Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Enhancement of Pre-authentication of PKMv2**
Date Submitted	**2004-11-15**
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	
Release	
Patent Policy and Procedures	

Enhancement of Pre-authentication for PKMv2

Chulsik Yoon, Mi-young Yun, and SungCheol Chang

ETRI

1. Introduction

Current pre-authentication mechanism for PKMv2 in P802.16e/D5 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."

PKMv2 Key Hierarchy text is not in the current specification, but the general concept of that is known to all of us as a DJ's contribution C802.16e-04/188r2. In PKMv2, 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 ~~MK~~MSK) then

AK = Dot16KDF(PMK, SSID || BSID || ~~AKID~~ AAID|| KDK || PAK || "AK", 160);

ElsIf (the authorization exchange has been used yielding PAK and the EAP authentication exchange has been used, but not yielding an ~~MK~~MSK) then

AK ~~<= PAK~~ = Dot16KDF(0, SSID || BSID || AAID || KDK|| PAK || "AK", 160);

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

~~AK <= PMK~~

AK = Dot16KDF(PMK, SSID || BSID || ~~AKID ||~~ "AK", 160);

Elsif (the authorization exchange has been used) then

AK ~~<= PAK~~= Dot16KDF(0, SSID || BSID || AAID || KDK|| PAK || "AK", 160);

Else

No security mode is selected

End if

In Figure 1, I have shown the general PKMv2 key hierarchy concept.

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 MK is the truncated key of AAA-key generated in the AAA and the SS (so there is no BS-dependency). Current mechanism of the pre-authentication provide the target BS with the same MK and the SSID, so the target BS and the handover MSS can generated the same PMK by using the MK, BSID, and SSID (SS's MAC Address), and then the AK:

PMK = Dot16KDF(MK, BSID|SSID, 160)
AK <= PMK

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

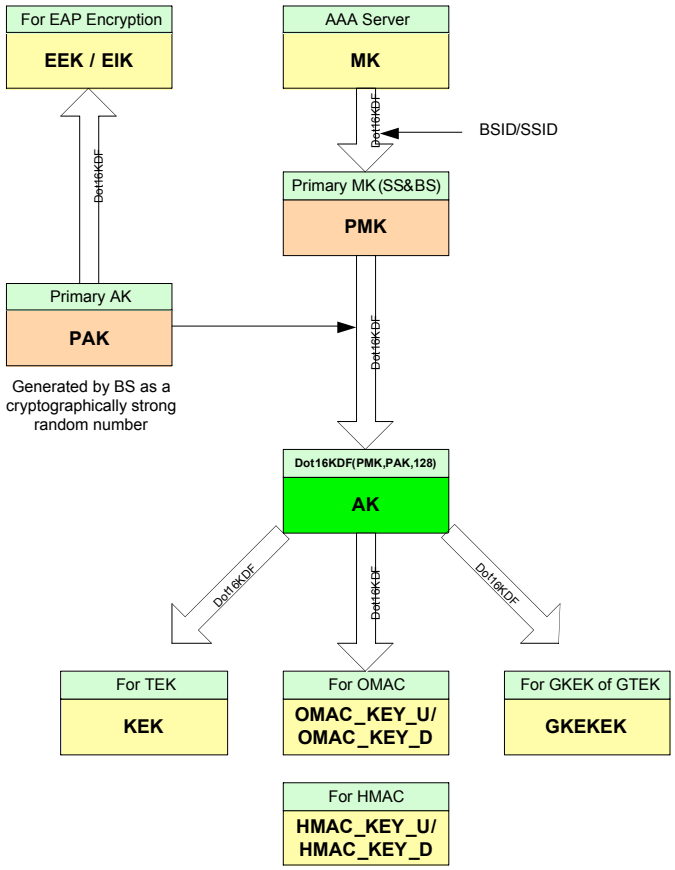

Figure 1. Description of the PKMv2 Key Hierarchy

To enhance this mechanism to every case of the authentication mode, the MSS and the target BS shall share not only the MK, 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.

