Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Enhancement of Pre-authentication of PKMv2**
Date Submitted	**2005-01-24**
Source(s)	Chulsik Yoon, Mi-young Yun, and Sungcheol Chang csyoon@etri.re.kr ETRI 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea
Re:	Contribution on comments to IEEE P802.16e/D5
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 Pre-authentication for PKMv2

Chulsik Yoon, Mi-young Yun, and Sungcheol Chang

ETRI

1. Problem Statement

There are some problems in pre-authentication concept in the draft specification P802.16e/D5a.

1) There are various types of authorization modes in PKMv2, such as RSA with EAP, RSA-only mode, EAP-only mode, etc. Current pre-authentication mechanism for PKMv2 in P802.16e/D5a is only applicable to the EAP-only authorization mode. 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 MSS 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. It can be achieved by entending the keys sharing between the BSs for the hierarchical level of PMK and PAK with no BS dependency. And, in each BS and handover MSS pair, they can generate the different and unique set of BS-SS pairwise AKs using the BSID and SSID as input parameters for generating AK.

2) In 6.3.2.3.9.16 Pre-Auth-Request message and 6.3.2.3.9.17 Pre-Auth-Reply message, and 6.3.2.3.9.18 Pre-Auth-Reject message, the message authentication mode supported is only for OMAC Tuple. But, the HMAC tuple can be used as in the case of authorization policy is negotiated in the SBC-REQ/SBC-RSP step to use the HMAC tuple than OMAC tuple. Therefore, it should be enhanced to support both of them.

3) In PKMv2 Key Hierarchy, (*adopted in session #34 but not reflected in the draft specification*) requires that the AAID is considered as a highest level of hierarchy in key hierarchy mechanism in PKMv2. But, currently in the pre-authentication mechanism in the draft specification, there is no means to exchange the AAID between the MSS and the target BS. ~~Therefore, it should be enhanced to include the AAID parameters in Pre-Auth-Request/Pre-Auth-Reply messages.~~ Therefore, the PKMv2 key hierarchy can be modified to delete the Aithorization Assoication ID and replace it with the AK context concept to harmonize with the contribution C802.16e-05/024r1.

2. Summary of Solution

In PKMv2 (*PKMv2 Key Hierarchy is adopted in session #34, but not fully reflected in the draft specification P802.16e/D5a. Therefore, in this contribution, we described the concept based on the adopted contributions C802.16e-04/217r1 and C802.16e-04/564*), according to the negotiated authorization policy four cases of AK derivation is possible:

If (the authorization exchange has been used yielding a PAK and the EAP authentication exchange has been used, yielding an MSK) then

AK = Dot16KDF(PMK, SSID || BSID || AAID|| KDK || PAK || “AK”, 160);

Else If (the authorization exchange has been used yielding PAK and the EAP authentication exchange has been used, but not yielding an MSK) then

AK = Dot16KDF(0, SSID|| BSID|| AAID|| KDK| PAK|| “AK”, 160);

Else if (the EAP authentication exchange has been used, yielding an MK) then

AK = Dot16KDF(PMK, SSID || BSID || “AK”, 160);

Else if (the authorization exchange has been used) then

AK = Dot16KDF(0, SSID|| BSID|| AAID|| KDK|| PAK|| “AK”, 160);

Else

No security mode is selected

End if

In Figure 1, the general PKMv2 key hierarchy concept is described.

Currently, the Pre-authentication is applied to the PMK, not PAK. In Figure 1, only the right branch of the key hierarchy tree can be applied the pre-authentication for fast handover. But for most of the cases including the left branch of the key hierarchy tree (the RSA only case, RSA with EAP yielding an MK case, and the RSA with EAP not yielding an MK case), the pre-authentication cannot be applied.

If the serving BS and the target BS pair can support the pre-authentication, then the pre-authentication concept is supported by small changes on the current specification.

The PAK is a cryptographically strong randomly generated number at BS (but not having the BS-dependency such as BSID) and the MSK is the master session key shared between the MSS and the AAA server, and the PMK is the leftmost 160 bits of MSK (There is no BS-dependency). Current mechanism of the pre-authentication provide the target BS with the same PMK and the SSID, so the target BS and the handover MSS can generated the same AK using the shared PMK, BSID, and SSID (SS’s MAC Address):

PMK = leftmost 160 bits of the MSK (Master Session Key)

AK = Dot16KDF(PMK|| SSID|| BSID|| “AK”, 160)

Then the MSS and the target BS can generate all the required keys for security support without re-authentication procedures during handover.

