Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Cipher-based MAC (CMAC) and
Date Submitted	**2005-05-04**
Source(s)	Jeff Mandin Runcom Hachoma 2 jeff@streetwaves-networks.com Rishon Lezion, Israel
Re:	IEEE P802.16REVe/D7 SB re circ
Abstract	Cipher-based MAC (CMAC) and other MAC issues
Purpose	Adopt changes.
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>.

Cipher-based MAC (CMAC) support

Jeff Mandin (Runcom)

1. Problem statement

1. 802.16e/D7 makes extensive use of "OMAC", which enables use of AES for MAC generation - but does not provide a reference for the algorithm

2. NIST has withdrawn its draft of OMAC. As a replacement proposal for a cipher-based MAC, it has selected the OMAC-1 variation - which it has renamed as CMAC.

3. The CMAC construction is still a draft and not yet an approved document however

2. Remedy

We should adopt CMAC, and specify that the intent is to use whatever algorithm is eventually approved by NIST (ie. not the current draft document). Essentially this means we are providing a hook for using CMAC in 802.16 after a final version has been approved

3. Text changes

[Replace every mention of "OMAC" with "CMAC"]

[Insert new paragraph 7.5.4:]

7.5.4 Cipher-based MAC (CMAC)

A BS or MS may support management message integrity protection based on Cipher-based MAC (currently under consideration by NIST) - together with the AES block cipher. NIST intends to publish the CMAC construction as **Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication** " upon approval.

[Renumber current 7.5.4 as 7.5.4.1]