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
Re:	Re: Security Adhoc PKMv2
Abstract	Supercede 200 and 206
Purpose	Discuss and Adopt as the baseline text
Notice	; 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>.

Revision History

Version	Changes
Rev 1.	1. Supercede C80216e-04/206r1 and harmonize together.

Pre-Authentication

David Johnston, Intel Corporation
Jesse Walter, Intel Corporation
Philip Barber, Broadband Mobile Technologies, Inc.
JunHyuk Song, Samsung Electronics
Young-Man Park, Korea Telecom
Doonie, Dongkie Lee, SK Telecom

Pre-Authentication is a secure, fast handover mechanism. It is based on the principle that a centralized AAA server established a shared private key MK between itself and the SS, using an EAP method, and populates multiple base stations with a PMK (Pairwise Master Key) that is derived from the MK and the identifies of the BS and SS.

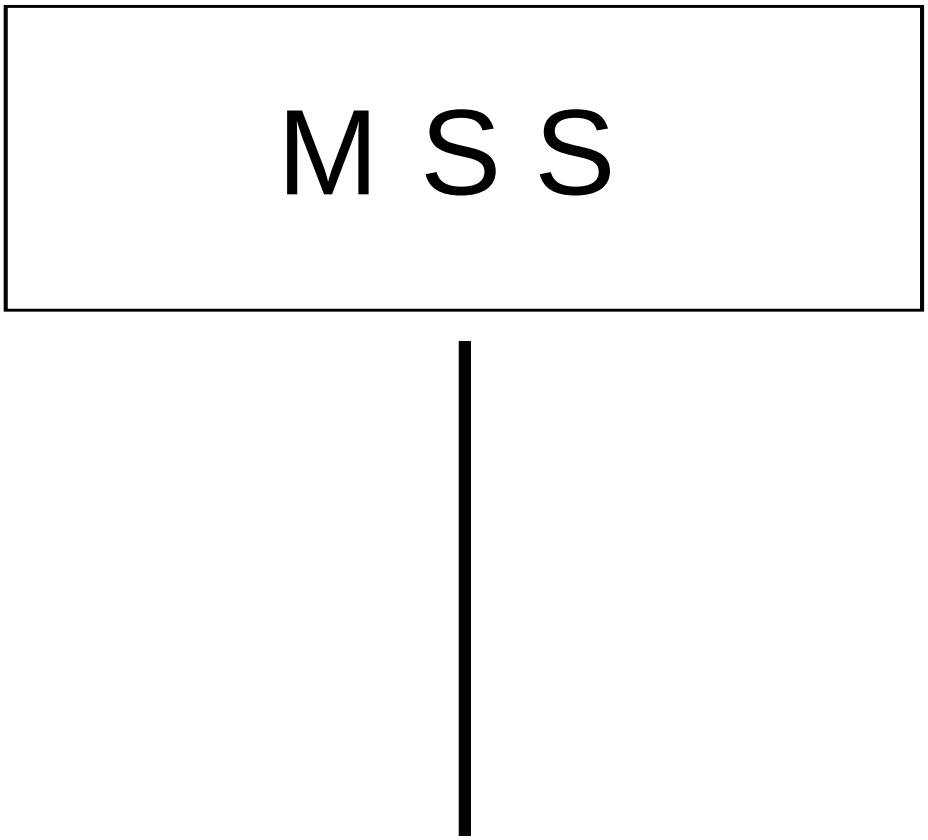

Figure-1 Example backbone message call flow

Figure-1 describes example call flow of pre-authentication that reduce PKM authorization and EAP messages. In this call flow Target BSs send a backbone message to AS so as to get MK (Master Key) that later on used for PMK generation in both MSS and determined target BS.

[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
18	Pre-Auth-Req	PKM-REQ
19	Pre-Auth-Rsp	PKM-RSP
20	Pre-Auth-Reject	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: 18

Attributes are shown in Table 40

Table 40-PKM-Pre-Auth-Req attributes

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

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

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

Inclusion of the keyed digest allows the receiving SS to authenticate the Pre Auth Request

6.3.2.3.9.13 Pre-Authentication Reply Message

Sent by the BS to a client SS in response to Pre-Authentication Request or unsolicited manners, the Pre Authentication Reply message contains one or more Target BSID and OMAC tuple that protect the message

Code: 19

Attributes are shown in Table 41

Table 41-PKM-Pre-Auth-Response attributes

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

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

Inclusion of the keyed digest allows the receiving SS to authenticate the Pre Auth Request

6.3.2.3.9.14 Pre-Authentication Reject Message

Sent by the BS to a client SS, receipt of a Pre-Auth Reject message indicates to the receiving SS, that the BS identified by the BSID in the associated Pre-Auth Request message and repeated in the response, is not populated with a valid PMK.

Code: 20

Attributes are shown in Table 41

Table 42-PKM-Pre-Auth-Reject attributes

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

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

Inclusion of the keyed digest allows the receiving SS to authenticate the Pre Auth Request

7.x.x.x Pre-Authentication

After a HO-REQ/RSP exchange, an SS may seek to use pre-authentication to effect a fast handover. An SS seeking to use pre-authentication shall transmit a PKM_PREAUTH-REQ.

A BS on recipt of a PKM-AUTH-REQ message shall reply with a PKM-PREAUTH-RSP message, or with a PKM_PREAUTH-REJECT message.

A BS may send an unsolicited PKM_AUTH-RSP message.

A PKM-PREAUTH-RSP indicates that the chosen BS is populated with a PMK coupled to the identity of the requesting SS.

The pre-authenticated SS may skip the authorization and EAP stages of network entry. The primary keying material available at the BS and SS shall be the computed PMK as defined in 7.x.x.x key Hierarchy. Therefore the AK computation will be based on the PMK and not the PAK, consistent with the AK computation rules in the PKMv2 key hierarchy.

[Modify Table 368 as follows:]

Type	PKM Attribute
0-5	*reserved*
6	Display-String
7	AUTH-Key
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	reserved
15	CBC-IV
16	Error-Code
17	CA-Certificate
18	SS-Certificate
19	Security-Capabilitie
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	Version
23	SA-Descriptor
24	SA-Type
25	AA-Descriptor
26	AA-Type
27	PKM Configuration Settings
28	Target BSID
29-255	reserved

[Add 11.9.21 as follows:]

11.9.21 Target BSID

Type	Length	Value
28	6	Target BSID