Project | **IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>  
---|---  
Title | Minor corrections for AES-CCM  
Date Submitted | **2005-03-17**  
Source(s) | Joël Demarty  
SEQUANS Communications. joel@sequans.com  
Ambroise Popper  
SEQUANS Communications ambroise@sequans.com  
Jeff Mandin  
Streetwaves Networking  
Amatzia 5  
Jerusalem, Israel jeff@streetwaves-networks.com  
Re: | IEEE P802.16REVd/D5-2004  
Abstract | Minor corrections for AES-CCM  
Purpose | Adopt changes.  
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>.  

Minor corrections in AES-CCM mode
Joël Demarty, Ambroise Popper (SEQUANS Communications)
Jeff Mandin (Streetwaves Networking)

1. Introduction
There are some minor errors/consistencies to be made to the description of the AES-CCM mode.

2. Text changes
[Replace the content of section 7.5.1.2.1 as indicated]

Change the first and third paragraph as indicated:

The PDU payload shall be prepended with a 4-byte PN (Packet Number). The PN shall be transmitted in little endian LSB first byte order. The PN shall not be encrypted. The ciphertext ICV is transmitted in little endian LSB first byte order.

[Modify figure 135 of 7.5.1.2.1 as follows]

Payload before encryption

L bytes

Plaintext before encryption

PDU after encryption Payload after encryption

6+L+12 Bytes

<table>
<thead>
<tr>
<th>Generic Mac Header</th>
<th>PN</th>
<th>Ciphertext payload</th>
<th>ICV</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>←  Security Header →</td>
<td>← Security Trailer →</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 135—Encrypted PDU format in AES-CCM mode

[Replace the content of section 7.5.1.2.2 page 33 as indicated]

Change the first sentence of the first paragraph as indicated:

The PN associated with an SA shall be set to 1 when the SA is established and when a new TEK is installed. The PN shall be transmitted in little endian LSB first order in the MAC PDU as described in 7.5.1.2.1.
7.5.1.2.3 802.16 Profile of CCM Algorithm

Change section 7.5.1.2.3 as indicated:

The NIST CCM specification defines a number of algorithm parameters. These parameters shall be fixed to specific values when used in SAs with a data encryption algorithm identifier of 0x02.

The number of octets in the message authentication code field $M$ shall be set to 8. Consistent with the CCM specification the 3 bit binary encoding of $M$ shall be 011.

The size $q$ of the length field $L$ shall be set to 2. Consistent with the CCM specification, the 3-bit binary encoding of the $q$ field shall be 001.

The length $a$ of the additional authenticated data string $l(a)$ shall be set to 0.

The nonce shall be 13 bytes long as shown in figure 135a. Bytes 0 through 4 shall be set to the first five byte of the Generic MAC Header GMH (thus excluding the HCS). The sixth byte of the Generic MAC Header is not included in the nonce since it is redundant. Bytes 5 through 8 are reserved and shall be set to 0x00000000. Bytes 9 through 12 shall be set to the value of the PN encoded in LSB first byte order. Byte 10 shall take the least significant byte and byte 13 shall take the most significant byte.

[Add figure 135a]

Consistent with the CCM specification, the initial block $B_0$ is formatted as shown in Figure 136.
Figure 136—Initial CCM Block $B_0$

Note the big-endian MSB first ordering of the DLEN $L$ value is opposite that of the normal little-endian LSB first representation.
This is to remain compliant with the letter of the NIST CCM specification.
The sixth byte of the GMH is not included in the nonce since it is redundant.

Consistent with the NIST CCM specification the counter blocks $C_{trAi}$ are formatted as shown in Figure 137.

<table>
<thead>
<tr>
<th>Byte number within CTR(i)</th>
<th>0</th>
<th>1...13</th>
<th>14...15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>1</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>Flag</td>
<td></td>
<td>Nonce</td>
<td>Counter</td>
</tr>
<tr>
<td>Contents</td>
<td>0x01</td>
<td>As specified in figure XXX</td>
<td>$i$ Length of data part not including padding</td>
</tr>
</tbody>
</table>

Figure 136—Construction of counter blocks $C_{trAi}$