMKv2 PMK and its associated AK(s) are synchronically created by both sides on re-authentication thus can be activated synchronically.

2. Proposed solution

Start using the new PMK for Tx immediately after successful SA-TEK exchange and add a TLV to SA-TEK-response defining in which frame the old PMK stop being valid for Rx as well

3. Changes summary

7.2.1.6 Authorization state machine

7.2.1.6.x PKMv2 PMK and AK switching methods

Once the SA-TEK 3-way hand shake is successfully completed, the BS and SS shall start using the new AK matching the new PMK context for transmitting packets.

The old AK matching the old PMK context may be used for receiving packets before the "frame number" attribute specified in SA-TEK-response message.

6.3.2.3.9.19 SA-TEK-Response message

Add the row to Table 37i—SA-TEK-Response message attributes

Attribute	Contents
NonceSS	…
BS_random	…
AKID	…
SA_TEK_Update	…
Frame_Number	An absolute frame number in which the old PMK and all its associate AKs should be discarded.
CMAC tuple/HMAC tuple	…

11.9 PKM-REQ/RSP management message encodings

Add to table 370 PKM attribute types

Type	Pkm attribute
Xx	Frame number

11.9.35 Frame number

Type	Length	value
xx	3	Lower 24 bits of the frame number in which the old PMK and all its associate AKs should be discarded.