Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**AES-CCM Text clarification**	
Date Submitted	**2004-08-17**	
Source(s)	JUNHYUK SONG, YONG CHANG, JICHEOL LEE Samsung Electronics	Voice: +82-31-279-3639 junhyuk.song@samsung.com Voice: +82-31-279-3639 jicheol.lee@samsung.com
Re:	IEEE P802.16e/D4-2004	
Abstract	Proposal for AES-CCM text change	
Purpose	Review and Adopt the suggested changes into P802.16e/D4	
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-CCM clarification

JUNHYUK SONG, YONG CHANG,JICHEOL LEE
Samsung Electronics

Introduction

AES-CCM has defined in addition to DES-CBC, however in current text there are some ambiguities needed to clear up. In this contribution we propose to change following

- “Little-endian” byte ordering specified for PN and ICV to big-endian ordering

Byte Ordering

802.16 specified big-endian byte ordering in Generic MAC header (see figure 1), and it is a basic assumption for packet format and other attribute has more than one octet. However AES-CCM specified little-endian ordering for PN and ICV. It is because AES-CCM specification specify initial block B0 and Ai in little-endian order (see figure 1). It is desirable to have big-endian byte ordering for PN and ICV for sake of consistency with GMH and other packet formats

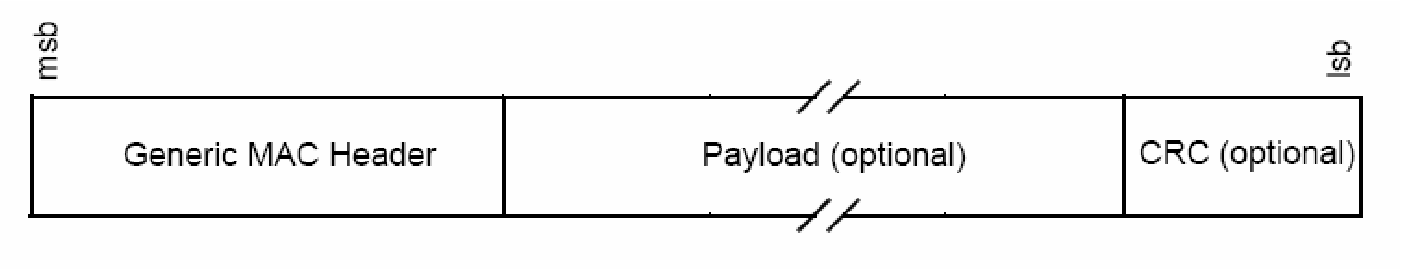
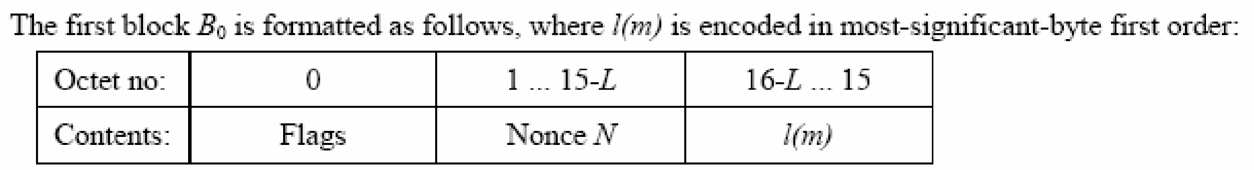


Figure 21—MAC PDU formats

Figure-1 MAC PDU formats



The first block B_0 is formatted as follows, where *l(m)* is encoded in most-significant-byte first order:

Octet no:	0	1 ... 15-*L*	16-*L* ... 15
Contents:	Flags	Nonce *N*	*l(m)*

Figure-2 (Initial Block B0 specified in NIST SP 800-38C)

Proposed Text

7.5.1.2.1 PDU Payload Format

The PDU Payload shall be prepended with a 4 byte PN (Packet Number). The PN shall be transmitted in big~~little~~ endian byte order. The PN shall not be encrypted.

The plaintext PDU shall be encrypted and authenticated using the active TEK, according to the CCM specification. This includes appending an 8 bytre ICV (Integrity Check Value) to the end of the payload and encrypting the both the plaintext payload and the appended ICV.

The ciphertext ICV is transmitted in big~~little~~ endian byte order.

The processing yields payload that is 12 bytes longer than the plaintext payload.