| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | Remedy of double EAP mode |
| Date Submitted | **2005-07-21** |
| Source(s) | Junhyuk Song, Jicheol Lee, Alper Yegin<br>Samsung Electronics<br>junhyuk.song@samsung.com<br>jicheol.lee@samsung.com<br>alper.yegin@samsung.com<br><br>Yoshihiro Ohba<br>Toshiba<br>yohba@tari.toshiba.com |
| Re: | IEEE P802.16e/D9 |
| Abstract | Remedy of double EAP mode Authentication<br><br>Double EAP mechanism is proposed in order to use an EAP method instead of RSA for device authentication. EAP framework enables use of various EAP methods and device credentials (including pre-shared secret based ones), instead of always using X.509/RSA. |
| Purpose | Adopt this contribution as a remedy of double 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, Jicheol Lee, Alper Yegin (Samsung Electronics)
Yoshihiro Ohba(Toshiba)

## 1. Main Motivation of Proposing double EAP mode

**Double EAP mechanism is proposed in order to use an EAP method instead of RSA for device authentication. EAP framework enables use of various EAP methods and device credentials (including pre-shared secret based ones), instead of always using X.509/RSA.**

# 2. IETF Review

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.

~~**"Main Motivation of Proposing double EAP"**~~

~~**Double EAP mechanism is proposed in order to use an EAP method instead of RSA for device authentication. EAP framework enables use of various EAP methods and device credentials (including preshared secret based ones), instead of always using X.509/RSA.**~~

# 3. 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.

1) ~~1)~~ AK Key Derivation

After MS and BS performs EAP in EAP mode according to authorization policy,
- First EAP method generates PMK between MS and BS
- Second EAP method generates PMK2 between MS and BS.( In case of re-authentication, this 2nd EAP can be skipped).

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.

2) Satisfy~~ing Satisfy~~ RFC4017 for second EAP
3) Describe how double EAP works.
Please see "proposed text change of 7.2.2.2.2 section"
4) Enable HMAC to use EIK (160bits)
EIK(128bits) → EIK(160bits)
5) Creates two new message to distinguish 1nd round EAP and 2nd round EAP
a. PKMv2 EAP Complete (to transfer 1nd EAP _Success/Failure in order to inform MS of completion of 1nd EAP. This message is used in initial authentication and reauthentication)
b. PKMv2 Authenticated EAP Start ( to initiated 2nd round EAP by signing EIK)
(This message are used only for initial authentication for double EAP)
6) In case of reauthentication, 2nd round EAP can be skipped by sending PKMv2 EAP Transfer message rather than sending PKMv2 EAP Complete according to decision of BS.
7) When using double EAP, 1st EAP may be used for device authentication, and the 2nd EAP for user authentication. Any authentication method that satisfies RFC 4017 (including cert and psk- based methods, e.g., EAP-PSK, EAP-SIM, EAP-AKA, EAP-TLS, etc.) can be used for the device and user authentication.~~When using double EAP, 1st EAP can be EAP-PSK for device authentication and 2nd round EAP can be used for EAP-AKA for user authentication.~~
~~EAP method for 1st EAP and 2nd EAP should satisfy IETF EAP guideline.~~

# 4. Proposed Text Changes

***[Please modify text 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~~ 160bits 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:

The PMK and EIK derivation from the MSK during first EAP method is as follows:
EIK | PMK = truncate (MSK, 320)

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 first and second EAP method should fulfill the "mandatory criteria" listed in section 2.2 of RFC 4017 such as EAP-PSK, EAP-AKA.

If MS and BS negotiate double EAP mode (a.k.a. Authenticated EAP after EAP), MS and BS perform two rounds of EAP as follows:

1) In order to initiate 1st round EAP of double EAP, MS may send PKMv2 EAP Start message with no attribute.
2) MS and BS shall perform 1st round EAP conversation with PKMv2 EAP Transfer message without HMAC/OMAC Digest.
3) During 1st EAP conversation, if BS has to send EAP-Success , BS shall send EAP payload to MS with PKMv2 EAP Complete message signed by newly generated EIK. BS shall resend the PKMv2 _EAP_Complete message by Second_EAP_Timeout. Total number of sending PKMv2_EAP_Complete message is EAP_Complete_Resend. After MS receives the PKMv2 EAP_Complete message which includes EAP-Success payload, MS can possess EIK and PMK. In this case, MS can validate the message. Otherwise, if MS receives EAP-Failure or can not validate the message, MS fails in authentication. After BS transfers the PKMv2 EAP Complete message to MS, BS activates the Second_EAP_Timeout in order to wait PKMv2 Authenticated EAP Start message. When the timer expires, BS shall regard the authentication as failure.
4) After the successful 1st round EAP, MS shall send PKMv2 EAP Start message signed by EIK to initiates 2nd round EAP conversation. If BS validates the PKMv2 EAP Start message by EIK, BS shall initiate 2nd EAP by sending PKMv2 Authenticated EAP message including EAP-Identity/Request to MS. If BS cannot validate the PKMv2 Authenticated EAP Start message, BS shall regard the authentication as failure.
5) MS and BS shall perform 2nd EAP conversation with PKMv2 Authenticated EAP message signed by EIK.
6) If 2nd round EAP succeeds, both MS and authenticator generate AK from PMK and PMK2. MS and BS shall perform SA-TEK 3way handshake.

