Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Definitions of the Security Sub-layer Protocol Stack**	
Data Submitted	**2006-09-21**	
Source(s)	Seokheon Cho 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 Std 802.16e-2005	
Abstract	The document contains definitions of the security sub-layer protocol stack.	
Purpose	Adoption of proposed changes into IEEE Std 802.16e-2005	
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>.	

Definitions of the Security Sub-layer Protocol Stack

Seokheon Cho and Chulsik Yoon

ETRI

Introduction

The security sublayer protocol stack is defined in the IEEE 802.16e-2005.

However, since there are no definitions for respective protocol stacks, it makes confusion to operate the security sublayer.

Proposed changes to IEEE Std 802.16e-2005

7.1 Architecture

[Insert the text below Figure 130j as indicated:]

- PKM Control Management: This stack controls all security components. Various keys are derived and generated in this stack.
- Traffic Data Encryption/Authentication Processing: This stack encrypts or decrypts the traffic data and executes the authentication function for the traffic data.
- Control Message Processing: This stack processes the various PKM-related MAC messages.
- Message Authentication Processing: This stack executes message authentication function. The HMAC, CMAC, or several short-HMACs can be supported.
- RSA-based Authentication: This stack performs the RSA-based authentication function using the SS's X.509 digital certificate and the BS's X.509 digital certificate, when the RSA-based authorization is selected as an authorization policy between an SS and a BS.
- EAP Encapsulation/Decapsulation: This stack provides the interface with the EAP layer, when the EAP-based authorization or the authenticated EAP-based authorization is selected as an authorization policy between an SS and a BS.
- Authorization/SA Control: This stack controls the authorization state machine and the traffic encryption key state machine.
- EAP and EAP Method Protocol: These stacks are outside of the scope of this standard.