Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Proposed New Clause 7.5**	
Date Submitted	**2001-09-06**	
Source(s)	Stanley Wang Ensemble Communications, Inc. 9890 Towne Centre Drive San Diego, CA 92121	Voice: (858) 625-7265 Fax: (858) 638-7142 mailto:stanley@ensemble.com
Re:	Call for comment on IEEE P802.16/D4-2001	
Abstract	This contribution contains a new proposed clause 7.5 to replace existing one in conjunction with a comment to replace DES and 3-DES by AES as the encrpytion standard.	
Purpose	A proposed new clause 7.5 to replace current cluase 7.5 in IEEE P802.16/D4-2001.	
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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Proposed New Clause 7.5

Stanley Wang
Ensemble Communications, Inc.

0.1 Cryptographic Methods

This section specifies the cryptographic algorithms and key sizes used by the PKM protocol. All BS and SS implementations shall support the method of packet data encryption/decryption specified in 7.5.1, encryption of TEKs specified in 7.5.2, message digest calculations specified in 7.5.3, derivation of keys specified in 7.5.4, authorization key encryption/decryption specified in 7.5.5, and digital signatures specified in 7.5.6.

0.1.1 Data Encryption with the Advanced Encryption Standard (AES)

If the Data Encryption Algorithm Identifier in the Cryptographic Suite of an SA equals 0x01, data on connections associated with that SA shall use the Cipher Block Chaining (CBC) mode of the Advanced Encryption Standard algorithm to encrypt and decrypt the MAC PDU payloads.

CBC mode of AES is a 128-bit (16-octet) block cipher which encrypts/decrypts data blocks (i.e., MAC PDU payloads) 16 octets at a time. It requires a 16-octet key and a 16-octet Initialization Vector (IV).

0.1.1.1 CBC Initialization Vector Calculation

The CBC IV shall be calculated using the IV parameter included in the TEK keying material along with the PHY Synchronization field in the DL maps as follows:

a) In the downlink, the CBC IV shall be initialized with the Exclusive-OR (XOR) of
   1) the random 128-bit IV parameter included in the TEK keying material, and
   2) the content of the PHY Synchronization field of the latest DL-MAP prepended with leading 0's for a total length of 128 bits.
b) In the uplink, the CBC IV shall be initialized with the XOR of
   1) the random 128-bit IV parameter included in the TEK keying material, and
   2) the content of PHY Synchronization field of the DL-MAP that is in effect when the UL-MAP for the uplink transmission is created/received prepended with leading 0's for a total length of 128 bits.

0.1.1.2 AES Block Cipher Processing

Block ciphers need to satisfy their respective block sizes and two issues can arise: (1) the MAC PDU payload (data block) may not be a multiple of the AES 128-bit block size, and (2) the MAC PDU payload (data block) may be less than the AES 128-bit block size. The first issue shall be handled by using ciphertext stealing and the second issue shall be handled by using padding.

When the MAC PDU payload is not a multiple of the AES 128-bit block size, Ciphertext Stealing shall be used to append the necessary number of octets to the final short block (or Residual Termination Block) prior to AES CBC encryption. Ciphertext stealing concatenates octets from the previous ciphertext block to the plaintext of the short block when the final block is less than 128 bits. The BS or SS shall concatenate the appropriate number of octets to the final short block to make it 128 bits in length prior to AES CBC encryption. For example, if the final short block is ABCDEFABCDEFABCD (8 octets) and the last ciphertext block is AABBCCDDEEFF0102030405060708, then 8 octets are needed from the last ciphertext block and these are appended to the final short block. The new ciphertext

stealing final block then becomes ABCDEFABCDEFABCD0102030405060708 prior to AES CBC encryption. Refer to Figure 9.5 of [B17] for additional discussion of Ciphertext Stealing in CBC mode.

When the special case of a MAC PDU payload being less than 128 bits is encountered, padding shall be used to make the block 128 bits in length prior to AES CBC encryption. Padding shall use the third method described in [FIPS-yyy] known as redundancy padding (also described in [RFC-2630]). Let *B* be the number of octets in the data blocks (for AES, *B* = 16) and *L* be the number of octets in the data string. The data string is padded at the trailing end with $B - (L \bmod B)$ octets, each of which is the binary representation of $B - (L \bmod B)$. See [FIPS-yyy] or [RFC-2630] for further details. Note that there are two conditions for using this method: the data blocks and the data string must be expressible in octets, i.e., their lengths are a multiple of 8 bits, and *B* must satisfy $2 \le B \le 256$.