Following the new version of the PKMv2 Key Hierarchy text (C802.16e-04/217r1) submitted on session #34, proposed Pre-authentication text should be changed appropriately. It is shown in Figure 2.:

MK should be changed to PMK, and the PMK is not BS-dependent.

AK is generated by the following rule.

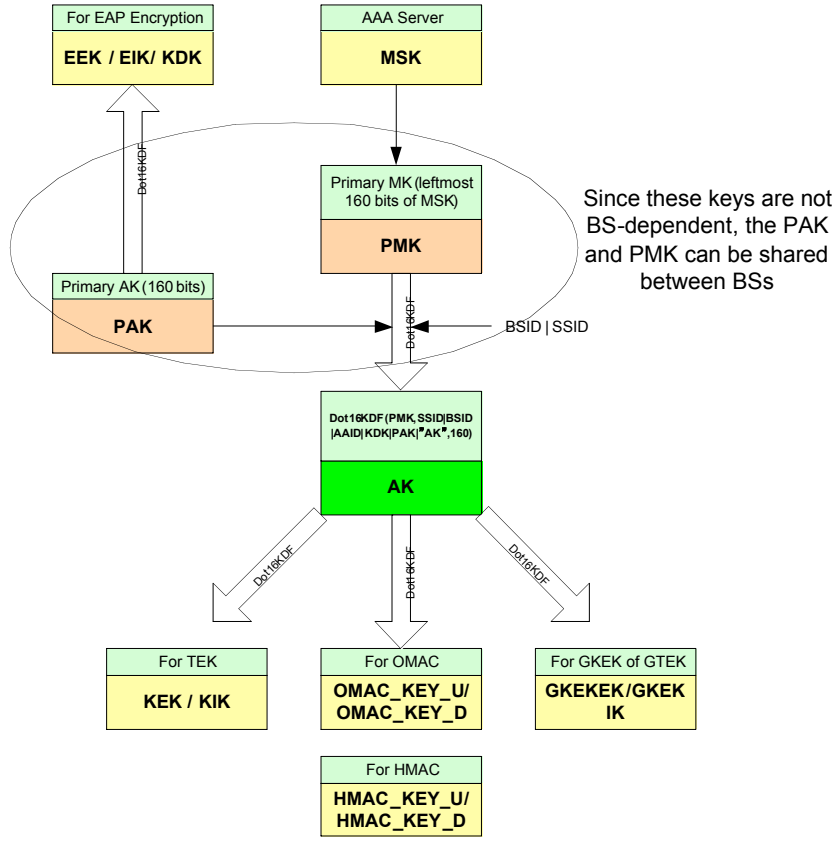

Figure 2. Description of the PKMv2 Key Hierarchy (Following the new version of Key Hierarchy text submitted in Session #34; C802.16e-04/217r1)

The PAK and the ~~MK~~ PMK sharing method between them is out-of-scope of the specification. There can be two possible methods: 1) Transfer the ~~MK~~ PMK and the PAK from the old serving BS to the target BS. 2) ASA server (including the AAA server conceptually) distribute the same MK and PMK to the target BS.

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

~~1) Generate the PMK using the MK, SSID, and BSID:~~
~~PMK = Dot16KDF(MK, BSID|SSID, 160)~~

~~2)~~ 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);

ElsIf (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);
Elsif (the EAP authentication exchange has been used, yielding an MK) then
AK = Dot16KDF(PMK, SSID || BSID || “AK”, 160);
Elsif (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
~~If (the authorization exchange has been used yielding a PAK and the EAP authentication exchange has been used, yielding an MK) then~~
~~AK <= Dot16KDF(PMK, PAK, 160);~~
~~ElsIf (the authorization exchange has been used yielding PAK and the EAP authentication exchange has been used, but not yielding an MK) then~~
~~AK <= PAK~~
~~Elsif (the EAP authentication exchange has been used, yielding an MK) then~~
~~AK <= PMK~~
~~Elsif (the authorization exchange has been used) then~~
~~AK <= PAK~~
~~No security mode is selected~~
~~End if~~

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

2. 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 recipt 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 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.