Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**>	
Title	CCM Endianess Disambiguation	
Date Submitted	2005-05-03	
Source(s)	David Johnston Intel Corporation Joel Demarty, Ambroise Popper SEQUANS Communications	Voice: (503) 264 3855 Email: dj.johnston@intel.com Voice : +33144894807 Email: joel@sequans.com, ambroise@sequans.com
Re:	Letter Ballot #17a, P802.16-2004/Cor1/D2	
Abstract		
Purpose	This document corrects out of scope text and resolves an abiguity in the D1 corrigendum text	
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>.	

CCM Endianess Disambiguation

David Johnston, Intel Corporation
Joël Demarty, Ambroise Popper, SEQUANS Communications

1 Introduction

PN and ICV ordering

Changes to clause 7.5.1.2.1 and 7.5.1.2.2 in the corrigendum draft 1 replace ‘little endian’ with ‘MSB first’ for both the PN and ICV fields.

Figure 136 in the base document also describes the ordering of the bytes in the PN and ICV fields. However this is inconsistent with the new text.

In either case (little endian or big endian) the meaning with respect to the ICV in the NIST CCM and AES specifications could be misconstrued.

These problems can be fixed either by amending figure 136 to resolve the ambiguities, or by undoing the reversal of the ordering of the PN and ICV octets in 7.5.1.2.1 and 7.5.1.2.2 and expressing the order of transmission of the ICV bytes in terms of the byte index (0-15) used in the AES and CCM specifications.

The security of the CCM mode is not affected by the ordering decision; however the ordering must be the same between systems for them to interwork. Thus the existing text in the base document is not in error.

Accordingly, the change in to the base document corrects neither an error, inconsistency nor ambiguity. So it is out of scope for the text in 7.5.1.2.1 and 7.5.1.2.2 to be changed in the fashion currently in the corrigendum draft. This means that of the two options for fixing the corrigendum, the only one open to us is to remove the changes to 7.5.1.2.1 and 7.5.1.2.2 and resolve any ambiguities, thus restoring consistency in the text and removing the out of scope changes. Changing the order of transmission is not an in-scope option.

Also the comment that led to the changes in 7.5.1.2.1 and 7.5.1.2.2 is classified as editorial. This is not correct, the changing of the transmission order is very much a technical change.

Test Vectors to Resolve Ambiguities

Taken as it stands, may still be possible to make multiple interpretations of the text. Existing practice in implementing CCM in other 802 documents (802.11i) leads to the intended interpretation, however this is not expressed directly in the spec.

One way of disambiguating between all possible interpretations is to write a lot more clarifying text about every bit field and byte field. A much simpler way to disambiguate the text is to show example enciphered packets along with their plain text. This document proposes such text.

Consistency with NIST SP 800-38C

Between the NIST draft CCM specification referenced in 802.16-2004 and the subsequently published final CCM standard SP 300 38C, the names of parts of the CCM standard were changed. E.G. the ICV is now the Message Authentication Code. We cannot use 'MAC', since the term is already defined in 802. Contribution C80216maint-05/024 corrects for these changes and provides alternatives for figure 135 and 136. However document 024 assumes the big endian PN ordering of Corr1/D1. Also there were some minor technical errors, E.G. the rounding of the PDU length in figure 135 and the inclusion of the CRC in the payload example. Appropriate changes from proposal 024 have been included in the proposed text, but alterations have been made to address the above problems.

2 Proposed Text Changes

[Resolution Part 1]

[Modify the changed against section 7.5.1.2.1 to be as follows]

7.5.1.2 Data encryption with AES in CCM mode
7.5.1.2.1 PDU Payload Format

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 LSB First~~in little endian byte order~~. The PN shall not be encrypted. The ciphertext ~~ICV~~Message Authentication Code is transmitted such that byte index 0 (as enumerated in the NIST AES Specification) is transmitted first and byte index 7 is transmitted last (i.e. LSB First).~~ in little endian byte order.~~

[Replace the changes to section 7.5.1.2.2 from the corrigendum draft to be as follows]

7.5.1.2.2 PN (Packet Number)

Modify 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 in the MAC PDU as described in 7.5.1.2.1.~~ After each PDU transmission, the PN shall be incremented by 1. On uplink connections, the PN shall be XORed with 0x80000000 prior to encryption and transmission. On downlink connections, the PN shall be used without such modification.[16]

[Resolution Part 2]

[Replace "Ciphertext ICV" in figure 135 with "Ciphertext Message Authentication Code"]

~~Ciphertext ICV~~Ciphertext Message Authentication Code

[Modify Labeling of Figure 135 in 7.5.1.2.1 as follows]

Figure 135 –~~TEK Management in BS and SS~~ Encrypted Payload Format in AES-CCM Mode

[Modify 7.5.1.2.3 as follows]

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.

