	IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>
Title	**Enhanced EAP-based User Authentication coexisting with PKM based Device Authentication**
Date Submitted	**2004-05-18**
Source(s)	Dongkie Lee, DongIl Moon, DongRyul Lee, JongKuk Ahn, Sungho Ha SK Telecom 15F, Seoul Finance Center, 84, Taepyungpro 1 ga, Chung-gu, Seoul, 100-768, Korea Voice: +82-2-6323-3147 Fax: +82-2-6323-4493 [mailto: {galahad,dimoon,drlee,jgahn,ss23}@sktelecom.com]
Re:	Response to IEEE 802.16-04/19 (Recirculation Ballot #14a Announcement)
Abstract	To minimize impact on the current standard and achieve two-tiered device/user authentication, EAP is performed after PKM Key exchange. EAP-based User Authentication is separate from Device Authentication and operators can choose any EAP-based User Authentication method based on their needs.
Purpose	Discuss and Adopt as the enhanced authentication procedure
Notice	s 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>.

Enhanced EAP-based User Authentication coexisting with PKM based Device Authentication

Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn
SK Telecom

1. Problem Statements

1.1 Pros and Cons of PKM EAP

With 802.11 WLAN, several EAP methods are developed and widely used due to the WEP's security weakness. It suffered also from the static key provisioning problem. That's why the so-called Dynamic WEP is introduced to WLAN. With Dynamic WEP, WEP keys are refreshed periodically using EAP-TLS, EAP-TTLS, PEAP, etc. Where Client and AAA negotiate master key, and the master key is sent to the AP from the AAA. Again as mentioned, proliferation of EAP is driven by WEP's static key provisioning problem and security weakness.

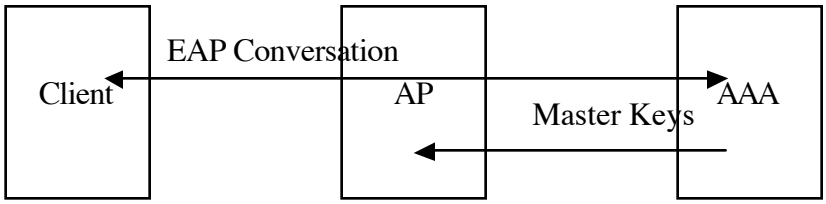


Figure 1 Transfer of EAP Master Key

But with 802.16, it's a different story. Although, PKM have somethings left to be enhanced, it's quite well defined and does not suffer from the problems of WEP. Public key systems which requires certificates of both sides such as EAP-TLS have suffered deployment and management problems. But with PKM, off-the-shelf SS and BS have embedded certificate and does not suffer from the deployment and management problem. TEK is refreshed periodically and does not suffer from the static key provisioning problem. And PKM does not suffer from the security flaw which is found in WLAN. This is the first reason EAP doesn't need not be tied to or tweaked with PKM.

Secondly EAP-MD5 does not have any master key generation mechanism and cannot be used. If we stick to PKM EAP which is proposed already, EAP-MD5 cannot be used. ANY EAP methods SHALL be supported for user authentication by IEEE standard. EAP-MD5 is not a exception.

Thirdly, if Authorization Key is derived from EAP AAA key, it'll make BS difficult to manage several timers. According to P802.16-REVd/D4, below 7 timer values are forwarded with Auth Reply message. If EAP is tweaked into PKM, 4 of these values should come from AAA and BS should parse EAP message, extract TEK-related values and somehow combine these 7 timers and forward to MSS in the Auth Reply. That is, AK related timer management entity and TEK timer management entity should be separated.

