Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Enhancement of 802.16e to Support Secure EAP PKM messages**
Date Submitted	**2004-05-17**
Source(s)	JunHyuk Song Samsung Electronics Voice: +82-31-xxx-xxxx Fax: mailto: junhyuk.song@samsung.com
Re:	This is a response to a Call for Comments IEEE 802.16e-03/58 on IEEE 802.16e-03/07r5
Abstract	This document contains suggestions to provide protection to EAP PKM messages
Purpose	The document is submitted for review by 802.16e Working Group members.
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>.

Enhancement of 802.16e to Support of Secure EAP PKM messages

JunHyuk Song
Samsung Electronics

1 Scope of this document

This document outlines how to provide the protection to the Extensible Authentication Protocol PKM messages

2 Background

Due to the working group's agreement on the EAP-based Authentication support (See Figure 1), the protection toward to EAP PKM messages is required. As C802.16-71/r3 [1] and RFC2284bis [2, section 7.1] Internet Draft described, EAP has been known for security vulnerability, such as lack of user identity and EAP negotiation protection, and Man in the Middle Attack. Those problems are more often caused by use of legacy authentication method (ex. CHAP MD5), however those are very often preferred means for user authentication to the operators due to the availability of its legacy user credentials and authentication algorithm deployments. By enabling message authentication, integrity and encryption toward to PKM EAP messages over Primary Management Connection will fix the above problems (See Figure 2)
In this contribution we propose to add PKM message code 15 for Secure EAP messages (See Figure 3) that can encapsulate data in the format that described in RFC2284bis encrypted and authenticated in addition to PKM EAP Transfer message codes previously decided 13 and 14

13	EAP Transfer Request	PKM-REQ
14	EAP Transfer Reply	PKM-RSP
15 ~ 255	reserved	

Figure-1 Previously approved PKM EAP message types

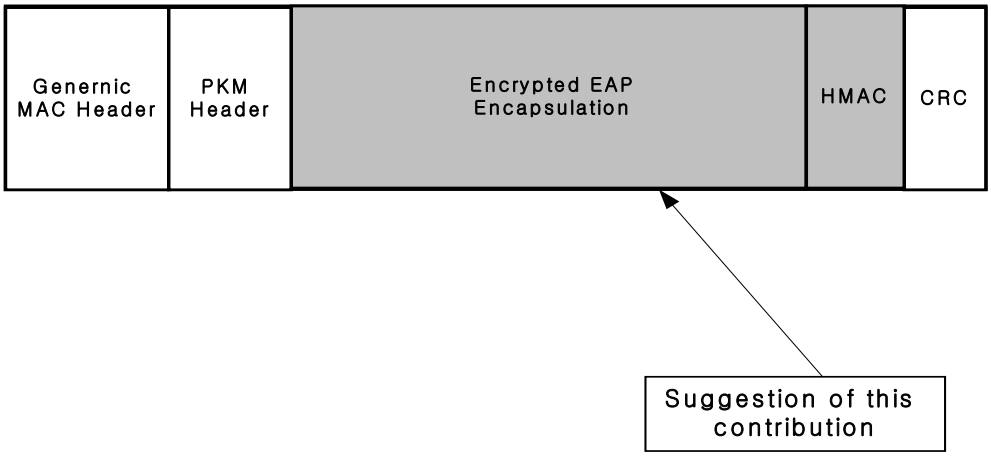


Figure-2 Proposed EAP PKM message encryption

15	Secure EAP Packet	PKM-REQ, PKM-RSP

Figure-3 Proposed EAP PKM message codes

3. Description of Protected EAP PKM messages

Figure-4 shows Control Plane of PKM message layer providing EAP Message Encryption, HMAC Generation, and Data Encryption

