

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >	
Title	AES-CCM Encryption and Authentication Mode for 802.16	
Date Submitted	2004-01-10	
Source(s)	David Johnston Intel Corp 2111 NE 25 th Avenue Hillsboro, OR 97124-5961	Voice: 503 264 3855 Fax: mailto:dj.johnston@intel.com
Re:	802.16e	
Abstract	This document describes changes to the 802.16 specification, for incorporation into the 802.16e amendment. These changes introduce a new encryption algorithm, authentication algorithm and key encryption algorithm based on AES operating in CCM mode. This new mode is incorporated into the extensible cipher selector mechanism that exists in the base specification.	
Purpose	These changes are to be incorporated into 802.16e in order to enhance the available cryptographic strength of the link cipher to 128 bits and to introduce data origin authentication and data integrity protection.	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding 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-CCM Encryption and Authentication Mode for 802.16

*David Johnston
Intel Corp*

**Copyright ©2002 Institute of Electrical and Electronics Engineers, Inc.
Reprinted, with permission, from [all relevant journal info].**

This material is posted here with permission of the IEEE. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE (contact pubs-permissions@ieee.org).

By choosing to view this document, you agree to all provisions of the copyright laws protecting it.

[Figure 1, Replace both instances of ‘Privacy Sublayer’ with ‘Security Sublayer’].

[1.4, Replace ‘Privacy Sublayer’ with ‘Security Sublayer’]

[2. References, Insert the following references]

FIPS 197, Advanced Encryption Standard (AES)

NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Model for Authentication and Confidentiality

[4. Abbreviations and Acronyms, Insert the following abbreviations]

AES Advanced Encryption Standard

CCM CTR mode with CBC-MAC

CBC-MAC Cipher Block Chaining Message Authentication Code

CTR Counter mode encryption

[Amend 6.4.3.6 as follows]

6.4.3.6 Cryptographic Protection of MAC PDUs

Deleted: Encryption

When transmitting a MAC PDU on a connection that is mapped to an SA, the sender shall perform encryption and data authentication of the MAC PDU payload as specified by that SA. When receiving a MAC PDU on a connection mapped to an SA, the receiver shall perform decryption and data authentication of the MAC PDU payload, as specified by that SA.

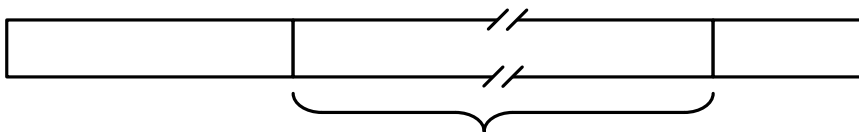
The generic MAC header shall not be encrypted. The Header contains all the information [EC Field, encryption key sequence (EKS) Field, and CID] needed to decrypt and/or authenticate a Payload at the receiving station. This is illustrated in Figure 32.

Deleted: NOTE—Data authentication is not currently defined.¶

Deleted: Encryption

Two bits of a MAC Header contain a key sequence number. Note that the keying material associated with an SA has a limited lifetime, and the BS periodically refreshes an SA’s keying material. The BS manages a 2 bit key sequence number independently for each SA and distributes this key sequence number along with the SA’s keying material to the client SS. The BS increments the key sequence number with each new generation of keying material. The MAC Header includes this sequence number to identify the specific generation of that SA keying material being used to encrypt the attached payload. Being a 2-bit quantity, the sequence number wraps around to 0 when it reaches 3.

Formatted: Font: (Default) TimesNewRoman, 10 pt



Generic MAC r

Figure 32—MAC PDU encryption

Deleted:

Comparing a received MAC PDU's key sequence number with what it believes to be the "current" key sequence number, an SS or BS can easily recognize a loss of key synchronization with its peer. An SS shall maintain the two most recent generations of keying material for each SA. Keeping on hand the two most recent key generations is necessary for maintaining uninterrupted service during an SA's key transition.

