| | | |
|---|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** | |
| Title | Minor corrections for AES-CCM | |
| Date Submitted | **2005-03-15** | |
| Source(s) | Joël Demarty<br>SEQUANS Communications. | joel@sequans.com |
| | Ambroise Popper<br>SEQUANS Communications | ambroise@sequans.com |
| | Jeff Mandin<br>Streetwaves Networking<br>Amatzia 5<br>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

[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

| Generic Mac Header | PN← | Ciphertext payload | ICV← | CRC |
|---|---|---|---|---|
| | ← Security Header → | | ← Security Trailer → | |

Figure 135—Encrypted PDU format in AES-CCM mode~~TEK management in BS and SS~~

[Modify 7.5.1.2.3 as follows]

**7.5.1.2.3** 802.16 Profile of **CCM Algorithm**

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 t~~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 XXX. 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 MSB first byte order. ~~Byte 10 shall take the least significant byte and byte 13 shall take the most significant byte~~

[Add figure XXX]

| Byte Number | 0…4 | 5…8 | 9…12 |
|---|---|---|---|
| Field | GMH | Reserved | PN |
| Contents | Generic MAC Header without the trailing HCS | 0x00000000 | packet number field from payload |

Figure XXX – Format of the Nonce

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

| Byte number ~~within MIC_IV Byte significance~~ | 0 | 1…13 | 14…15 |
|---|---|---|---|
| Bytes | 1 | 13 | 2 |
| Field | Flag | Nonce→ | L ~~DLEN~~ ←- |
| Contents | 0x19 | As specified in figure XXX | Length of *plaintext payload* ~~data part not including padding~~ |

Figure 136—Initial CCM Block $B_0$

~~Note the big endian ordering of the DLEN value is opposite that of the normal little endian 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 $Ctr_i$ ~~Ai~~ are formatted as shown in Figure 137.

| Byte number ~~within CTR(i) Byte significance~~ | 0 | 1…13 | 14…15 |
|---|---|---|---|
| Bytes | 1 | 13 | 2 |
| Field | Flag | Nonce | C*ounter* ←- |

| | | | |
|---|---|---|---|
| Contents | 0x01 | As specified in figure XXX | *i* ~~Length of data part not includir padding~~ |

Figure 136—Construction of counter blocks $Ctr_i$ ~~Ai~~