Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**CMAC/HMAC-Digest Generation Method using the EIK**
Data Submitted	**2005-07-14**
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/D9
Abstract	A PKMv2 Authenticate-EAP-Transfer message includes CMAC/HMAC-Digest. CMAC/HMAC-Digest in this message is generated with EIK. However, since there is no method for generating CMAC/HMAC-Digest by using EIK, it is necessary to specify the generation method.
Purpose	Adoption of proposed changes into P802.16e/D9
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>.

CMAC/HMAC-Digest Generation Method using the EIK

Seokheon Cho, Taeyong Lee, and Chulsik Yoon

ETRI

Introduction

0.1 IEEE P802.16e/D9 Status and Problems

A PKMv2 Authenticated-EAP-Transfer message contains the CMAC/HMAC-Digest for message authentication. The CMAC_KEY_* (CMAC authentication key) and the HMAC_KEY_* (HMAC authentication key) used to generate the CMAC/HMAC-Digest are derived from the EIK, which is derived from pre-PAK in the RSA-based authorization procedure.

However, the generation method for the CMAC_KEY_* and the HMAC_KEY_* using the EIK is not defined in IEEE P802.16e/D9. It is necessary to specify the generation method.

0.2 Solutions

A method for generating message authentication keys used in a PKMv2 Authenticated-EAP-Transfer message is proposed as follows:

The keys used for CMAC key and for KEK are as follows:

CMAC_KEY_U | CMAC_KEY_D <= Dot16KDF(EIK, SSID | BSID | "CMAC_KEYS ", 256)

The keys used for HMAC key and for KEK are as follows:

HMAC_KEY_U | HMAC_KEY_D <= Dot16KDF(EIK, SSID | BSID | "HMAC_KEYS", 320)

Proposed Changes into IEEE P802.16e/D9

[Change sub-clauses 7.2.2.2.9 as follows]

7.2.2.2.9 Message authentication keys (CMAC/HMAC) and KEK derivation

MAC (message authentication code) keys are used to sign management messages in order to validate the authenticity of these messages. The MAC to be used is negotiated at SS Basic Capabilities negotiation.

There is a different key for UL and DL messages. ~~and also a CMAC key~~ Also, a different message authentication key is generated for a multicast message ~~for each multicast group~~ (this is DL direction only) and for a unicast message.

In general, the message authentication keys used to generate the CMAC value and the HMAC-Digest are derived from the AK.

The keys used for CMAC key ~~calculation~~ and for KEK are as follows:

CMAC_KEY_U | CMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | "CMAC_KEYS+KEK", 384)

CMAC_KEY_GD <= Dot16KDF(GKEK, "GROUP CMAC KEY",128) (Used for ~~group management messages MAC~~ multicast MAC message such as a PKMv2 Group-Key-Update-Command message)

The keys used for HMAC key ~~calculation~~ and for KEK are as follows:

HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, SSID | BSID | "HMAC_KEYS+KEK", 448)

HMAC_KEY_GD <= Dot16KDF(GKEK, "GROUP HMAC KEY", 160) (Used for ~~group management messages MAC~~ multicast MAC message such as a PKMv2 Group-Key-Update-Command message)

Exceptionally, the message authentication keys for the CMAC/HMAC-Digest included in a PKMv2 Authenticated-EAP-Transfer message are derived from the EIK instead of the AK

The keys used for CMAC key and for KEK are as follows:

CMAC_KEY_U | CMAC_KEY_D <= Dot16KDF(EIK, SSID | BSID | "CMAC_KEYS ", 256)

The keys used for HMAC key and for KEK are as follows:

HMAC_KEY_U | HMAC_KEY_D <= Dot16KDF(EIK, SSID | BSID | "HMAC_KEYS", 320)

[Add following contents below Figure 135 in sub-clause 7.2.2.2.10]

7.2.2.2.10 Key Hierarchy

Figure 136 outlines the process to calculate message authentication keys derived from the EIK. The message authentication keys are used to generate the CMAC value or the HMAC-Digest included in a PKMv2 Authenticated-EAP-Transfer message.