PKM configuration	Relation	
Authorize wait timeout		AK
Reauthorize wait		AK
Authorization grace time		AK
Operational wait timeout	TEK	
Rekey wait timeout	TEK	
TEK grace time	TEK	
Authorize reject wait		AK

Therefore separation of PKM and user authentication has minimal impact on the current standard and it'll benefit both operators and vendors also. According to this contribution, EAP method for user authentication shall be performed after PKM key exchange phase is complete. So shared key or master key is not transferred from AAA to BS. EAP-MD5, EAP-TTLS, EAP-TLS, EAP-AKA etc whatever may be used and

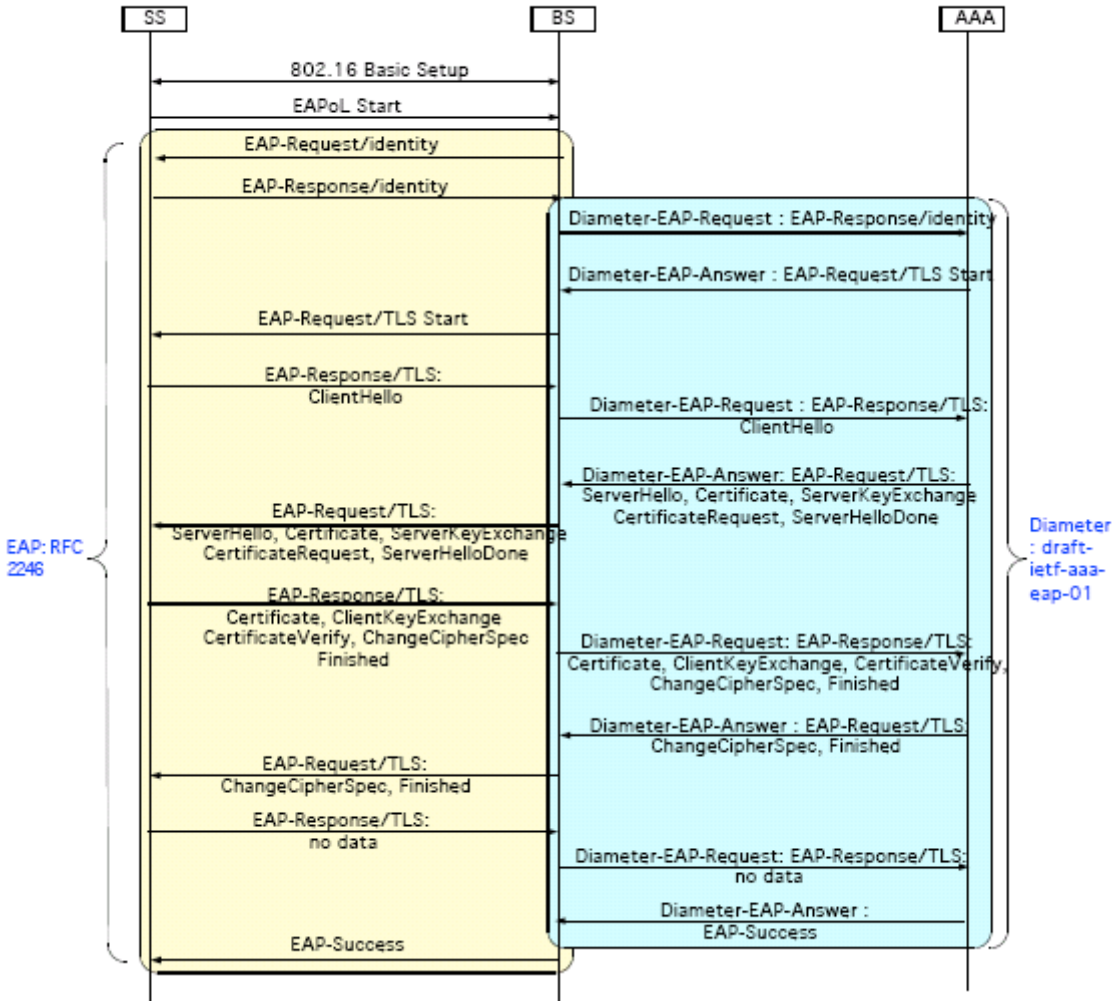
is up to the operators. If operators would like to use light-weight method, there's EAP-MD5. If operators would like to use integrated method with CDMA 2000, there's EAP-AKA or EAP-CAVE. If operators would like to use certificate based authentication, there's EAP-TLS/TTLS/PEAP.