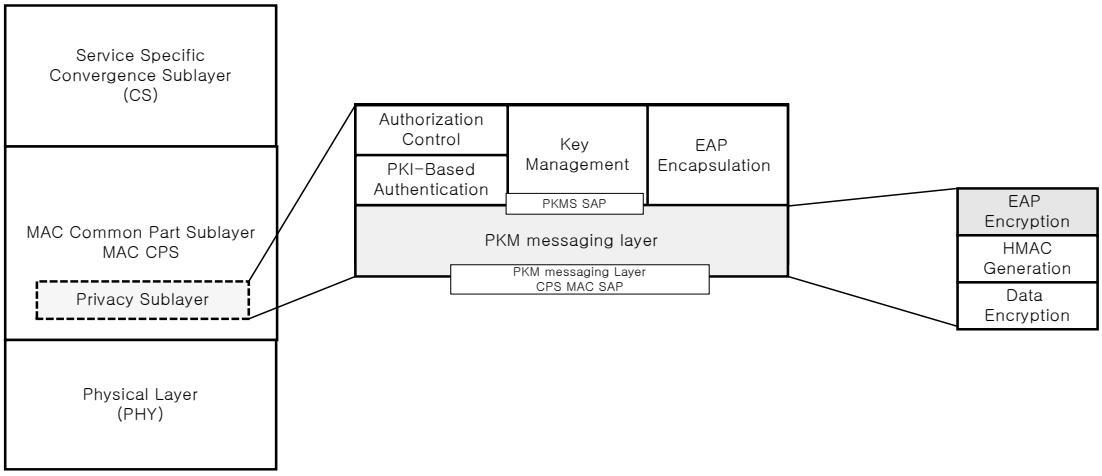


Figure 4 Control Plane

3.1 SEK (Secure EAP Key) based Secure EAP messages

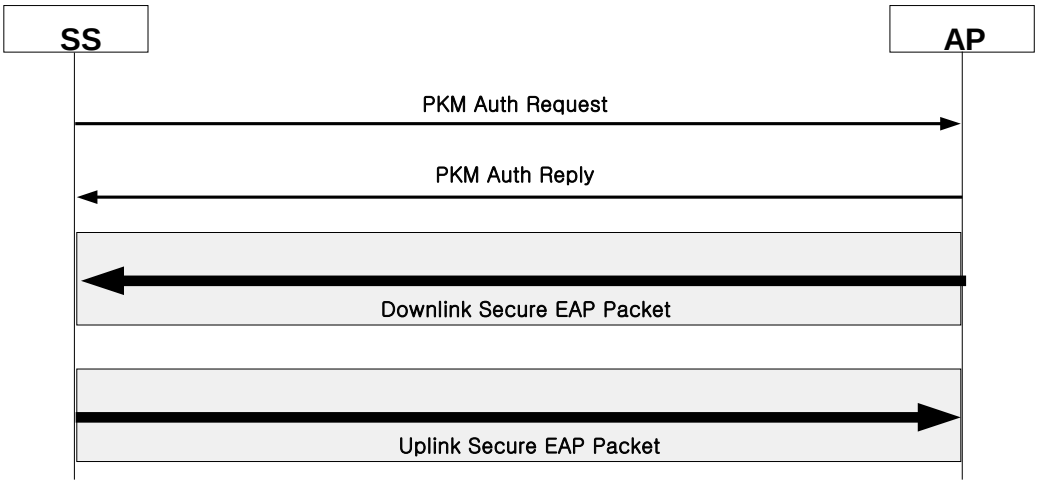
PKM EAP packet messages shall be encrypted by SEK derived from AK and authenticated by HMAC Key. In this way Primary Management Connection is not mapped to SA, however Message encryption will be performed to PKM EAP Packet messages based on SEK and authenticated by HMAC Key. (Note that Secure EAP support will be negotiated during SBC Capability negotiation by turning on both Legacy PKM authentication and PKM EAP based authentication support bits)

The SEK shall be derived as follows:

- SEK_D (128bits) = Truncate (SHA (S_PAD_D | AK), 128)
- SEK_U (128bits) = Truncate (SHA (S_PAD_U | AK), 128)

S_PAD_D = 0x3B repeated 64 times
S_PAD_U = 0x5D repeated 64 times

PKM EAP Transfer message shall be encrypted by AES ECB mode.
Encryption: C = Es1[P]
Decryption: P = Ds1[C]
S1= the 128bits SEK_D/SEK_U
E[ ] = 128-bits AES ECB mode encryption
D[ ] = 128-bits AES ECB mode decryption



Proposed Text Change

[Change/Delete the following as shown]

6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)

PKM employs two MAC message types: PKM Request (PKM-REQ) and PKM Response (PKM-RSP), as described in Table 24.

Table 24—**PKM MAC messages**

Type Value	Message name	Message description
9	PKM-REQ	Privacy Key Management Request [SS <-> BS]
10	PKM-RSP	Privacy Key Management Response [BS <-> SS]

These MAC management message types distinguish between PKM requests (SS–to–BS or BS-to-SS) and PKM responses (BS–to–SS or SS-to-BS). Each message encapsulates one PKM message in the Management Message Payload.

PKM request protocol messages transmitted from the SS to the BS shall use the form shown in Table 25. They are transmitted on the SSs Primary Management Connection.

PKM response protocol messages transmitted from the BS to the SS shall use the form shown in Table 26. They are transmitted on the SSs Primary Management Connection.

Table 25—PKM request (PKM-REQ) message format

Syntax	Size	Notes
PKM-REQ_Message_Format() {		
Management Message Type = 9	8 bits	
Code	8 bits	
PKM Identifier	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

Table 26—PKM response (PKM-RSP) message format

Syntax	Size	Notes
PKM-RSP_Message_Format() {		
Management Message Type = 10	8 bits	
Code	8 bits	
PKM Identifier	8 bits	
TLV Encoded Attributes	*variable*	TLV specific
}		

The parameters shall be as follows:

Code

The Code is one byte and identifies the type of PKM packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table 27.