After the successful initial authentication, MS and BS shall perform reauthentication by PMK/PMK2 lifetime. In performing reauthentication, MS and BS perform double EAP just like initial authentication. Otherwise, MS and BS can perform EAP once.

When MS and BS perform reauthentication with double EAP also, the following procedure shall be performed as follows:

1) In order to initiate reauthentication, MS may send PKMv2 EAP Start message signed by H/CMAC_KEY_U derived from AK.
2) MS and BS shall use PKMv2 EAP Transfer message to carry 1st round EAP conversation
3) BS shall carry EAP-Success ~~or EAP-Failure~~ message with PKMv2 EAP Complete message signed by AK generated from the previous double EAP.
4) After successful 1st round EAP, MS shall initiate 2nd round EAP by sending PKMv2 EAP Start message signed by H/CMAC_KEY_U generated from AK (previous double EAP generated this key).
5) MS and BS shall perform 2nd round EAP conversation with PKMv2 EAP Transfer message signed by AK which is generated by previous double EAP.
6) MS and BS shall perform SA-TEK 3way handshake.

When MS and BS perform reauthentication with double EAP, MS and BS can perform EAP once as follows:

1) In order to initiate reauthentication, MS may send PKMv2 EAP Start message signed by H/CMAC_KEY_U derive

d from AK.
2) MS and BS shall use PKMv2 EAP Transfer message to carry 1st round EAP conversation
3) BS shall carry EAP-Success or EAP-Failure message with PKMv2 EAP Transfer instead of sending PKMv2 EAP Complete signed by AK. It means that BS doesn't want to run 2nd round EAP.

***[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 right 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.

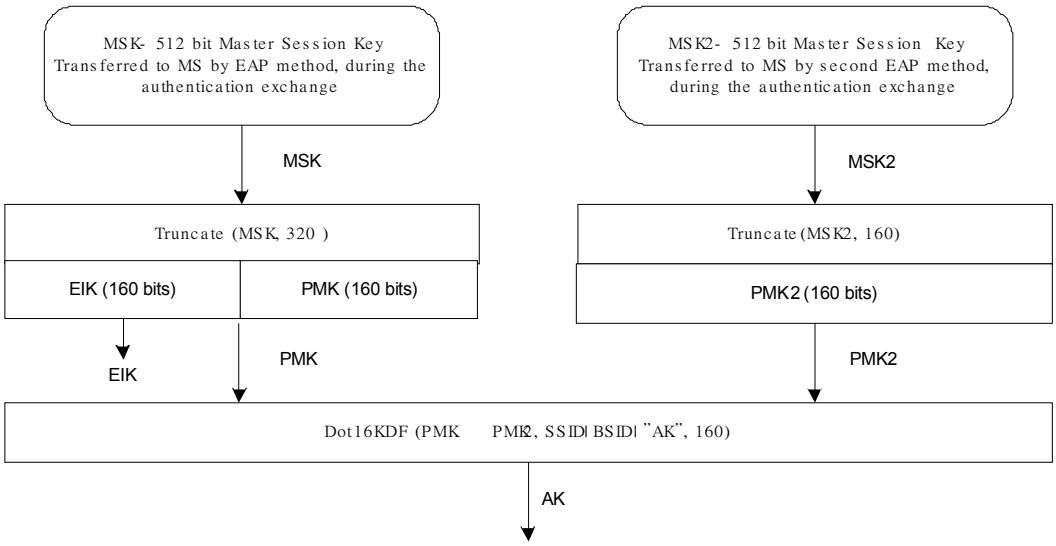


Figure 133a- AK with PMK and PMK2
(EAP-based authorization and Authenticated EAP-based authorization)

