Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Cryptosynchronized**
Date Submitted	**2004-05-07**
Source(s)	JunHyuk Song, Lim Geunhwi, Yong Chang 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>.

802.16e Crypto Synchronized HMAC Message Authentication

JunHyuk Song, Lim Geunhwi, Yong Chang
Samsung Electronics

1 Scope of this document

This document outlines how to provide Crypto Synchronized HMAC Message Authentication

2 Background

Current Message Authentication Code, HMAC-Digest doesn't include any time related information that shall open for replay attacks for some messages such as Location Update message in idles state. In this contribution propose to add PHY_SYNC in DL_MAP in computation for HMAC-DIGEST

3 Attack Scenario

Rogue SS could capture Location Update message and replay Location Update message later on to produce-unauthorized effect.

4 Proposed solution

HMAC Digest for Location Update message shall be computed as below:

- HMAC (160bits) = SHA (HMAC_KEY_D/U XOR opad, SHA(HMAC_KEY_D/U XOR ipad, text))

  - ipad (512 bits) = 0x36 repeated 64 times
  - opad (512 bits) = 0x5c repeated 64 times
  - Message text = DL_MAP의 PHY Synchronization field (32bits) XOR LSB 32bits of Location Update message

Proposed Text Change

TBD