Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**AES Key Wrap for TEK Exchange**
Date Submitted	**2004-7-7**
Source(s)	David Johnston Intel Corporation 2111 NE 25th Ave. Hillsboro 97124 Voice: +1 (503) 264-3855 [mailto:dj.johnston@intel.com]
Re:	IEEE 802.16e Security Adhoc
Abstract	Use of AES Key Wrap algorithm for TEK exchange
Purpose	To enable secure and FIPS approvable TEK key exchange.
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>.

AES Key Wrap for TEK Exchange

David Johnston

The AES key wrap algorithm is a NIST algorithm suitable for the encryption of keys for transportation.

This proposal describes how it may be used to encrypt a TEK.

Editor Instructions:
[Insert section 7.5.2.4]

7.5.2.4 Encryption of TEK-128 with AES Key Wrap

This method of encrypting the TEK-128 shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x04.

The BS encrypts the value fields of the TEK-128 in the Key Reply messages it sends to client SS. This field is encrypted using the AES Key Wrap Algorithm.

encryption: C,I = Ek[P]
decryption: P,I = Dk[C]
P = Plaintext 128-bit TEK
C = Ciphertext 128-bit TEK
I = Integrity Check Value
k = the 128-bit KEK
Ek[ ] = AES Key Wrap encryption with key k
Dk[ ] = AES Key Wrap decryption with key k

The AES key wrap encryption algorithm accepts both a ciphertext and an integrity check value. The decryption algorithm returns a plaintext key and the integrity check value. The default integrity check value in the NIST AES Key Wrap algorithm shall be used.

[Insert section reference]

‘http://csrc.nist.gov/CryptoToolkit/kms/key-wrap.pdf’ Draft NIST AES Key Wrap Specification.

[Insert the following delta to table 375 in the base document]

Insert into table 375 a new row and change the final row :

4	AES Key Wrap with 128-bit key
45-255	*reserved*

Insert a new row into table 376 – Allowed Cryptographic suites

0x020004	CCM Mode AES, no data authentication, AEK key wrap