Protection of the payload is indicated by the EC bit field. A value of 1 indicates the payload is cryptographically protected and the EKS field contains meaningful data. A value of 0 indicates the payload is not cryptographically protected. A PDU with no payload shall not be protected. Any unencrypted MAC PDU received on a connection mapped to an SA requiring encryption shall be discarded unless the PDU contains no payload.

- Deleted: Encryption
- Deleted: encrypted
- Deleted: encrypted

[Amend clause 7 as follows]

7. Security sublayer

Deleted: Privacy

The security sublayer provides subscribers with privacy, authentication or confidentiality¹⁵ across the broadband wireless network. It does this by applying cryptographic transforms to MPDUs carried across connections between SS and BS.

- Deleted: Privacy
- Deleted: fixed
- Deleted: ¶ encrypting
- Deleted: Privacy
- Deleted: enforcing encryption of
- Deleted: Privacy
- Deleted: basic privacy

In addition, security provides operators with strong protection from theft of service. The BS protects against unauthorized access to these data transport services by securing the associated service flows across the network. Security employs an authenticated client/server key management protocol in which the BS, the server, controls distribution of keying material to client SS. Additionally, the transport connection security mechanisms are strengthened by adding digital-certificate-based SS device-authentication to its key management protocol.

7.1 Architecture

Security has two component protocols as follows:

Deleted: Privacy

- a) An encapsulation protocol for securing packet data across the BWA network. This protocol defines (1) a set of supported *cryptographic suites*, i.e., pairings of data encryption and authentication algorithms, and (2) the rules for applying those algorithms to a MAC PDU payload.
- b) A key management protocol (PKM) providing the secure distribution of keying data from BS to SS. Through this key management protocol, SS and BS synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services.

- Deleted: encrypting
- Deleted: fixed

7.1.1 Packet data encryption

Encryption services are defined as a set of capabilities within the MAC Security Sublayer. MAC Header information specific to encryption is allocated in the generic MAC header format.

Deleted: Privacy

Encryption is applied to the MAC PDU payload when required by the selected ciphersuite; the generic MAC header is not encrypted. All MAC management messages shall be sent in the clear to facilitate registration, ranging, and normal operation of the MAC.

Deleted: always

The format of MAC PDUs carrying secured packet data payloads is specified in 6.4.3.6.

Deleted: encrypted

¹⁵ In security parlance, confidentiality = privacy + authenticity

7.1.2 Key management protocol

An SS uses the PKM protocol to obtain **device** authorization and traffic keying material from the BS, and to support periodic reauthorization and key refresh. The key management protocol uses X.509 digital certificates [IETF RFC 3280], the RSA public-key encryption algorithm [PKCS #1], and strong symmetric algorithms to perform key exchanges between SS and BS.

The PKM protocol adheres to a client/server model, where the SS, a PKM “client,” requests keying material, and the BS, a PKM “server,” responds to those requests, ensuring that individual SS clients receive only keying material for which they are authorized. The PKM protocol uses MAC management messaging, i.e., PKM-REQ and PKM-RSP messages defined in 6.4.2.3.

The PKM protocol uses public-key cryptography to establish a shared secret (i.e., an AK) between SS and BS. The shared secret is then used to secure subsequent PKM exchanges of TEKs. This two-tiered mechanism for key distribution permits refreshing of TEKs without incurring the overhead of computation intensive public-key operations.

A BS authenticates a client SS during the initial authorization exchange. Each SS carries a unique X.509 digital certificate issued by the SS’s manufacturer. The digital certificate contains the SS’s Public Key and SS MAC address. When requesting an AK, an SS presents its digital certificate to the BS. The BS verifies the digital certificate, and then uses the verified Public Key to encrypt an AK, which the BS then sends back to the requesting SS.

The BS associates an SS’s authenticated identity to a paying subscriber, and hence to the data services that subscriber is authorized to access. Thus, with the AK exchange, the BS establishes an authenticated identity of a client SS and the services (i.e., specific TEKs) the SS is authorized to access.