Table 1Comparison between PKM EAP and this Proposal

	Current 802.16e/D2	This Proposal
Impact on 802.16 standard	AK is derived from EAP AAA key.	PKM AK is used as is defined in standard.
EAP Usage	EAP Key Exchange and user authentication is done and AAA key is used as AK.	EAP Key Exchange and user authentication is done after PKM.
Device Authenticati on	Is not performed.	Is performed as is defined in standard.
AK/TEK state machine	Is managed by BS.	AK state machine is managed by AAA and TEK state machine is managed by BS. Timer values in Auth Reply should be separately defined between BS, AAA.
Mutual Authentication	depends on EAP method	depends on EAP method
BS/AAA Overhead	BS : Light AAA : Heavy	BS : Same as PKM AAA : Light

1.2 EAP REQ vs PKM REQ direction mismatch

[Reference] Call flow



EAP Request message is sent from BS to MSS, however PKM Request message is sent from MSS to BS. So EAP Request message is not mapped to PKM Request message. If BS sends EAP Request message, it should send it in *unsolicited* PKM Response message, which is not described in the standard. It's better to newly define EAP-REQ/RSP, which could be used for downlink/uplink and EAP-Request/Response/Success/Failure. Finally, EAP-Success, which dose not trigger response, should also be considered in designing protocol.

2. Overview of Proposed Solutions

In this contribution, two issues are discussed.

One is about remedying the direction mismatch problem between PKM message and EAP message.

The other is about new EAP authentication which is performed after PKM key exchange.

[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

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

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~~ MSS and BS uses the identifier to match a ~~BS~~ response to the ~~SS's~~ requests.

The MSS and the BS shall increment (modulo 256) the Identifier field whenever ~~it~~they issue~~s~~ a new PKM message. A "new" message is an Authorization Request, ~~or~~ Key Request, EAP Transfer Request, or EAP Transfer Response 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

	PKM Message Type	MAC Message Type
13	EAP Transfer Request	PKM-REQ
14	EAP Transfer Reply	PKM-RSP
	reserved	

[Add the following to section 6.4.2.4.9:]

6.3.2.3.9.11 EAP Transfer Request message

When a BS has an EAP message received from an EAP method for transmission to the SS, it encapsulates it in an EAP Transfer Request message. EAP Transfer Request message contains EAP Request, EAP Response, EAP Success or EAP Failure message.

Attributes are shown in Table 39a.

Table 39a-EAP Transfer Request attributes

Attribute	Contents
EAP Protocol	Contains the EAP Request, EAP Success, Failure message, not interpreted in the MAC

The EAP Payload field carries data in the format described in RFC2284bis (see section 4).

6.3.2.3.9.12 EAP Transfer Response message

When an SS has an EAP message received from an EAP method for transmission to the BS, it encapsulates it in an EAP Transfer Response message. After several EAP Request Transfer and EAP Response Transfer message exchanges, EAP Success or Failure message is sent to the SS from the BS. On receiving EAP Success or Failure Transfer message, MSS responds with EAP Transfer Response which has no EAP Payload.

Code: 14
Attributes are shown in Table 39b.

Table 39b—EAP Transfer Response attributes

Attribute	Contents
EAP Payload	Contains the EAP Response message or null, not interpreted in the MAC

The EAP Payload field carries data in the format described in RFC2254bis (or successor RFC) section 4.

7.2 PKM protocol

7.2.1.1 Authorization via PKM RSA Authentication Protocol and EAP Authentication

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 EAP packets that carries data in the format described in RFC2284bis. This EAP authentication is performed if it is negotiated with SBC-REQ/RSP.

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

4	1	Bit# 0: IEEE 802.16 essential privacy (Legacy PKM Bit# 1: Authorization via PKM EAP Bit# 2: Authentication via Legacy PKM and EAP based authentication Bit# ~~1~~3-7: Reserved for open privacy. Set to 0	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)