Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Remedy of EAP in EAP mode
Date Submitted	**2005-07-14**
Source(s)	Junhyuk Song junhyuk.song@samsung.com Jicheol Lee jicheol.lee@samsung.com Samsung Electronics
Re:	IEEE P802.16e/D9
Abstract	Remedy of EAP-in-EAP mode Authentication
Purpose	Adopt this contribution as a remedy of EAP-in-EAP mode
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>.

Remedy of EAP-in-EAP mode

Junhyuk Song (junhyuk.song@samsung.com)
Jicheol Lee (Jicheol.lee@samsung.com)
Samsung Electronics

1. Motivation

According to IETF's security review, there was a comment and a suggestion on the "Authenticated EAP" mode.

> 3. "Authenticated EAP" mode
>
> [RFC3748] Section 2.1 states:
>
> " An EAP conversation MAY utilize a sequence of methods. A common example of this is an Identity request followed by a single EAP authentication method such as an MD5-Challenge. However, the peer and authenticator MUST utilize only one authentication method (Type 4 or greater) within an EAP conversation, after which the authenticator MUST send a Success or Failure packet."
>
> The prohibition on sequences of EAP methods was added to avoid a potential man-in-the-middle vulnerability described in [KEYFRAME] Section 6.4:
>
> " As described in [I-D.puthenkulam-eap-binding], EAP method sequences and compound authentication mechanisms may be subject to man-in-the-middle attacks. When such attacks are successfully carried out, the attacker acts as an intermediary between a victim and a legitimate authenticator. This allows the attacker to authenticate successfully to the authenticator, as well as to obtain access to the network."
>
> By enabling use of a sequence of EAP conversations without support for cryptographic binding, "Authenticated EAP" mode creates a vulnerability to man-in-the-middle attack.
>
> IEEE 802.16e D8 Section 7.2.2.2.2 states:
>
> "Note that this EAP authentication method shall not derive key material and PMK"
>
> We assume this implies that the PMK generated by the second EAP authentication is not utilized, rather than a prohibition on EAP methods that derive keys.
>
> However, not requiring the BS to demonstrate possession of PMKs from all EAP authentications enables the man-in-the-middle attack, described in [BINDING]. This is a critical vulnerability, and
>
> we strongly suggest that IEEE 802.16e address it prior to publication.
>
> **One potential way to achieve this is for cryptographic binding to be utilized so that the BS can demonstrate possession of all of the PMKs.**

<From the review.txt of IETF>

IETF suggested remedy for EAP in EAP mode in 802.16e.

2. Proposed solution

According to the review, “it is suggested that cryptographic binding to be utilized so that the BS can demonstrate possession of all of the PMKs”.

Although there was a suggested remedy, the BRC security subteam just removed the “EAP-in-EAP mode” instead of doing suggested remedy.

So, we propose the suggested remedy for this.

After MS and BS performs EAP in EAP mode according to authorization policy,

1) First EAP method generates PMK between MS and BS
2) Second EAP method generates PMK2 between MS and BS.

We shall have to generate AK
AK <= Dot16KDF(PMK   PMK2, BSID|MSID|”AK”,160);

Finally the “middle-man” can be detected by SA-TEK 3 way handshake through sign by H/OMAC key derived from AK which is generated from PMK and PMK2.

3. Proposed Text Changes

[Insert highlighted text and remove red texts in section 7.2.2.2.2 in page 212 of 802.16e/D9]

7.2.2.2.2 EAP authentication

If a RSA mutual authorization took place before the EAP exchange or if the first EAP took place during EAP-in-EAP mode, the EAP messages may be protected using EIK - EAP Integrity Key derived from pre-PAK (see 7.2.2.2.1) or MSK. EIK is 128 bits long.

The product of the EAP exchange which is transferred to 802.16 layer is the MSK. This key is derived (or may be equivalent to the 512-bits Master Session Key (MSK)). This key is known to the AAA server, to the Authenticator* (transferred from AAA server) and to the MS. The MS and the authenticator derive a PMK (Pairwise Master Key) and optional EIK by truncating the MSK to 288 bits.
The PMK derivation from the MSK is as follows:

~~PMK = truncate (MSK, 160)~~
~~If more keying material is needed for future link ciphers, the key length of the PMK may be increased.~~

The PMK and EIK derivation from the MSK during first EAP method is as follows:
EIK | PMK = truncate (MSK, 288)

The PMK2 derivation from the MSK2 during second EAP method is as follow:
PMK2 := truncate(MSK2, 160)

If more keying material is needed for future link ciphers, the key length of the PMK may be increased.

