| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **Pre Authentication for PKMv2** |
| Date Submitted | **2004-6-21** |


| | | |
|---|---|---|
| Source(s) | David Johnston<br>Intel Corporation<br>2111 NE 25th Ave.<br>Hillsboro 97124 | Voice: +1 (503) 264-3855<br>[mailto:dj.johnston@intel.com] |


| | |
|---|---|
| Re: | IEEE 802.16e Security Adhoc |
| Abstract | A Key Derivation based Pre-Authentication scheme for PKMv2 |
| Purpose | To create an authorization procedure in PKMv2, similar in style to PKMv2, but secure. |
| 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>. |

# Pre Authentication for PKMv2

*David Johnston (Intel)*
*Jesse Walker (Intel)*
*JunHyuk Song (Samsung)*

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 identities of the BS and SS.

Thus the SS is able to compute the PMK for any base station, since it is based on the MK it possesses, its own identity (MAC address in this case) and the publicly known identity of any target BS it may hand over to.

This foreknowledge of the PMK enables a fast handover in which normal key exchanges are not necessary.

The airside messaging to support this requires a handshake to enable and SS to determine when it may make a pre-authenticated handover, in place of the full, secure network entry procedure. This 2 message PKM-PREAUTH-REQ/RSP exchange is made prior to the HO-Ind message is sent by the SS.

The key derivation for the PMK is described in the Key Hierarchy proposal, C802.16e-04/188.

*Editor Instructions:*
*[Insert into clause 7 in the appropriate PKMv2 subsection, 7.x.x.x Pre-AuthenticationChange.]*

**7.x.x.x Pre-Authentication**

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

A BS on receipt 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. A PKM-PREAUTH-REJECT indicates that the chosen BS is not 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.

*[In the section where PKM messages are defined 6.3.2.3.9.x probably, insert.]*

**6.3.2.3.9.x Pre Auth Request (PKM-PREAUTH-RSP) Message**

Receipt of a Pre Auth Request message indicates to the receiving BS, that the sending SS is seeking to perform a pre-authenticated handover. The BS may response with a Pre Auth Response message if the target BS has been populated with a PMK tied to the target BS's BSID and requesting SS's SSID.

*Code:* x

Attributes are shown in Table xx.

| Attribute | Contents |
|---|---|
| Target BSID | BSID |
| Requesting SSID | SSID |
| Digest | HMAC or OMAC Digest |

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

Inclusion of the keyed digest allows the receiving BS to authenticate the Pre Auth Request message.

**6.3.2.3.9.x+1 Pre Auth Response (PKM-PREAUTH-RSP Message)**

Receipt of a Pre Auth Response 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 populated with a valid PMK.

*Code:* x

Attributes are shown in Table xx.

| Attribute | Contents |
|---|---|
| Target BSID | BSID |
| Requesting SSID | SSID |
| Digest | HMAC or OMAC Digest |

The Digest 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 Response message.

**6.3.2.3.9.x+1 Pre Auth Reject (PKM-PREAUTH-REJECT Message)**

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:* x

Attributes are shown in Table xx.

| Attribute | Contents |
|---|---|
| Target BSID | BSID |
| Requesting SSID | SSID |
| Digest | HMAC or OMAC Digest |

The Digest 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 Reject message.