***[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 authenticated EAP after EAP. |
| PMK/PMK2 lifetime ~~lifetime~~ | | The lifetime of PMK derived from EAP PMK lifetime, when the EAP-based authorization is ac MSK is obtained.<br>The value of PMK lifetime may be transferred from the EAP method or may be set by a vendor.<br>If MSK has infinite lifetime, PMK lifetime should be set to default PMK lifetime.<br>In case of authenticated EAP after EAP, PMK/PMK2 lifetime is MIN(PMK,PMK2).<br>If both PMK and PMK2 have infinite value, PMK/PMK2 lifetime is set to default PMK lifetim |
| | | |
| 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-authentication is needed.<br>AK lifetime = MIN(PMK lifetime, PMK2 lifetime) in case of Authenticated EAP after EAP |
| EIK | 160 | EAP Integrity Key for authenticating Authenticated EAP message |

***[Please insert the red text into subsection 6.3.2.3.9.17 in page 50]***

#### 6.3.2.3.9.17 PKMv2 Authenticated EAP Transfer messages

This message can be used in case of negotiating Authenticated EAP-based authorization as authorization policy (by Authorization Policy Support included in the SBC-REQ/RSP message) between an MS and the BS. Moreover, if EIK is available and an MS or BS has an EAP payload received from an EAP protocol for transmission, it encapsulates EAP payload in a PKMv2 Authenticated EAP Transfer message.

Code: 19

Attributes are shown in Table 37f

**Table 37f PKMv2 Authenticated EAP message Attribute**

| Attribute | Contents |
|---|---|

| | |
|---|---|
| PAK Sequence Number | PAK Sequence Number (optional) |
| EAP Payload | Contains the EAP authentication data, not interpreted |
| HMAC/CMAC Digest | Message Digest calculated using EIK |

The EAP Payload field carries EAP data in the format described in RFC 3748
The CMAC-Digest's or HMAC-Digest's attribute shall be the final attribute in the message's attribute list.
Inclusion of the CMAC or HMAC-Digest allows the MS and BS to cryptographically bind previous authorization and following EAP authentication by authenticating the EAP payload. The CMAC-Digest's or HMAC Digest's authentication key is derived from the EIK

PAK Sequence Number attribute carries PAK sequence number only if MS and BS negotiate "Authenticated EAP after RSA" mode.

***~~[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]~~***

***[Please insert two following subsections just after section 6.3.2.9.27 in page 58]***

### 6.3.2.3.9.28 PKMv2 EAP Complete

In double EAP mode (EAP after EAP), BS sends the PKMv2 EAP Complete message to MS with EAP-Success ~~or EAP-Failure~~ to inform MS of completing 1st EAP conversation.
This message is used only if MS and BS negotiate EAP in EAP mode.
The Key Sequence Number and HMAC/CMAC Digest attributes of this message appear only in re-authentication.

**Table 37q PKMv2 EAP Complete Attribute**

| **Attribute** | **Contents** |
|---|---|
| EAP Payload | Contains the EAP authentication data, not interpreted in the MAC layer |
| Key Sequence Number | AK sequence number appear only if AK is available from previous double EAP |
| HMAC/CMAC Digest | Message Digest calculated using AK only if AK is available from previous double EAP<br>Message Digest calculated using EIK when initial authentication |

### 6.3.2.3.9.29 PKMv2 Authenticated EAP Start

In double EAP mode (EAP after EAP), MS sends the PKMv2 EAP Authenticated EAP Start message to BS in order to initiate 2nd round EAP . This message is signed by EIK which is generated by 1nd EAP.
This message is used only for initial authentication of double EAP.

**Table 37r PKMv2 Authenticated EAP Start Attribute**

| **Attribute** | **Contents** |
|---|---|
| MS_Random | Random number generated by MS. |
| HMAC/CMAC Digest | Message Digest calculated using EIK |

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

| | | | | | |
|---|---|---|---|---|---|
| BS | Second_EAP_Timeout | Time in seconds to wait for PKMv2_EAP_Start or PKMv2_Authenticated_EAP_Start after the success of the first EAP in double EAP mode | 0.3 | 1 | 1 |
| BS | EAP_Complete_Resend | Total number of sending PKMv2_EAP_Complete message in double EAP mode | 1 | 3 | 3 |

***[Please insert the following rows into the table 26, section 6.3.2.3.9 in page 46]***

| | | |
|---|---|---|
| 29 | PKMv2 EAP Complete | PKM-RSP |
| 30 | PKMv2 Authenticate EAP Start | PKM-REQ |