Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Enhancement of PKMv2 Pre-authentication**
Date Submitted	**2005-03-09**
Source(s)	Chulsik Yoon csyoon@etri.re.kr Seokheon Cho Taeyong Lee Sungcheol Chang ETRI 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea
Re:	Contribution on comments to IEEE P802.16e/D6
Abstract	In this contribution, we propose to enhance the pre-authentication concept to the various cases of authorization modes.
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 text 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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Enhancement of PKMv2 Pre-authentication

Chulsik Yoon, Seokheon Cho, Taeyong Lee, and Sungcheol Chang

ETRI

Introduction

There are some problems in pre-authentication concept in the draft specification P802.16e/D6.

1) There are various types of authorization modes in PKMv2, such as only RSA-based Authorization procedure, only EAP-based Authorization procedure, and both RSA-based Authorization and EAP-based Authorization (e.g. EAP Transfer mode and protected EAP Transfer mode) procedure. Current pre-authentication mechanism for PKMv2 in P802.16e/D6 is only applicable to the only EAP-based authorization procedure. In section 7.7 Pre-authentication, it is described as:

"The pre-authenticated MSS may skip the authorization and EAP stages of network entry. The primary keying material available at the BS and the MS shall be 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."

Therefore, the pre-authentication mechanism should be enhanced to support various types of authorization modes.

2) After performing pre-authentication mechanism, both BS and MS shall share the same AK. However, the AK sequence number and the AK lifetime cannot share between BS and MS. In order to share those parameters, those parameters should be included in the response message to pre-auth request.

3) It is reasonable that Nonce from the MS and Nonce from the BS are used to derive the Authorization Key (AK). Also, the AK should be shared before the RNG-REQ/RNG-RSP exchange between the MS and the target BS for assuring message authentication. Therefore, Nonce exchange between the MS and the target BS is necessary in the pre-authentication procedure.

This contribution provides a resolution for those problems.

Proposed Text Changes

[In P802.16e/D6, Modify the Section 7.7 as follows:]

7.7 Pre-authentication

After a HO-REQ/RSP exchange, an MS may seek to use pre-authentication to effect a fast handover. An MS seeking to use pre-authentication shall transmit a ~~PKM_PREAUTH-REQ~~ PKMv2 Pre-Authentication-Request message.

A BS on receipt of a ~~PKM_PREAUTH-REQ~~ PKMv2 Pre-Authentication-Request message shall reply with a ~~PKM_PREAUTH-RSP~~ PKMv2 Pre-Authentication-Reply message, or with a ~~PKM_PREAUTH-REJECT~~ PKMv2 Pre-Authentication-Reject message.

A BS may send an unsolicited ~~PKM_PREAUTH-RSP~~ PKMv2 Pre-Authentication-Reply message.

A ~~PKM_PREAUTH-RSP~~ PKMv2 Pre-Authentication-Reply indicates that the target BS has a valid PAK or/and a valid PMK. ~~that the chosen BS is populated with a PMK coupled to the identity of the requesting MS and the PAK transferred from the serving BS or from the ASA server.~~

The pre-authenticated MS may skip ~~the authorization and EAP stages of network entry~~ the RSA-based Authorization procedure or/and the EAP-based Authorization procedure and even the MS's Authorization Key procedure. The primary keying material available at the BS and MS shall be the computed using the PAK and the PMK as defined in ~~7.x.x.x~~ 7.2.2.2.10 key Hierarchy. Therefore the AK computation will be based on the PAK and the PMK ~~and not the PAK~~ depending on the authorization mode of the MS and the target BS, consistent with the AK computation rules in the PKMv2 key hierarchy.

[Reorder sub-clauses 6.3.2.3.9.12-6.3.2.3.9.14 to 6.3.2.3.9.28-6.3.2.3.9.30] and
[Change reordered sub-clauses as follows]

~~6.3.2.3.9.12 Pre-Authentication Request message~~
6.3.2.3.9.28 PKMv2 Pre-Authentication-Request message

The ~~Pre-Auth-Request~~ PKMv2 Pre-Authentication-Request message is sent by MS to BS to establish ~~Primary Master Key (PMK)~~ Authorization Key (AK) with Target BS for Handoff.

Code: ~~18~~ 30

Attributes are shown in Table ~~37f~~ 37r.

