Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Enhanced Pre-Auth-request/reply message
Date Submitted	**2005-01-25**
Source(s)	Jianjun(Alen) Wu, Duke Dang HUAWEI No.98,Lane91,Eshan Road,Pudong ,Shanghai,China Pudong Lujiazui Software Park ,200127 P.R. China, Voice: 86-21-68644808-24717 Fax: 86-21-50898375 mailto: wujianjun@huawei.com
Re:	Contribution on comments to IEEE P802.16e/D5a
Abstract	Enhanced Auth-request/reply message
Purpose	Adoption
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>.

Enhanced Pre-Auth- request/reply message

Jianjun (Alen) Wu, Duke Dang
HUAWEI

1. Introduction

In the current IEEE P802.16e/D5a, it defines HO process. To shorten handover process, the network re-entry and initiation process during HO can complete in advance by using pre_authentication process.
In the current draft, pre_authentication during handover have not included the authentication process , just the Serving BS notify authentication result to Target BS.
We think this process is not reasonable for RSA based certificate authentication method, because the process is based on the following Assumption:

1. Assume the Serving BS is security.
2. Assume the Serving BS cannot leak out the key.

We think that we need an intact pre_authentication process. In order to accomplish the intact pre_authentication process, we must enhance the pre-auth-request and pre-auth-reply message. We can add the Authentication Message TLV encoded attributes included by Auth-request/reply and EAP-request/reply message.When pre-authentication can be accomplished by serving BS and Target BS on backbone network, and after accomplishing the Ranging process between the MSS and Target BS, the Target BS can unsolicited send Pre-auth-reply/reject to the MSS for notifying the authentication result£¨or Target BS can notifying the authentication result by Serving BS unsolicited sending Pre-auth-reply/reject to the MSS before the MSS performing the actual handover.
Before the MSS hand over to a Target BS, the MSS can send pre-auth-request to Serving BS, and Serving BS will accomplish the pre-authentication process to Target BS by backbone network.

This contribution enhances the messages pre-auth-request and pre-auth-reply.

2. Proposed Text Changes

Modify the text of Page 38£¨Line21 in IEEE P802.16e/D5a in section 6.3.2.3.9.16 shown as following .

6.3.2.3.9.16 Pre-Auth-Request message

The Pre-Auth-Request message is sent by the MSS to the BS to establish Pairwise Master Key with the target BS for handoff.
Code: 18
Attributes are shown in Table 37f.

Table 37f—PKM Pre-Auth-Request attributes

Attributes	Contents
Target BSID	The BSID to which an MSS will connect after HO.
Authentication Message	The Content of the auth request message or EAP request message.
OMAC Tuple	Message Digest calculated using OMAC_KEY

The target BSID attribute contains one or more target BSIDs. The MSS notified the serving BS of these BSID(s) for handoff.

The Authentication Message attribute shall include TLV encoded attributes included by Auth-request/EAP-request in normal auth request process°£

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

Inclusion of the keyed digest allows the receiving MSS to authenticate the Pre-Auth-Request.

Modify the text of Page 38£ Line55 in IEEE P802.16e/D5a in section 6.3.2.3.9.17 shown as following .

6.3.2.3.9.17 Pre-Auth-Reply message

Sent by the BS to a client SS in response to Pre-Auth-Request or in an unsolicited manner, the Pre- Auth-Reply message contains one or more target BSIDs and an OMAC tuple.
Code: 19
Attributes are shown in Table 37g.

Table 37g—PKM Pre-Auth-Reply attributes

Attributes	Contents
Target BSID	The BSID that MSS will connect after HO.
Authentication Message	The Content of the auth reply message or EAP reply message.
OMAC Tuple	Message Digest calculated using OMAC_KEY

The Authentication Message attribute shall include TLV encoded attributes included by Auth-Reply/EAP-Reply in normal auth reply process°£

The OMAC Tuple attribute shall be the final attribute in the message's attribute list.
Inclusion of the keyed digest allows the receiving MSS to authenticate the Pre-Auth-Request.