IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>

Title	**Bi-directional PKM messages for EAP messages**	
Date Submitted	**2004-07-07**	
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]
	Sungcheol Chang, ETRI	
	Junhyuk Song, Samsung	junhyuk.song@SAMSUNG.COM
	David Johnston, Intel	dj.johnston@INTEL.COM
Re:	Recirculation Ballot #14b Announcement	
Abstract	To remedy direction mismatch problem between PKM messages and EAP messages, PKM messages shall be bi-directional and EAP messages Container, which is transparent to lower MAC layer, is consolidated to one.	
Purpose	Discuss and Adopt as the baseline text	
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>.	

1

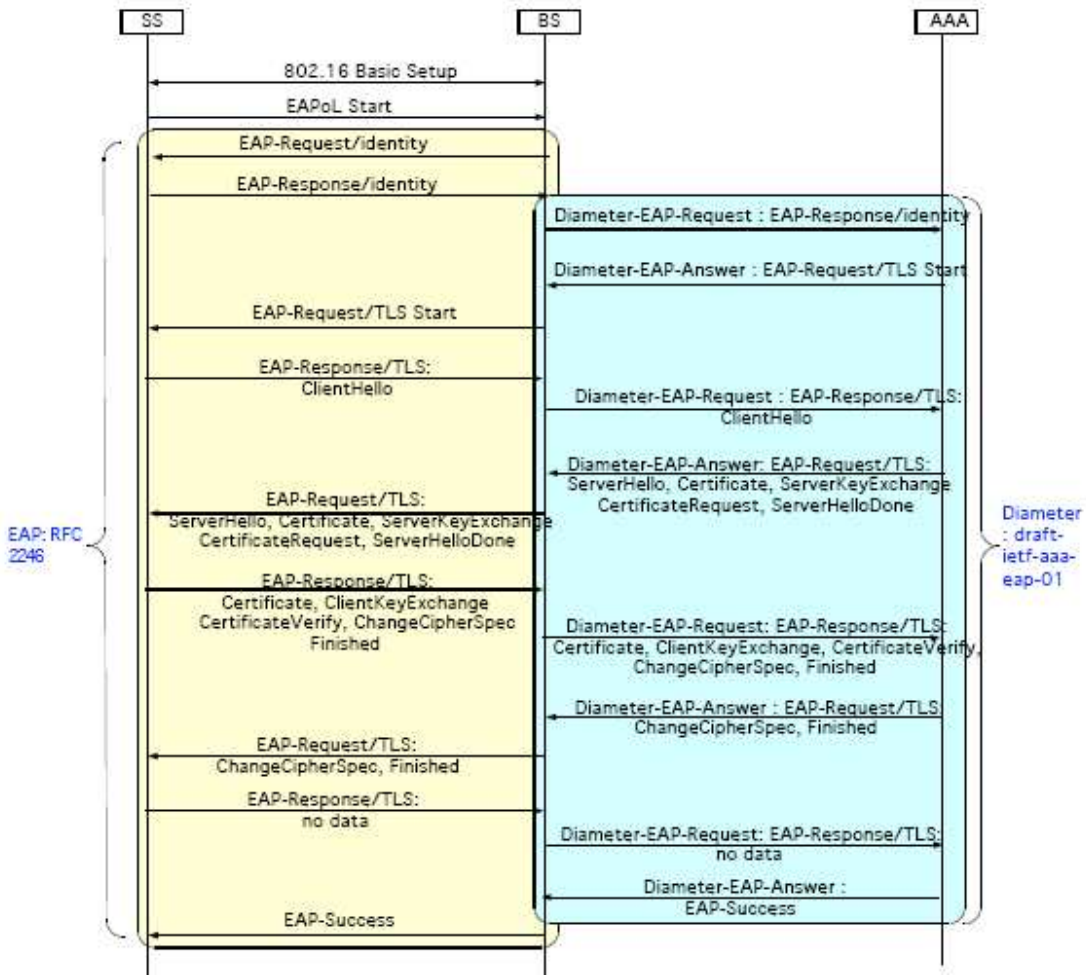
Bi-directional PKM messages for EAP messages

Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn, SK Telecom
Sungchul Chang, ETRI
Junhyuk Song, Samsung
DavidJohnston, Intel

1. Problem Statements

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. In order to solve this problem, PKM messages should be changed to bi-directional. And considering the fact that MAC management layer is agnostic about EAP messages code, EAP-Transfer-Request and EAP-Transfer-Response messages shall be incorporated into one EAP-Transfer message.

[Reference] Call flow



2 Proposed Changes

[Add~~Change/Delete~~ the following as shown to IEEE 802.16e/D3]

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 or EAP Transfer 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/PKM-RSP
~~14~~	~~EAP Transfer Reply~~	~~PKM-RSP~~
14~~15~~	EAP Establish-Key Request	PKM-REQ~~SP~~
15~~16~~	EAP Establish-Key Reply	PKM-RSP~~EQ~~
16~~17~~	EAP Establish-Key Reject	PKM-RSP~~EQ~~
17~~18~~	EAP Establish-Key Confirm	PKM-REQ~~SP~~
18~~9~~-255	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 MSS, it encapsulates it in an EAP Transfer message, which MAC message type is PKM-REQ. When an MSS ~~or a BS~~ has an EAP message received from an EAP method for transmission to the BS~~other side BS~~, it encapsulates it in an EAP Transfer ~~Request~~ message, which MAC message type is PKM-RSP.

Attributes are shown in Table 39a.

Table 39a-EAP Transfer ~~Request~~ attributes

Attribute	Contents
EAP Protocol	Contains the EAP Request/Response/Success/Failure, 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 a BS has an EAP message received from an EAP method for transmission to the SS, it encapsulates it in an EAP Transfer Response message.~~

~~Code: 14~~

~~Attributes are shown in Table 39b.~~

~~Table 39b—EAP Transfer Response attributes~~

~~Attribute~~	~~Contents~~
~~EAP Payload~~	~~Contains the EAP authentication data, not interpreted in the MAC~~

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