After successful EAP based authorization, if the MS or BS negotiates authorization policy as “Authenticated EAP after

EAP" mode, the authenticated EAP messages shall carry second EAP message. It shall cryptographically bind previous EAP authentication and following EAP authentication session, while protecting second EAP messages. In order to prevent "man-in-the-middle attack", the second EAP method should fulfill the "mandatory criteria" listed in section 2.2 of RFC 4017

[Insert highlighted lines at sub-clauses 7.2.2.2.3 in line 15 to 35 of page 213 in 802.16e/D9 as follows]

```
If (PAK and PMK)
        AK <= Dot16KDF (PAK    PMK, SSID | BSID | "AK", 160)
Else If (PMK and PMK2)
        AK <= Dot16KDF (PMK    PMK2, SSID | BSID | "AK", 160)
Else
    If (PAK)
            AK <= Dot16KDF (PAK, SSID | BSID | "AK", 160)
    Else
            AK <= Dot16KDF (PMK, SSID | BSID | "AK", 160)
    Endif
Endif
```

[Add following figure and text just after figure 133 in page 216 of 802.16e/D9]

Figure 133a outlines the process to calculate the AK when EAP in EAP mode authentication exchange has taken place, first EAP yielding EIK and MSK and second EAP yielding MSK2.

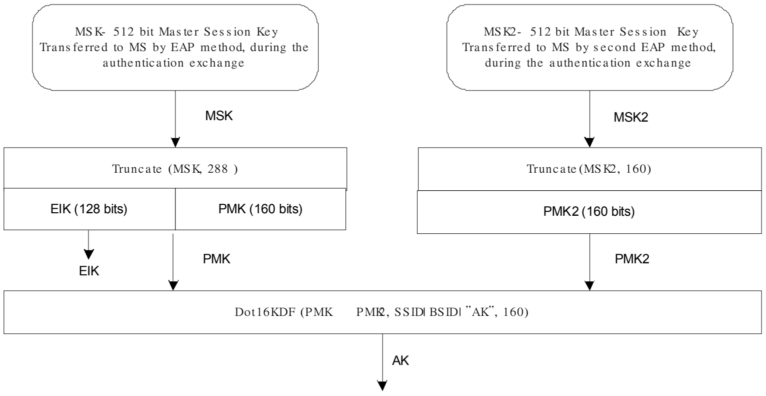
MSK- 512 bit Master Session Key Transferred to MS by EAP method, during the authentication exchange
MSK2- 512 bit Master Session Key Transferred to MS by second EAP method, during the authentication exchange
MSK
MSK2
Truncate (MSK, 288)
Truncate (MSK2, 160)
EIK (128 bits)
PMK (160 bits)
PMK2 (160 bits)
EIK
PMK
PMK2
Dot16KDF (PMK PMK2, SSID| BSID| "AK", 160)
AK

Figure 133a- AK with PMK and PMK2
(EAP-based authorization and Authenticated EAP-based authorization)

[Change the row and insert new rows of table 133 in page 200]

PMK	160	A key yield from the EAP-based authentication
PMK2	160	A key yield from the second EAP authentication in case of au EAP after EAP.
PMK/PMK2 lifetime ~~lifetime~~		The lifetime of PMK derived from EAP PMK lifetime, when authorization is achieved and the MSK is obtained. The value of PMK lifetime may be transferred from the EAP method or may be set by a vendor. If MSK has infinite lifetime, PMK lifetime should be set to default PMK lifetim In case of authenticated EAP after EAP, PMK/PMK2 lifetime is MIN(PMK,PM If both PMK and PMK2 have infinite value, PMK/PMK2 lifetime is set to defau
AK lifetime	160	This is the time this key is valid; it is calculated AK lifetime = MIN(PAK lifetime, PMK lifetime) - when this expires, re-aut is needed. AK lifetime = MIN(PMK lifetime, PMK2 lifetime) in case of EAP after EAP

[Please insert the following sentence just after section 6.3.2.9.17 in page 50]
~~and insert new rows of table 133 in page 200]~~
PAK Sequence Number appears only if Authorization Policy is "Authenticated EAP after RSA authentication." If authorization policy is "authenticated EAP after EAP", PAK sequence number is not included in this message.

[Please change the section 6.3.2.3.9.15 in page 49]

6.3.2.3.9.15 PKMv2 EAP Start message

When an MS seeks to initiate an EAP-based authentication or reauthentication procedure with a BS, it sends a PKMv2 EAP Start message.

Code: 17

This message has no attributes when it is used during initial authentication.
When this message is used to initiate the second EAP in case of authenticated EAP after EAP, this message is singed by EIK generated from the first EAP.

Table 37da PKMv2 EAP Start message

Attribute	Contents
MS_Random	Random number generated by MS
CMAC Digest	CMAC Digest using EIK

[Please insert the following row into the table 343, section 10.2 in page 503]

BS	EAP_Start_Timeout	Time in seconds to wait for PKMv2_EAP_Start after the success of the first EAP in EAP-in-EAP mode	1	3	3