Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Clarification on the PKM-REQ/RSP Management Message Encodings**	
Data Submitted	**2005-06-08**	
Source(s)	Seokheon Cho Taeyong Lee Chulsik Yoon ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr
Re:	IEEE P802.16e/D8	
Abstract	Some attributes used in the PKM-REQ/RSP messages are not defined as a field in the PKM-REQ/RSP message encodings. This contribution defines those attributes in the PKM-REQ/RSP message encodings.	
Purpose	Adoption of proposed changes into P802.16e/D8	
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:chiar@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>.

Clarification on the PKM-REQ/RSP Management Message Encodings

Seokheon Cho, Taeyong Lee, and Chulsik Yoon

ETRI

Introduction

Some attributes used in the PKM-REQ/RSP messages are not defined in the PKM-REQ/RSP management message encodings. For example, Auth Result Code used in the PKMv2 RSA-Acknowledgement message and EAP Payload used in the PKMv2 EAP -Transfer message and the PKMv2 Authenticated EAP Transfer message.

On the contrary, even though some attributes are not included in the PKM-REQ/RSP messages, they are defined as a field in the PKM-REQ/RSP management message encodings. For instance, EAP-Master-Key-ID, Target BSID, AA-Descriptor, and AA-Type are not used any more.

This contribution corrects those problems by defining the above mentioned attributes as a TLV field in the PKM-REQ/RSP management message encodings.

Proposed Changes into IEEE P802.16e/D8

[Change the Table 370 in sub-clause 11.9:]

11.9 PKM-REQ/RSP management message encodings

Table 370-PKM attribute types

Type	PKM attribute
22	~~Version~~ Reserved
28	~~EAP-Master-Key-ID~~ EAP Payload
29	Nonce
30	~~Target BSID~~ Auth Result Code
31	~~AA-Descriptor~~ Reserved
32	~~AA-Type~~ Reserved
33	SS_RANDOM
34	BS_RANDOM
	… **Rest of the attributes of this table remains the same.**

[Delete the following sub-clause in 11.9:]

~~11.9.21 Target BSID~~

~~Type~~	~~Length~~	~~Value~~
~~30~~	~~6~~	~~Target BSID~~

[Add the following two sub-clauses in the section 11.9:]

and [Renumber the following two sub-clauses based on the "Type Value" in the section 11.9:]

11.9.x1 EAP Payload

Description: This attribute contains the payload used in the upper EAP authorization layer. The security sublayer doesn't interpret this attribute.

Type	Length	Value
28	Variable	EAP payload

11.9.x2 Auth Result Code

Description: This attribute contains the result code of the RSA-based authorization (only for PKMv2).

Type	Length	Value
30	1	0, Success 1, Reject 2-255, reserved.

[Change following sub-clause 6.3.2.3.9.15]

~~6.3.2.3.9.15 PKMv2 EAP Transfer message~~

6.3.2.3.9.16 PKMv2 EAP-Transfer message

When an MS has an EAP payload ~~message~~ received from an EAP method protocol for transmission to the BS or when a BS has an EAP payload ~~message~~ received from an EAP method protocol for transmission to the MS, it encapsulates it in a PKMv2 EAP Transfer message.

Code: ~~17~~ 18

Attributes are shown in Table 37e.

Table 37e – PKMv2 EAP-Transfer attributes

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

The EAP Payload field carries data in the format described in section 4 of RFC 2284bis.

[Change sub-clauses 6.3.2.3.9.16 as follows]

~~6.3.2.3.9.16 PKMv2 Authenticated EAP Transfer message~~

6.3.2.3.9.17 PKMv2 Authenticated EAP-Transfer message

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. ~~If~~ Moreover, if EIK is available and an MS or BS has an EAP payload ~~message~~ received from an EAP method protocol for transmission, it encapsulates EAP payload ~~message~~ in a PKMv2 Authenticated EAP Transfer message. ~~In other words, this message may be used in case that both an MS and BS negotiate RSA-based authorization and Authenticated EAP-based authorization as authorization policy support.~~

Code: ~~18~~ 19

Attributes are shown in Table 37f.

Table 37f – PKMv2 Authenticated EAP Transfer attributes

Attribute	Contents
PAK Sequence Number	PAK Sequence Number
EAP ~~Protocol~~ Payload	Contains the EAP authentication data, not interpreted in the MAC
CMAC/HMAC Digest	Message Digest calculated using EIK

The EAP Payload field carries EAP data in the format described in RFC 3748.

The CMAC-Digest or HMAC-Digest attribute shall be the final attribute in the message's attribute list.

Inclusion of the OMAC digest or HMAC-Digest allows the MS and BS to cryptographically bind previous authorization and following EAP authentication by authenticating the EAP payload ~~message~~. The OMAC-Digest's authentication key is derived from the ~~AK~~ EIK.