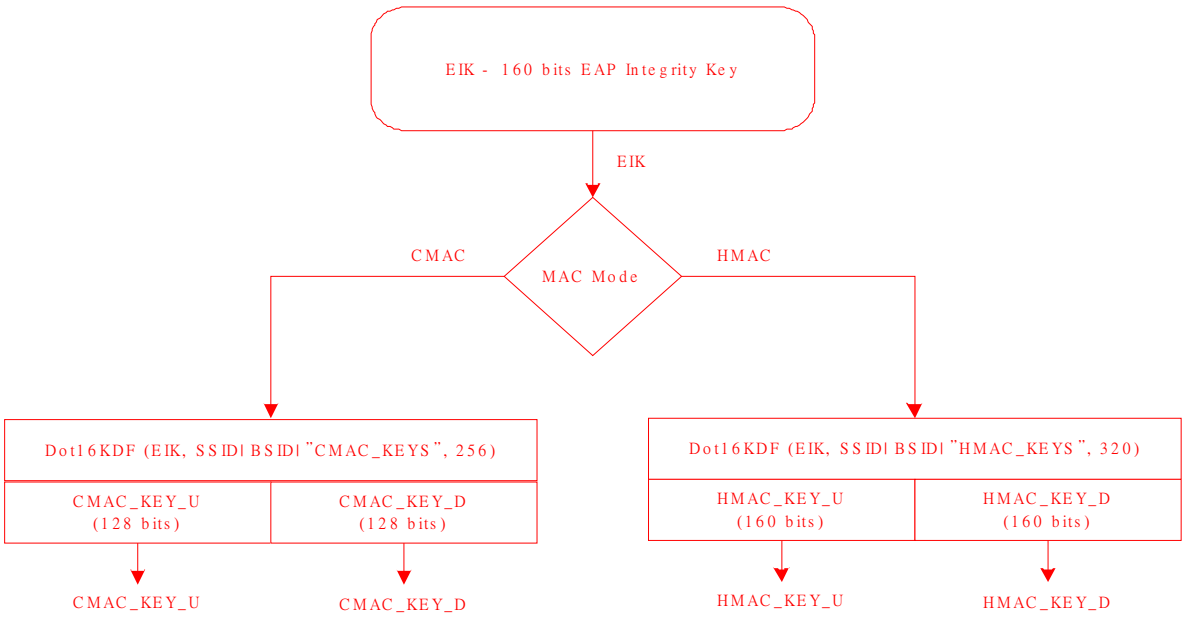

Figure 136-HMAC/CMAC authentication key derivation from EIK

[Change contents of Table 37f in sub-clause 6.3.2.3.9.17 as follows]

6.3.2.3.9.17 PKMv2 Authenticated EAP Transfer message

Table 37f - PKMv2 Authenticated EAP Transfer attributes

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

[Modify following contents in sub-clause 7.2.2.2.1]

7.2.2.2.1 RSA-based authorization

When the RSA-based authorization is negotiated as authorization policy, the PKMv2 RSA-Request, the PKMv2 RSA-Reply, the PKMv2 RSA-Reject, and the PKMv2 RSA-Acknowledgement messages are used to share the pre-PAK (Primary Authorization Key).

The pre-PAK is sent by the BS to the MS encrypted with the public key of the MS certificate. Pre-PAK is mainly used to generate the PAK. The optional EIK for transmitting authenticated EAP payload (see 7.2.2.2.2) are also generated from pre-PAK:

EIK | PAK = Dot16KDF(pre-PAK, SSID | BSID | "EIK+PAK", ~~288~~ 320)

PAK will be used to generate the AK (see below) if RSA authorization was used. PAK is 160 bits long.