Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Empty security suite definition**
Date Submitted	**2005-06-08**

Source(s)	Avishay Shraga	Avishay.shraga@intel.com
	Yigal Eliaspur	Voice: +972-54-5551063
	Intel corp.	Yigal.Eliaspur@intel.com
		Voice: +972-54-7884877

Re:	IEEE P802.16e/D8
Abstract	Add an empty security suite to allow SA with no security that make it possible to negotiate un protected SF
Purpose	Allow unprotected SF
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>.

Empty security suite definition

Avishay Shraga

1. Motivation

The standard allows unprotected transport but the way to negotiate it is not well defined.
Each SF must be linked to a Security Association thus it is "protected" and it looks like the only reasonable way to create an unprotected SF under these definitions is to define an Empty security suite.

2. Proposed solution

Define an Empty security suite which does not include either of the 3 parameters, when the SS gets a SA like that it does not have to manage a TEK FSM for this SA..

3. Changes summary

Change 11.9.14 Cryptographic suite

Table 377 – TEK encryption algorithm identifiers

Value	Description
0	No Tek Encryption Algorithm
1	3-DES EDE with 128-bit key
2	RSA with 1024-bit key
3	ECB mode AES with 128-bit key
4	AES Key Wrap with 128-bit key
5-255	Reserved

Add to Table 378—Allowed cryptographic suites

Value	Description
0x000000	No data encryption, no data authentication & No Tek Encryption