Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**PEAP Clarification**
Date Submitted	**2005-03-~~10~~16**
Source(s)	JUNHYUK SONG, JICHEOL LEE, YONG CHANG Voice: +82-31-279-3639 Samsung Electronics junhyuk.song@samsung.com
Re:	Re: IEEE P802.16e/D5a
Abstract	PEAP Clarification
Purpose	Discuss and Adopt as the baseline text
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>.

PKM version 2

Protected EAP Clarification Rev 1

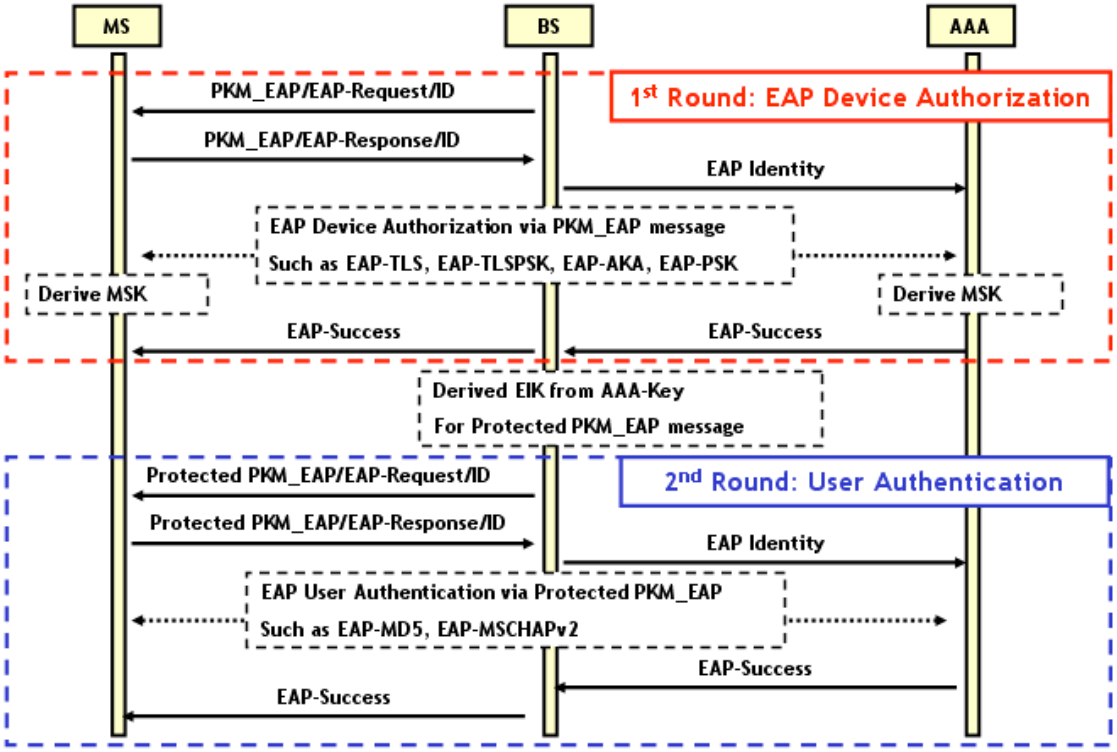
JUNHYUK SONG, JICHEOL LEE, YONG CHANG
Samsung Electronics

INTRODUCTION

Per decision in last meeting, D6 text adopted PKM Protected EAP message and EIK. It will protect subsequent EAP authentication messages encapsulated in PKM management message from possible forgery attack when RSA based Authorization executed. However current text is not clear about how Protected EAP message could be used in case of EAP only mode. In EAP only mode when EAP authentication method such as EAP-PSK or EAP-AKA is used as a device authentication method, MS and BS may run second round of EAP authentication method for user authentication by exchanging PKM Protected EAP messages.
In this contribution we will specify the EIK derivation when EAP only mode is used.

Secondly, the name of message (Protected EAP) is confused with PEAP, so we introduced new name "Authenticated EAP Message".

Twice EAP example



Changes to 802.16e D6 text

7.2.2.2.2 EAP authentication

If a RSA mutual authorization took place before the EAP exchange, the EAP messages may be protected using EIK - EAP Integrity Key derived from pre-PAK (see 7.2.2.2.1). EIK and EEK are 128 bits long.

The product of the EAP exchange which is transferred to 802.16 layer is the AAA-key. This key is derived ~~(~~or may be equivalent to the 512-bits Master Session Key (MSK)~~)~~. This key is known to the AAA server, to the Authenticator* (transferred from AAA server) and to the MS. The MS and the authenticator derive a PMK (Pairwise Master Key) and optional EIK by truncating the AAA-key ~~after~~ to 288~~160~~ bits.

