Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**AES Key Wrap support for TEK encryption in Table 377**
Date Submitted	**2005-03-10**
Source(s)	JUNHYUK SONG, JICHEOL LEE, YONG CHANG Voice: +82-31-279-3639 Samsung Electronics junhyuk.song@samsung.com
Re:	Re: IEEE P802.16e/D5a
Abstract	AES-Key Wrap clarification
Purpose	Discuss and Adopt as the baseline text
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>.

PKM version 2

AES-KEY WRAP Clarification

JUNHYUK SONG, JICHEOL LEE, YONG CHANG
Samsung Electronics

INTRODUCTION

AES-KEY WRAP is supported in PKMv2 but Table 377 and 378 doesn't specify AES-KEY WRAP

Changes to 802.16e D6 text

11.9.14 EAP Cryptographic Suite

Table 377—TEK encryption algorithm identifiers

Value	Description
0	Reserved
1	3-DES EDE with 128-bit key
2	RSA with 1024-bit key
3	ECB mode AES with 128-bit key
~~3~~4-255	*Reserved*

Table 378—Allowed cryptographic suites

Value	Description
0x000001	No data encryption, no data authentication & 3-DES, 128
0x010001	CBC-Mode 56-bit DES, no data authentication & 3-DES, 128
0x000002	No data encryption, no data authentication & RSA, 1024
0x020002	CBC-Mode 56-bit DES, no data authentication & RSA, 1024
0x020103	CCM-Mode 128-bit AES, CCM-Mode, 128-bit AES, ECB mode AES with 128-bit key
0x800003	MBS CTR Mode 128 bits AES with 32 bits nonce, no data authentication, AES ECB mode AES with 128-bit key
All remaining values	Reserved

[Change Table 377]

Table 377—TEK encryption algorithm identifiers

Value	Description
0	Reserved
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

[Change Table 378]

Table 378—Allowed cryptographic suites

Value	Description
0x000001	No data encryption, no data authentication & 3-DES, 128
0x010001	CBC-Mode 56-bit DES, no data authentication & 3-DES, 128
0x000002	No data encryption, no data authentication & RSA, 1024
0x0120002	CBC-Mode 56-bit DES, no data authentication & RSA, 1024
0x020103	CCM-Mode 128bits AES, CCM-Mode, ~~AES~~ ECB mode AES with 128-bit key
0x020104	CCM-Mode 128bits AES, CCM-Mode, AES Key Wrap with 128-bit key
0x800003	MBS CTR mode 128 bits AES~~ with 32 bits nonce~~, no data authentication, ~~AES~~ ECB mode AES with 128-bit key

0x800004	MBS CTR mode 128 bits AES, no data authentication, AES Key Wrap with 128-bit key
All remaining values	Reserved