PKM Identifier

The Identifier field is one byte. An SS and BS uses the identifier to match thea BS response to the SS's requests.

The SS and the BS shall increment (modulo 256) the Identifier field whenever it issues a new PKM message. A "new" message is an Authorization Request ,or Key Request, EAP Transfer Request, EAP Transfer Reply or Secure EAP packet that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Identifier field shall remain unchanged.

The Identifier field in Authentication Information messages, which are informative and do not effect any response messaging, shall be set to zero. The Identifier field in a BS's PKM-RSP message shall match the Identifier field of the PKM-REQ message the BS is responding to. The Identifier field in TEK Invalid messages, which are not sent in response to PKM-REQs, shall be set to zero. The Identifier field in unsolicited Authorization Invalid messages shall be set to zero.

On reception of a PKM-RSP message, the SS associates the message with a particular state machine (the Authorization state machine in the case of Authorization Replies, Authorization Rejects, and Authorization Invalids; a particular TEK state machine in the case of Key Replies, Key Rejects, and TEK Invalids).

An SS shall keep track of the identifier of its latest, pending Authorization Request. The SS shall discard Authorization Reply and Authorization Reject messages with Identifier fields not matching that of the pending Authorization Request.

An SS shall keep track of the identifiers of its latest, pending Key Request for each SA. The SS shall discard Key Reply and Key Reject messages with Identifier fields not matching those of the pending Key Request messages.

Attributes

PKM attributes carry the specific authentication, authorization, and key management data exchanged between client and server. Each PKM packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a PKM message. The end of the list of attributes is indicated by the LEN field of the MAC PDU header.

Table 28a – PKM Message codes

15	Secure EAP Packet	PKM-REQ, PKM-RSP
16~255	Reserved	

6.3.2.3.9.13 Secure EAP Packet message

When the SS and BS have an EAP message received from an EAP method for transmission, SS and BS encapsulates it in an EAP Packet message.

Code : 15

Attributes are shown in Table 39c.

Table 39c-Secure EAP Packet attributes

Attribute	Contents
Key-Sequence-Number	AK Sequence Number
EAP Protocol	Contains the EAP Packet, not interpreted in the MAC
HMAC-Digest	Keyed SHA message Digest

The EAP Payload field carries encrypted and authenticated EAP data in the format described in RFC2284bis

EAP Protocol attribute shall be encrypted by SEK.

The HMAC-Digest attribute shall be the final attribute in the message's attribute list. Inclusion of the keyed digest allows the BS to authenticate the Secure EAP Packet message. The HMAC-Digest's authentication key is derived from the AK

7.2 PKM protocol

7.2.1.1 Authorization via PKM RSA Authentication Protocol

An SS begins authorization by sending an Authentication Information message to its BS. The Authentication Information message contains the SS manufacturer's X.509 certificate, issued by the manufacturer itself or by an external authority. The Authentication Information message is strictly informative; i.e., the BS may choose to ignore it. However, it does provide a mechanism for a BS to learn the manufacturer certificates of its client SS.

The SS sends an Authorization Request message to its BS immediately after sending the Authentication Information message. This is a request for an AK, as well as for the SAIDs identifying any Static Security SAs the SS is authorized to participate in. The Authorization Request includes

a) a manufacturer-issued X.509 certificate
b) a description of the cryptographic algorithms the requesting SS supports; an SS's cryptographic capabilities are presented to the BS as a list of cryptographic suite identifiers, each indicating a particular pairing of packet data encryption and packet data authentication algorithms the SS supports
c) the SS's Basic CID. The Basic CID is the first static CID the BS assigns to an SS during initial ranging—the primary SAID is equal to the Basic CID

In response to an Authorization Request message, a BS validates the requesting SS's identity, determines the encryption algorithm and protocol support it shares with the SS, activates an AK for the SS, encrypts it with the SS's public key, and sends it back to the SS in an Authorization Reply message. The authorization reply includes:

a) an AK encrypted with the SS's public key
b) a 4-bit key sequence number, used to distinguish between successive generations of Aks
c) a key lifetime
d) the identities (i.e., the SAIDs) and properties of the single primary and zero or more static SAs the SS is authorized to obtain keying information for

While the Authorization Reply shall identify Static SAs in addition to the Primary SA whose SAID matches the requesting SS's Basic CID, the Authorization Reply shall not identify any Dynamic SAs.