0.1.2 Calculation of HMAC Digests

The calculation of the keyed hash in the HMAC-Digest attribute and the HMAC Tuple shall use the HMAC [RFC-2104] with the SHA-1 hash algorithm [FIPS-180-1].

The downlink authentication key HMAC_KEY_D shall be used for authenticating messages in the downlink direction. The uplink authentication key HMAC_KEY_U shall be used for authenticating messages in the uplink direction. Uplink and downlink message authentication keys are derived from the Authorization Key (see 7.5.4 below for details).

The HMAC Sequence Number in the HMAC Tuple shall be equal to the AK Sequence Number of the AK from which the HMAC_KEY_D/U was derived.

The digests shall be calculated over the entire MAC management message with the exception of the HMAC-Digest and HMAC Tuple attributes.

0.1.3 Derivation of TEKs, KEKs and Message Authentication Keys

The BS shall generate Authorization Keys (AKs), Traffic Encryption Keys (TEKs) and Initialization Vectors (IVs) using a random or pseudo-random number generator. Regardless of the method used to generate IVs, IVs shall be unpredictable.

[B9] provides recommended practices for generating random or pseudo-random numbers for use within cryptographic systems.

0.1.3.1 AES Keys

The AES key size (i.e., the key size for TEKs) shall be 128 bits (16 octets) and the AES block size shall be 128 bits (16 octets). The BS shall generate the 128-bit (16-octet) IV using a random or pseudorandom number generator which should satisfy the unpredictability requirement discussed in, for example, [B9].

0.1.3.2 KEK with the Advanced Encryption Standard

TEKs shall be encrypted by the Electronic CodeBook (ECB) mode of AES prior to being sent to the SS.

The 128-bit key needed for AES is called the Key Encryption Key (KEK) and the KEK shall be used to encrypt the TEK on the BS and to decrypt the TEK on the SS.

The KEK shall be derived from the active AK as follows:

KEK = Truncate(SHA(K_PAD_KEK | AK), 128)
K_PAD_KEK = 0x53 repeated 64 times, i.e., a 512-bit string

Truncate(*x*, *n*) denotes the result of truncating *x* to its most significant *n* bits. SHA(*x*| *y*) denotes the result of applying the SHA-1 [FISP-180-1] function to the concatenated bit strings *x* and *y.* Every time a new AK is being activated, the KEK shall use that AK for generating the KEK.

0.1.3.3 HMAC Message Authentication Keys

The HMAC message authentication keys are derived as follows:

HMAC_KEY_D = SHA(H_PAD_D | AK)
HMAC_KEY_U = SHA(H_PAD_U | AK)

with

H_PAD_D = 0x3A repeated 64 times
H_PAD_U = 0x5C repeated 64 times.

SHA(*x*|*y*) denotes the result of applying the SHA-1 [FISP-180-1] function to the concatenated bit strings *x* and *y.*

0.1.4 Public-Key Encryption of Authorization Key

Authorization keys in Authorization Reply messages shall be RSA public-key encrypted, using the SS's public key. The protocol shall use 65537 (0x010001) as its public exponent and a modulus length of 1024 bits. The PKM protocol employs the RSAES-OAEP encryption/decryption scheme specified in version 2.0 of the PKCS#1 standard [RSA]. RSAES-OAEP requires the selection of a hash function, a mask-generation function, and an encoding parameter string. The default selections specified in [RSA], which are SHA-1 for the hash function, MGF1 with SHA-1 for the mask-generation function, and the empty string for the encoding parameter string, shall be used when encrypting the authorization key.

0.1.5 Digital signatures

The PKM protocol employs the RSA Signature Algorithm [ANSI X9.31-1998] with SHA-1 [FIPS-180-1] for the Manufacturer and SS certificate types as defined per the Digital Signature Standard (DSS) [FIPS-186-2].

As with RSA encryption keys, the digital signature shall use 65537 (0x010001) as the public exponent for all signature operations.

The Manufacturer Certification Authority (CAs) shall employ signature key modulus lengths of at least 1024 bits, and no greater than 2048 bits for signing the SS certificates it issues. The Manufacturer CA itself shall be considered a self-signed certificate. Certificates shall conform to ANSI X.509 V.3 and RFC-2459 as discussed in 7.6 below.

All keying material, generation of keys, testing of keys, signing operations and signing validation shall be in conformance to DSS [FIPS-186-2] and RSA Signature Algorithm [ANSI X9.31-1998].