‘*Tlen*’ shall equal 64 and t shall equal 8, meaning, the ~~The~~ number of ~~octet~~ bytes in the Message Authentication Code field ~~authentication field M~~ shall be set to 8. Consistent with the CCM specification the 3 bit binary encoding $[(t\text{-}2)/2)]_3$ of ~~M~~ bits 5, 4 and 3 of the ‘Flags’ byte in B_0 shall be 011.

The size q of the length field Q shall be set to 2. Consistent with the CCM specification, the 3-bit binary encoding $[q\text{-}1]_3$ of the q field in bits 2, 1 and 0 of the ‘Flags’ byte in B_0 shall be 001.

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

The nonce shall be 13 bytes long as shown in figure 135a. Bytes 0 through 4 ~~1 through 5~~ shall be set to the first five bytes of the Generic MAC Header ~~GMH~~ (thus excluding the HCS). The HCS of the Generic MAC Header is not included in the nonce since it is redundant. Bytes 5 through 8 ~~Bytes 6 through 9~~ are reserved and shall be set to 0x00000000. ~~Bytes 10 through 13~~ Bytes 9 through 12 shall be set to the value of the PN. The PN Bytes shall be ordered such that Byte 9 ~~10~~ shall take the least significant byte and byte 12 ~~13~~ shall take the most significant byte.

Byte Number	0 ... 4	5 ... 8	9 ... 12
Field	Generic MAC Header	Reserved	PN
Contents	Generic Mac Header omitting HCS	0x00000000	packet number field from payload

Figure 135a Nonce N Construction

[Modify 136 and following text of 7.5.1.2.1 to be as follows. Delete Other features of figure 136]

~~Byte within MIC_IV~~ Byte Number	0	1 13	14 15
Byte Significance			MSB LSB
Number of Bytes	1	13	2
Field	Flag	Nonce	*L*~~DLEN~~
Contents	0x19	As Specified in Figure 135a	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 big endian , consistent ~~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 ~~A_i~~ are formatted as shown in Figure 137.

[Modify Figure 137of 7.5.1.2.1 as follows. Delete other features of figure 137]

~~Byte within *CTRi*~~ Byte Number	0	1 13	14 15
Byte Significance			MSB LSB
Number of Bytes	1	13	2
Field	Flag	Nonce	C*ounter*
Contents	0x01	As Specified in Figure 135a	*i* ~~Length of data part not including padding~~

Figure 137 – Construction of counter blocks Ctr_j ~~A_i~~

[Resolution Part 3]

[Insert a new section 7.5.1.2.5 "AES-CCM Mode Example Encrypted MPDUs"]

7.5.1.2.5 AES-CCM Mode Cryptographic Method Examples

The following two examples show 802.16 MPDUs in both plaintext and enciphered form in transmission order. In addition, the post-decryption plaintext of the Message Authentication Code is shown.

Example AES-CCM PDU #1

Plaintext PDU

Generic MAC Header = `00 40 0A 06 C4 30`

Payload = `00 01 02 03`

Ciphertext PDU where TEK = 0xD50E18A844AC5BF38E4CD72D9B0942E5 and PN=0x2157F6BC

Generic MAC Header = `40 40 1A 06 C4 5A`

PN Field = `BC F6 57 21`

Encrypted Payload = `E7 55 36 C8`

Encrypted Message Authentication Code =
`27 A8 D7 1B 43 2C A5 48`

CRC = `CB B6 5F 48`

After Decryption

Plaintext Message Authentication Code =
`01 59 09 A0 ED CC 21 D3`

Example AES-CCM PDU #2

Plaintext PDU

Generic MAC Header = `00 40 27 7E B2 AD`

Payload =
```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20
```

Ciphertext PDU where TEK = 0xB74EB0E4F81AD63D121B7E9AECCD268F and PN=0x78D07D08

Generic MAC Header = `40 40 37 7E B2 C7`

PN Field = `08 7D D0 78`

Encrypted Payload =
```
71 3F B1 22 B9 73 4F DB FD 68 2E AD 9D CA 9F 44
1F 62 FE 0F 4A 2C 45 B5 53 17 3D 66 5B 2D 53 C1
B3
```

Encrypted Message Authentication Code =
`E7 E4 8D 2D B7 61 CF 94`

CRC = `92 1B 32 41`

After Decryption

Plaintext Message Authentication Code =
`0B DB 85 3C 0A CA E6 5F`