Since the BS authenticates the SS, it can protect against an attacker employing a *cloned* SS, masquerading as a legitimate subscriber’s SS. The use of the X.509 certificates prevents cloned SSs from passing fake credentials onto a BS.

All SSs shall have factory-installed RSA private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If an SS relies on an internal algorithm to generate its RSA key pair, the SS shall generate the key pair prior to its first AK exchange, described in 7.2.1. All SSs with factory-installed RSA key pairs shall also have factory-installed X.509 certificates. All SSs that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer-issued X.509 certificate following key generation.

The PKM protocol is defined in detail in 7.2.

7.1.3 Security Associations

A *Security Association* (SA) is the set of security information a BS and one or more of its client SSs share in order to support secure communications across the IEEE Std 802.16 network. Three types of SAs are defined: *Primary*, *Static*, and *Dynamic*. Each SS establishes a Primary Security association during the SS initialization process. Static SAs are provisioned within the BS. Dynamic SAs are established and eliminated, on the fly, in response to the initiation and termination of specific service flows. Both Static and Dynamic SAs can be shared by multiple SSs.

An SA’s shared information shall include the Cryptographic Suite employed within the SA. The shared information may include TEKs and Initialization Vectors. The exact content of the SA is dependent on the SA’s Cryptographic Suite.

SAs are identified using SAIDs.

Each SS shall establish an exclusive Primary SA with its BS. The SAID of any SS's Primary SA shall be equal to the Basic CID of that SS.

Using the PKM protocol, an SS requests from its BS an SA's keying material. The BS shall ensure that each client SS only has access to the SAs it is authorized to access.

An SA's keying material [e.g., Data Encryption Standard (DES) key and CBC Initialization Vector] has a limited lifetime. When the BS delivers SA keying material to an SS, it also provides the SS with that material's remaining lifetime. It is the responsibility of the SS to request new keying material from the BS before the set of keying material that the SS currently holds expires at the BS. Should the current keying material expire before a new set of keying material is received, the SS shall perform network entry as described in 6.4.9.

In certain ciphersuites, key lifetime may be limited by the exhaustion rate of a number space [e.g. the PN (Packet Number) in AES-CCM mode]. In this case, the key ends either at the expiry of the key lifetime or the exhaustion of the number space, which ever is earliest. Note that in this case, security is not determined by the key lifetime.

▼ The PKM protocol specifies how SS and BS maintain key synchronization.

Deleted:

7.2 PKM protocol

7.2.2 TEK exchange overview

7.2.2.1 TEK exchange overview for PMP topology

Upon achieving authorization, an SS starts a separate TEK state machine for each of the SAIDs identified in the Authorization Reply message. Each TEK state machine operating within the SS is responsible for managing the keying material associated with its respective SAID. TEK state machines periodically send Key Request messages to the BS, requesting a refresh of keying material for their respective SAIDs.

The BS responds to a Key Request with a Key Reply message, containing the BS's active keying material for a specific SAID.

TEKs and KEKs may be either 64 bits or 128 bits long. SAs employing any ciphersuite with a basic block size of 128 bits shall use 128 bit TEKs and KEKs. Otherwise 64 bit TEKs and KEKs shall be used. The name TEK-64 is used to denote a 64 bit TEK and TEK-128 is used to denote a 128 bit TEK. Similarly, KEK-64 is used to denote a 64 bit KEK and KEK-128 is used to denote a 128 bit KEK.

For SAs using a ciphersuite employing DES-CBC the TEK in the Key Reply is triple DES (3-DES) (encrypt-decrypt-encrypt or EDE mode) encrypted, using a two-key, 3-DES KEK derived from the AK.

Deleted: T

For SAs using a ciphersuite employing 128 bits keys, such as AES-CCM mode, the TEK in the key Reply is AES encrypted using a 128 bit key derived from the AK and a 128 bit block size.

Note that at all times the BS maintains two active sets of keying material per SAID. The lifetimes of the two generations overlap such that each generation becomes active halfway through the life of its predecessor and expires halfway through the life of its successor. A BS includes in its Key Replies *both* of an SAID's active generations of keying material.