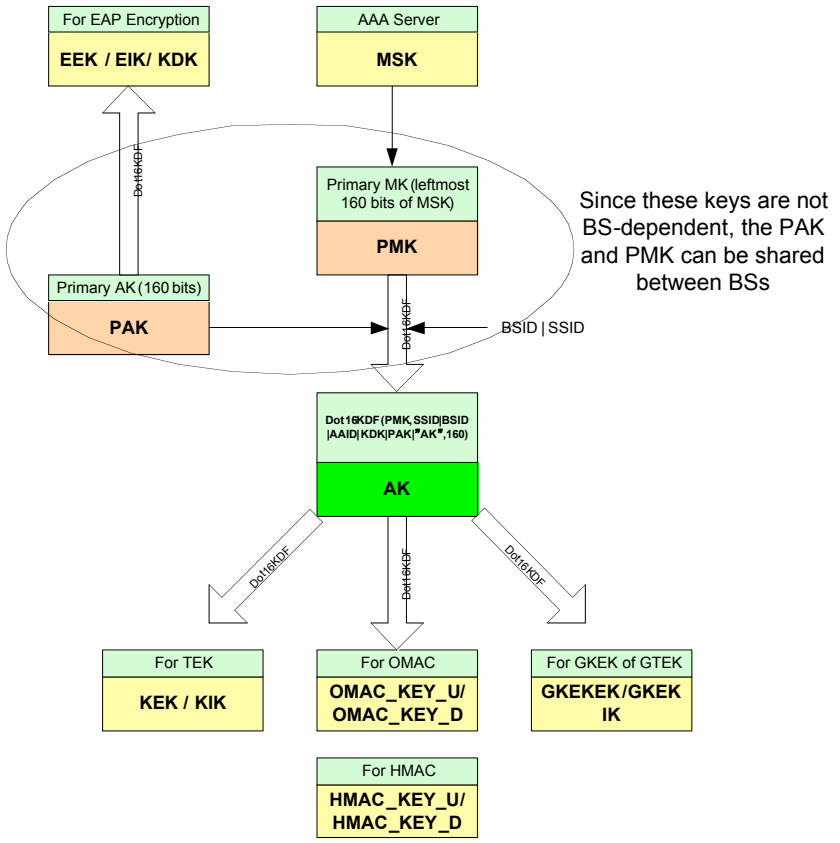

Figure 1. Description of the PKMv2 Key Hierarchy

To enhance this mechanism to every case of the authentication mode, the MSS and the target BS shall share not only the PMK, but also the PAK. During the HO procedure the serving BS transfer the MSS's capability information to the target BS, and then the target BS know the authorization capability of the MSS. Therefore, the MSS and the target BS can generate the same AK using the same AK generating rule for the initial network entry procedure, without PKM message transaction between them over the air.

The PAK and the PMK sharing method between them is out-of-scope of the specification. There can be two possible methods: 1) Transfer the PMK and the PAK from the old serving BS to the target BS. 2) ASA server (including the AAA server conceptually) ~~distribute~~ only keeping the keys of PMK and PAK, and the BS-specific keys, i.e., the AK can be generated using the BSID and SSID as an input parameters for generating the AK and distribute to the target BS~~the same MK and PMK to the target BS~~.

~~If the~~The ~~target BS get the PMK and the PAK, then the MSS and the target BS can derive the same~~can get the AK ~~between them using the PMK, PAK, and SSID, BSID, AAID, and KDK by the following step~~by generating and distributing the AK using the PMK, PAK, SSID and BSID:

Derive the AK using the AK generating rule:

If (the authorization exchange has been used yielding a PAK and the EAP authentication exchange has been used, yielding an MSK) then

AK = Dot16KDF(PMK, SSID || BSID || ~~AAID || KDK||~~PAK || "AK", 160);
Else If (the authorization exchange has been used yielding PAK and the EAP authentication exchange has been used, but not yielding an MSK) then
AK = Dot16KDF(0, SSID || BSID || ~~AAID ||KDK||~~PAK || "AK", 160);
Else if (the EAP authentication exchange has been used, yielding an MSK) then
AK = Dot16KDF(PMK, SSID || BSID || "AK", 160);
Else if (the authorization exchange has been used) then
AK = Dot16KDF(0, SSID || BSID || ~~AAID || KDK||~~PAK || "AK", 160);
Else
No security mode is selected
End if

Therefore, we can apply the pre-authentication in any case of the authorization mode negotiated.