The PMK and EIK derivation from the AAA-key is as follows:

EIK|PMK = truncate (AAA-key, 288~~160~~)

If more keying material is needed for future link ciphers, the key length of the PMK may be increased.

[Change Figure 133]

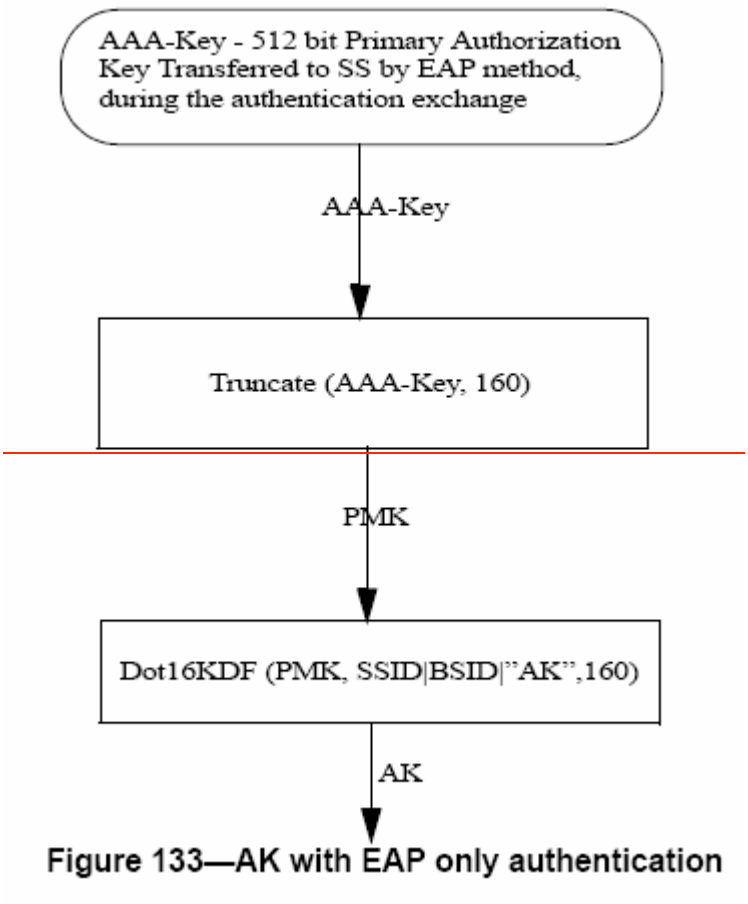


Figure 133—AK with EAP only authentication

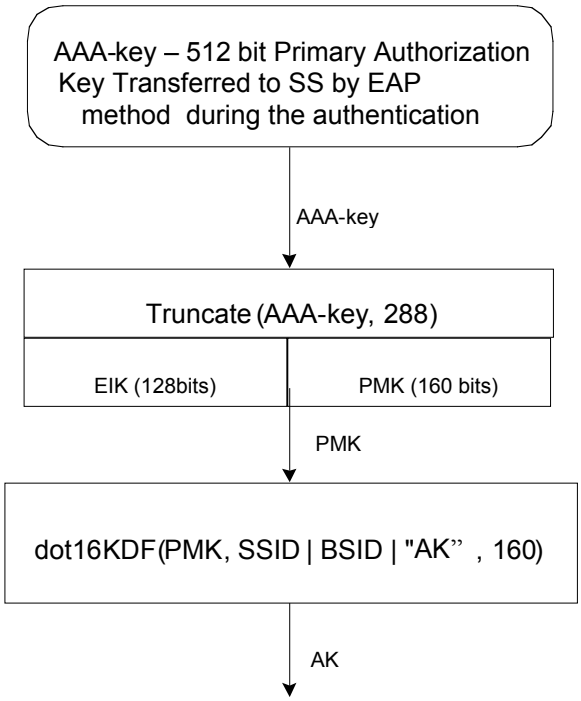


Figure 133-AK with EAP only authentication

Proposed changes of name from "protected EAP" to "authenticated EAP" in D6text.

- table 20 of page 40
- table 37h of page 46
- 6.3.2.8.9.18 line 1 and line 7 of page 46
- 7.2.1.3 line 43 of page 179
- line 51 of page 180 (7.2.1.3.1)
- line 27 of page 182 (7.2.1.3.2)
- 7.2.2.2.2 (end of paragraph) add below
  - After successful EAP based authorization if the MS or BS wants to run additional EAP authentication (Note: This EAP authentication method shall not derive key materials and PMK), the authenticated~~protected~~ EAP messages shall carry EAP message. It shall cryptographically bind previous ~~RSA~~ EAP authentication~~authorization~~ and following~~further~~ EAP authentication session, while protecting second~~following~~ EAP messages.