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	**2004-05-07**
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

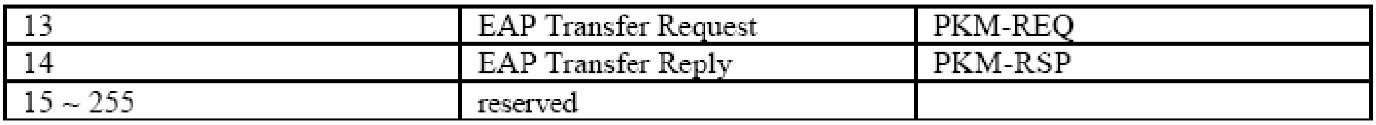
Samsung Electronics

1 Scope of this document

This document outlines how to provide the protection to the Extensible Authentication 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] Internet Draft described, EAP has been known for security vulnerability, such as lack of user identity protection and Man in the Middle Attack. Those problems are more often caused by use of legacy authentication method, 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. Enabling encryption toward to Primary Management Connection PKM EAP messages for user authentication will fix the above problems (See Figure 2)
In this contribution we propose to add PKM message code 15, 16,17, and 18 for Secure EAP messages (See Figure 3) in addition to PKM EAP message codes previously decided 13 and 14 for User Authentication



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

Figure-1 Approved new PKM message types

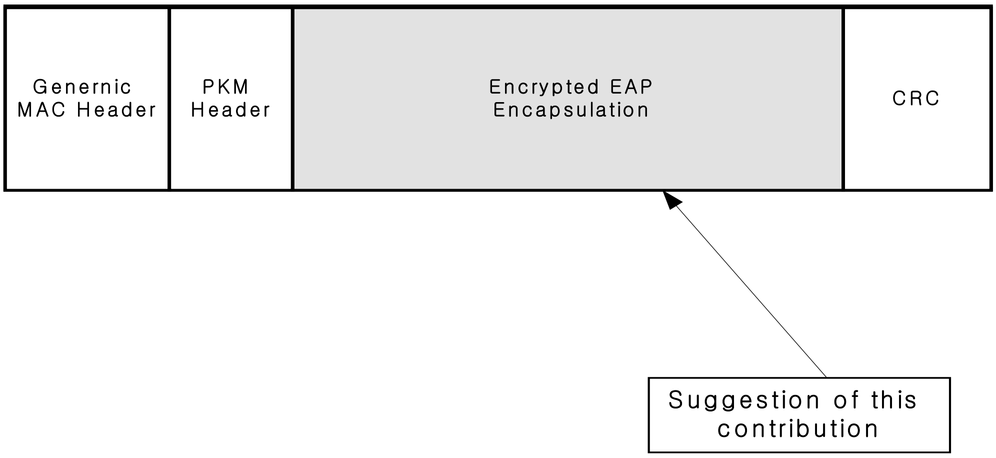


Figure-2 Proposed EAP PKM message encryption

15	Secure EAP Transfer Request	PKM-REQ
16	Secure EAP Transfer Reply	PKM-RSP
17	Secure EAP Transfer Success	PKM-REQ
18	Secure EAP Transfer Failure	PKM-REQ
16~255	Reserved	

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

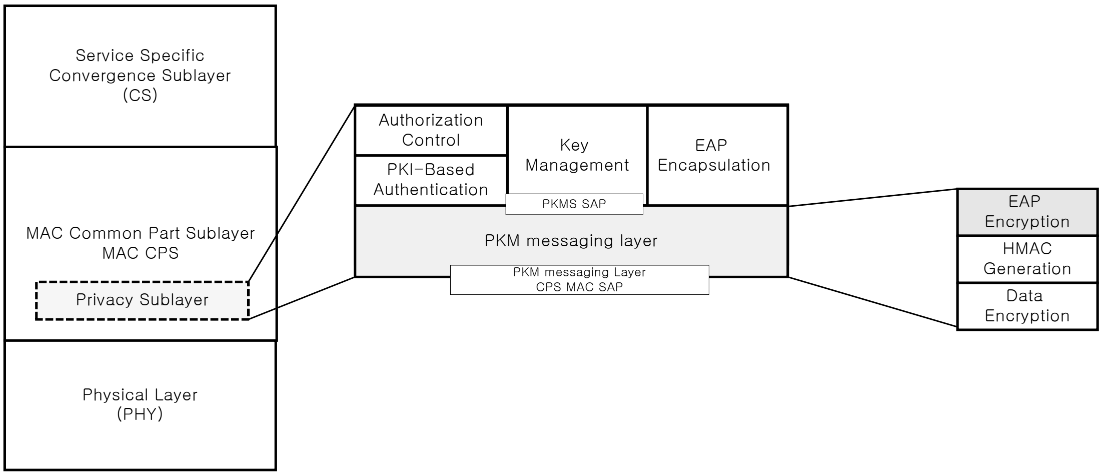


Figure 4 Control Plane

3.1 SEK (Secure EAP Key) based Secure EAP messages

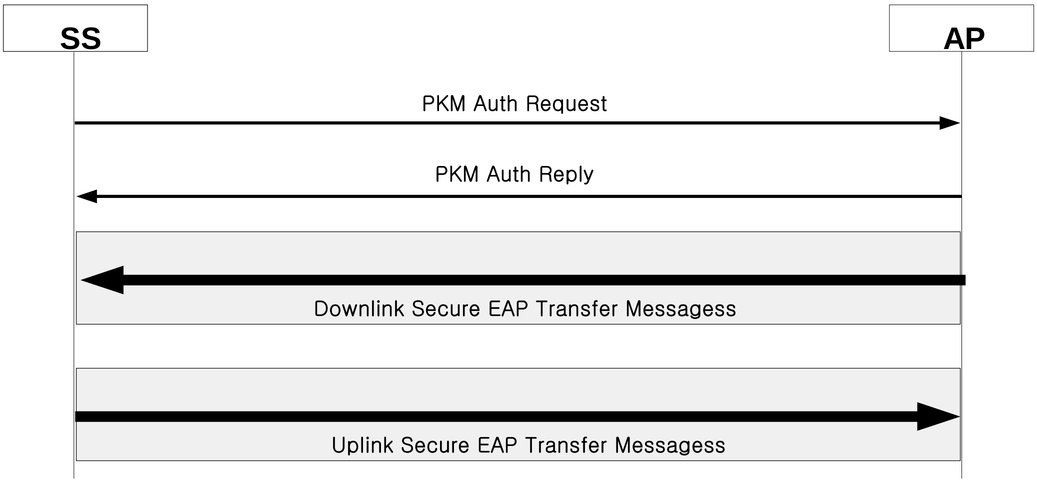
PKM EAP transfer messages can be secured by SEK derived from AK. In this way Primary Management Connection is not mapped to SA, however Message encryption will be performed to PKM EAP transfer message based on SEK derived from AK. (Note that Secure EAP support will be negotiated during SBC Capability negotiation in addition to exiting Authorization Policy)

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


SS
AP
PKM Auth Request
PKM Auth Reply
Downlink Secure EAP Transfer Messagess
Uplink Secure EAP Transfer Messagess

Proposed Text Change

TBA

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