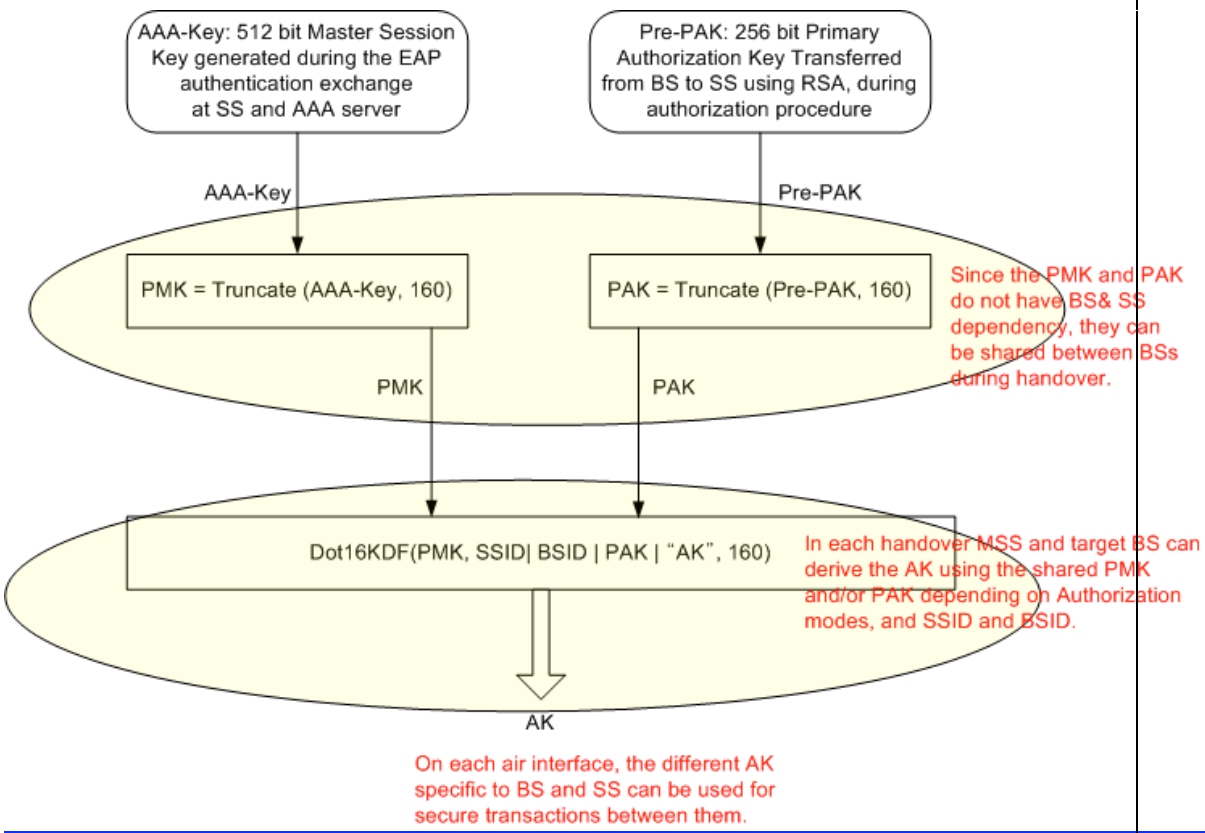

Figure 2. Description of proposed modification of key hierarchy and preauthentication concept

3. Proposed Text Changes

[In P802.16e/D5, Modify the Section 7.7 as follows:]

7.7 Pre-authentication

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

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

A BS may send an unsolicited PKM_PREAUTH-RSP message.

A PKM-PREAUTH-RSP indicates that the chosen BS is populated with a PMK coupled to the identity of the requesting MSS and the PAK transferred from the serving BS or from the ASA server.

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

[In P802.16e/D5, Modify the Section 6.3.2.9.16 as follows:]

6.3.2.3.9.16 Pre-authentication Request message

The message is sent by MSS to BS to establish ~~Pairwise~~ Primary Master Key (PMK) with Target BS for Handoff.

Code: 18

Attributes are shown in Table 37f.

Table 37f – PKM Pre-Auth-Request attribute

Attribute	Contents
Target BSID	The BSID that an MSS will connect after HO
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMAC_KEY

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

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.

[In P802.16e/D5, Modify the Section 6.3.2.9.17 as follows:]

6.3.2.3.9.17 Pre-Authentication Reply message

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

Code: 19

Attributes are shown in Table 37g.

Table 37g– PKM Pre-Auth-Reply attribute

Attribute	Contents
Target BSID	The BSID that an MSS will connect after HO
Authorization Mode	Authorization mode negotiated between the target BS and the MSS.
~~AA Descriptor~~	~~Specifies AAID and its type~~
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMAC_KEY

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.

6.3.2.3.9.18 Pre-Authentication Reject message

Sent by the BS to a client MSS, receipt of a Pre-Auth Reject message indicates to the receiving MSS, 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 and/or a valid PAK.

Code: 20

Attributes are shown in Table 37h.

Table 37h – PKM Pre-Auth-Reject attribute

Attribute	Contents
Target BSID	The BSID that an MSS will connect after HO
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMAC_KEY

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.