The BS, in responding to an SS's Authorization Request, shall determine whether the requesting SS, whose identity can be verified via the X.509 digital certificate, is authorized for basic unicast services, and what additional statically provisioned services (i.e., Static SAIDs) the SS's user has subscribed for. Note that the protected services a BS makes available to a client SS can depend upon the particular cryptographic suites SS and BS share support for.

An SS shall periodically refresh its AK by reissuing an Authorization Request to the BS. Reauthorization is identical to authorization with the exception that the SS does not send Authentication Information messages during reauthorization cycles. Subclause 7.2.4's description of the authorization state machine clearly indicates when Authentication Information messages are sent.

To avoid service interruptions during reauthorization, successive generations of the SS's AKs have overlapping lifetimes. Both SS and BS shall be able to support up to two simultaneously active AKs during these transition periods. The operation of the Authorization state machine's Authorization Request scheduling algorithm, combined with the BS's regimen for updating and using a client SS's AKs (see 7.4), ensures that the SS can refresh.

After achieving successful authorization, SS and BS may seek for further EAP based authentication by exchanging PKM Secure EAP packets that carries data in the format described in RFC2284bis

7.5.4 Derivation of TEKs, KEKs, ~~and~~ message authentication keys, and SEKs

The BS generates AKs, TEKs and IVs. A random or pseudo-random number generator shall be used to generate

AKs and TEKs. A random or pseudo-random number generator may also be used to generate IVs. Regardless of how they are generated, IVs shall be unpredictable. Recommended practices for generating random numbers for use within cryptographic systems are provided in IETF RFC 1750 [B30].

7.5.4.1 DES Keys

FIPS 81 defines 56-bit DES keys as 8-byte (64-bit) quantities where the seven most significant bits (i.e., seven leftmost bits) of each byte are the independent bits of a DES key, and the least significant bit (i.e., rightmost bit) of each byte is a parity bit computed on the preceding seven independent bits and adjusted so that the byte has odd parity.
PKM does not require odd parity. The PKM protocol generates and distributes 8-byte DES keys of arbitrary parity, and it requires that implementations ignore the value of the least significant bit of each.

7.5.4.2 KEKs

7.5.4.2.1 3-DES KEKs

The keying material for two-key 3-DES consists of two distinct (single) DES keys.
The 3-DES KEK used to encrypt the TEK-64 is derived from a common AK. The KEK shall be derived as follows:
KEK=Truncate(SHA(K_PAD_KEK | AK),128)
K_PAD_KEK=0x53 repeated 64 times, i.e., a 512-bit string.
Truncate(x,*n*) denotes the result of truncating x to its leftmost *n* bits.

SHA(*x*|*y*) denotes the result of applying the SHA-1 function to the concatenated bit strings *x* and *y*.vThe keying material of 3-DES consists of two distinct DES keys. The 64 most significant bits of the KEKvshall be used in the encrypt operation. The 64 least significant bits shall be used in the decrypt operation.

7.5.4.2.2 AES KEKs

The construction of the KEK for use with TEK-128 keys shall be the same as for 3-DES KEKs as described in 7.5.4.2.1 except that the full 128 bits of the KEK are used directly as the 128 bit AES key, instead of the KEK being split into two 64 bit DES keys.

7.5.4.4 AES SEKs

The SEK shall be derived as follows:

- SEK_D (128bits) = Truncate (SHA (S_PAD_D | AK), 128)
- SEK_U (128bits) = Truncate (SHA (S_PAD_U | AK), 128)

S_PAD_D = 0x3B repeated 64 times
S_PAD_U = 0x5D repeated 64 times

PKM Secure EAP packet message shall be encrypted by AES ECB mode.
Encryption: C = Es1[P]
Decryption: P = Ds1[C]
S1= the 128bits SEK_D/SEK_U
E[ ] = 128-bits AES ECB mode encryption

D[ ] = 128-bits AES ECB mode decryption

11.3.2.11 Authorization Policy Support

This field indicates authorization policy that both SS and BS need to negotiate and synchronize. A bit value of 0 indicates “not supported” while 1 indicates “supported.” If this field is omitted, then both SS and BS shall use the IEEE 802.16 essential privacy method, constituting X.509 digital certificates and the RSA public key encryption algorithm, as authorization policy.

Type	Length	Value	Scope
5.25	1	Bit# 0: IEEE 802.16 essential privacy (Legacy PKM) -Default Bit# 1: Authorization via PKM EAP ~~7: Reserved for open privacy. Set to 0~~ Bit# 0 and 1: Authorization via Legacy PKM and EAP based authentication over Secure EAP PKM message Bit# 2-7: Reserved for open privacy. Set to 0	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)

Reference

- IEEE C802.16-71/r4, Enhancement of 802.16e to Support EAP-based Authentication/Key Distribution Rev.4 Streetwaves Networking
- RFC 2284bis IETF Internet Draft