Project	IEEE 802.16 Broadband Wireless Access Working Group <*http://ieee802.org/16*>	
Title	Truncate() function clarifications	
Date Submitted	2006-09-26	
Source(s)	Walter Goulet, Mark Cudak	Voice: +1 847 576 7036 Walter.goulet@motorola.com
Re:	Clarifications to the Truncate() function referenced in IEEE Std. 802.16	
Abstract	This contribution address an ambiguity in the definitions given for the Truncate() function which is used several places in the standard for key derivation. Additionally, this contribution replaces the use of 'rightmost' and 'leftmost' bits in the key derivation functions with different terms and specifies the endianess of the bits within a byte to insure that all conforming implementations will interpret the functions identically.	
Purpose	Adopt proposed 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>.	

Clarifications to the Truncate() function referenced in IEEE Std. 802.16

Walter Goulet (Motorola)

Problem Definition

In general, the definition of the Truncate() function in IEEE Std. 802.16 is inconsistent. IEEE 802.16d-2004 includes a definition of the 'Truncate' in this section that is different than the definition given by 802.16e-2005 on page 309 section 7.5.4.6.1. The definition given for 'Truncate' should be identical in all places in the spec. Additionally, the terms ‘rightmost and leftmost bits’ are ambiguous since they can be interpreted differently depending on byte endianness. Finally, reference is made to a function ‘Truncate64’. This reference is unnecessary since the intended functionality is more appropriately expressed in terms of the existing ‘Truncate’ function.

Remedy

Change #1

Section Number: Section 7.5
Insert the following text in section 7.5

All inputs to key derivation and other supporting functions must be byte aligned. Furthermore, each byte must be in canonical form as defined in IEEE Std. 802-2001 where the leftmost bit in each byte is the most significant bit and the rightmost bit is the least significant bit.

Change #2
Section Number: Section 7.5.4.2
Page Number: 305

Line Number: 6

Replace line 6 in section 7.5.4.2 (from 802.16d-2004) with the following lines in section 7.5.4.2 :
~~Truncate(*x*,*n*) denotes the result of truncating *x* to its leftmost *n* bits~~.

Truncate(x,y) is defined as the last 'y' bits of x if and only if y <=x. The values ‘x’ and ‘y’ must be aligned to byte boundaries.

The following examples illustrate the expected output of Truncate given inputs for ‘x’ in hexadecimal, decimal, and binary:

Hex:
Truncate(0x66,0x2) = 0x2
Truncate(0x65,0x2) = 0x1

Decimal:
Truncate(102,2) = 2
Truncate(101,2) = 1

Binary:
Truncate(1100110,10) = 10
Truncate(1100101,10) = 01

Change #3
Section Number: 7.5.4.2 (from 802.16d-2004)
Page Number: 300
Line Number: last 2 lines in section

Replace last 2 lines in section 7.5.4.2 (from 802.16d-2004) with the following lines in section 7.5.4.2 of 802.16e-2005:

~~The keying material of 3-DES consists of two distinct DES keys. The 64 most significant bits of the KEK~~
~~shall be used in the encrypt operation. The 64 least significant bits shall be used in the decrypt operation.~~

The keying material of 3-DES consists of two distinct DES keys. The most significant 64 bits of the KEK
shall be used in the encrypt operation. The least significant 64 bits shall be used in the decrypt operation.

Example:
KEK=0xAB CD 12 34 DC BA 43 21 12 34 DC BA AB AC BC BD
Encypt Key = 0xAB CD 12 34 DC BA 43 21, where 0xAB = 10101011, 0xCD = 11001101 and so on
Decrypt Key = 0x12 34 DC BA AB AC BC BD

Change #4:

Section Number: Section 7.5.4.6.1
Page Number: 309
Line Number: Last sentence in section 7.5.4.6.1

Replace last sentence in section 7.5.4.6.1 (from 802.16e-2005) with the following:

~~Truncate(*x*, *y*) is the rightmost *y* bits of a value *x* only if *y* <= *x*.~~

The Truncate() function is defined in Section 7.5.4.2.

Change #5
Section Number: Section 7.5.4.4.1
Page Number: 305
Line Number: 2nd to last line in section

Replace 2nd to last line in section 7.5.4.4.1 (from 802.16e-2005) with the following:

~~CMAC value <= Truncate64 (CMAC (CMAC_KEY_*, AKID CMAC key sequence number | CMAC_PN |~~
~~CID |16-bit zero padding | MAC_Management_Message))~~

CMAC value <= Truncate (CMAC (CMAC_KEY_*, AKID ~~CMAC key sequence number~~ | CMAC_PN | CID |16-bit zero padding | MAC_Management_Message), 64)

Change #6:

Section Number: Section 7.5.4.5.2.1 (from 802.16e-2005)
Page Number: 306
Line Number: 3rd and 4th lines from the bottom

Replace 3rd and 4th lines from the bottom with the following:

~~k1 = leftmost 64 bits of the 128-bit KEK~~
~~k2 = rightmost 64 bits of the 128-bit KEK~~
k1 = most significant 64 bits of the 128-bit KEK
k2 = least significant 64 bits of the 128-bit KEK

Change #7:

Section Number: Section 7.5.2.1
Page Number: 304
Line Number: 7
Insert new subclause 7.5.2.1 in 802.16e-2005

Replace the 7th and 8th sentences in the subclause with the following text

~~k1 = leftmost 64 bits of the 128-bit KEK~~
~~k2 = rightmost 64 bits of the 128-bit KEK~~
k1 = most significant 64 bits of the 128-bit KEK
k2 = least significant 64 bits of the 128-bit KEK