IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>

Title	**Pre-Authentication support for PKMv2**	
Date Submitted	**2004-06-24**	
Source(s)	JUNHYUK SONG, Samsung	junhyuk.song@SAMSUNG.COM
	David, Johnston, Intel	dj.johnston@INTEL.COM
	Youngman Park, Korea	Youngman@kt.co.kr
Re:	Re: Security Adhoc PKMv2	
Abstract	Proposal for Pre-Authentication for PKMv2	
Purpose	Discuss and Adopt as the baseline text	
Notice	s 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>.	

1

Pre-Authentication

JunHyuk Song, Samsung Electronics
David Johnston, Intel corp
Young-Man Park, Korea Telecom

The Pre_authentication is one of the requirements of PKMv2 that reduces authentication signaling messages when MSS handoff to target. With the introduction of new PKM messages, PKM-PRE-AUTH MSS is given a chance to skip a number of PKM authentication messages. This will allow MSS to handoff to target BS in seamless way

[Add the following as shown]

Attributes

PKM attributes carry the specific authentication, authorization, and key management data exchanged between client and server. Each PKM packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a PKM message. The end of the list of attributes is indicated by the LEN field of the MAC PDU header.

Table 28a – PKM Message codes

Code	PKM Message Type	MAC Message Type
14	Pre-Auth-Req	PKM-REQ
15	Pre-Auth-Rsp	PKM-RSP

[Add the following to section 6.4.2.4.9:]

6.3.2.3.9.12 Pre-Authentication Request message

The message is sent by MSS to BS to establish Pairwise Master Key with Target BS for Handoff

Code: 14

Attributes are shown in Table 40

Table 40-PKM-Pre-Auth-Req attributes

Attribute	Contents
Target BSID	Target BSID that MSS will connect after HO
OMAC Tuple	Message Digest calculated using OMAC_KEY

The Target BSID attribute contains target BSID that MSS notified Serving BS for Handoff.

The OMAC Tuple attribute shall be the final attribute in the message's attribute list

6.3.2.3.9.13 Pre-Authentication Reply Message

Sent by the BS to a client SS, the Pre Authentication Reply message contains Target BSID, PMK, the key's lifetime, and OMAC tuple that protect the message

Code: 15

Attributes are shown in Table 41

Table 41-PKM-Pre-Auth-Response attributes

Attribute	Contents
Target BSID	Target BSID that MSS will connect after HO
PMK	Pairwise Master Key generated by Authorization Server, encrypted with MSS's public Key
PMK-Lifetime	PMK's active lifetime
OMAC Tuple	Message Digest calculated using OMAC_KEY_