Table ~~37f~~ 37r– ~~PKM Pre-Auth-Request~~ PKMv2 Pre-Authentication-Request attribute

Attribute	Contents
(one or more) Target	The BSID that an MSS will connect after HO

BSID(s)	
MS_Nonce	A 64bit freshly-generated number from the MS
OMAC Tuple	Message Digest calculated using OMAC_KEY_U

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

MS_Nonce is a freshly generated number from the MS. This attribute is used to derive the new AK that is valid with the target BS.

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

Inclusion of the keyed digest allows the receiving MS to authenticate the ~~Pre-Auth Request~~ PKMv2 Pre-Authentication-Request message. The OMAC_KEY_U is shared between the MS and the serving BS.

~~6.3.2.3.9.12 Pre-Authentication Reply message~~
6.3.2.3.9.29 PKMv2 Pre-Authentication Reply message

Sent by the BS to a client SS in response to ~~Pre-Authentication Request~~ PKMv2 Pre-Authentication Reply message or in an unsolicited manner, the PKMv2 Pre-Authentication Reply message contains one or more Target BSID and OMAC tuple.

Code: ~~19~~ 31

Attributes are shown in Table ~~37g~~ 37s.

Table ~~37g~~ 37s– ~~PKM Pre-Auth-Reply~~ PKMv2 Pre-Authentication-Reply attribute

Attribute	Contents
(one or more) Target BSID(s)	The BSID that an MS will connect after HO
Privacy Capabilities Parameters	Privacy capabilities negotiated with the target BS
Key Sequence Number	AK sequence number generated from the target BS
Key Lifetime	AK sequence number generated from the target BS
BS_Noncea	A 64bit freshly-generated number from the Target BS
MS_Nonce	MS_Nonce included in the PKMv2 Pre-Authentication Request message
OMAC Tuple	Message Digest calculated using OMAC_KEY_D

Privacy Capabilities Parameters attribute indicates privacy capabilities negotiated with the target BS. The Authorization Policy Support and the Message Authentication Code Mode sub-attributes shall be included in this Privacy Capabilities Parameters attribute for this message.

Key Sequence Number and Key Lifetime are an AK sequence number and AK lifetime generated from the target BS.

BS_Nonce is a freshly-generated number from the target BS. This attribute is used to derive a new AK that is valid with the Target BS.

MS_Nonce is one which was included in the PKMv2 Pre-Authentication Request message

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

Inclusion of the keyed digest allows the receiving MS to authenticate the ~~Pre-Auth Request~~ PKMv2 Pre-Authentication-Reply message. The used OMAC_KEY_U is shared one between the MS and the serving BS.

Target BSID, Privacy Capabilities Parameters, Key Sequence Number, Key lifetime, and BS_Nonce shall appear as many as the number of target BSIDs. But, MS_Nonce and OMAC Tuple shall appear only one time irrespective of the number of target BSIDs in this message.

~~6.3.2.3.9.18 Pre-Authentication Reject message~~
6.3.2.3.9.30 PKMv2 Pre-Authentication Reject message

Sent by the BS to a client MS, receipt of a ~~Pre-Auth Reject~~ PKMv2 Pre-Authentication Reject message indicates to the receiving MS, that the BS identified by the BSID in the associated ~~Pre-Auth Request~~ PKMv2 Pre-Authentication Request message and repeated in the response, is not populated with a valid PAK or/and a valid PMK.

Code: : ~~20~~ 32

Attributes are shown in Table ~~37h~~ 37t.

Table 37h 37t– ~~PKM Pre-Auth-Reject~~ PKMv2 Pre-Authentication-Reject attribute

Attribute	Contents
(one or more) Target BSID(s)	The BSID that an MSS will connect after HO
Error-Code	Error code identifying the reason for rejection of pre-authentication request
Display-String (optional)	Display string providing the reason for rejection of pre-authentication request
BS_Nonce	Freshly generated number from the Target BS
MS_Nonce	MS_Nonce included in the PKMv2 Pre-Authentication Request message
OMAC Tuple	Message Digest calculated using OMAC_KEY_D

MS_Nonce is one which was included in the PKMv2 Pre-Authentication Request message

BS_Nonce is freshly generated number from the target BS. This attribute is used to derive new AK that is valid with the Target BS.

The OMAC/HMAC 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~~ PKMv2 Pre-Authentication Reject message. The used OMAC_KEY_U is shared between the MS and the serving BS.

Target BSID, Error-Code, and BS_Nonce shall appear as many as the number of target BSIDs. But, MS_Nonce, and OMAC Tuple shall appear only one time irrespective of the number of target BSIDs in this message.