Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Reply comment: Clarifications for the attachment of HMAC/CMAC Tuple**
Data Submitted	**2007-03-15**
Source(s)	Kyeong-Tae Do, Samsung Electronics Co. Voice: +82-31-279-5748 kyeongtae.do@samsung.com
Re:	P80216/Cor2/D2
Abstract	The document contains suggestions on the clarification of the attachment of HMAC/CMAC Tuple
Purpose	Adoption of proposed changes into P80216/Cor2/D2
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:chiar@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 for the attachment of HMAC/CMAC Tuple

Introduction

The receivers can verity the validity of management messages by authenticating messages with HMAC or CMAC Tuples. HMAC/CMAC Tuple is computed with H/CMAC_KEY_* which is derived from AK, GKEK or EIK. So, HMAC/CMAC Tuple cannot be computed without support of authentication. If the MS and BS do not support authentication, it is not needed to attach HMAC/CMAC Tuple.

Proposed changes to P80216/Cor2/D2

[Add following text to 6.3.2.3.7 p.25 of IEEE 802.16 Cor2/D2]

Change the second paragraph below Table 21 as follows:

The REG-REQ shall contain the following TLV~~s~~ if authentication is supported:

Hashed Message Authentication Code (HMAC)/CMAC Tuple

Shall be final attribute in the message's TLV attribute list (11.1.2).

[Add following text to 6.3.2.3.10 p.31 of IEEE 802.16 Cor2/D2]

6.3.2.3.10 DSA-REQ message

Change the paragraphs below Table 38 as follows:

The DSA-REQ message shall contain the following:

Service Flow Parameters (see 11.13)

Specification of the service flow's traffic characteristics and scheduling requirements

Convergence Sublayer parameter Encodings(see 11.13.19)

The DSA-REQ message shall contain the following if authentication is supported:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple attribute contains a keyed message digest (to authenticate the sender). The HMAC Tuple attribute shall be the final attribute in the DSx message's attribute list.

[Add following text to 6.3.2.3.11 p.31 of IEEE 802.16 Cor2/D2]

6.3.2.3.11 DSA-RSP message

Change the paragraphs below Table 39 as follows:

Whether successful or unsuccessful, the message shall include the following if authentication is supported:

~~Change the explanation text of the "HMAC" field as indicated:~~

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple attribute contains a keyed message digest (to authenticate the sender). The HMAC Tuple attribute shall be the final attribute in the DSx message's attribute list.

[Add following text above the section 6.3.2.3.23 p.31 of IEEE 802.16 Cor2/D2]

6.3.2.3.13 DSC Request (DSC-REQ) message

Change the paragraphs below Table 41 as follows:

A DSC-REQ shall contain the following:

Service Flow Parameters (see 11.3)

Specifies the service flow's new traffic characteristics and scheduling requirements. The Admitted and Active QoS Parameter Sets currently in use by the service flow. If the DSC message is successful and it contains service flow parameters, but does not contain replacement sets for both Admitted and Active QoS Parameter Sets, the omitted set(s) shall be set to null. The service flow parameters shall contain a FID.

A DSC-REQ shall contain the following if authentication is supported:

~~***Change the explanation text of the "HMAC" field as indicated:***~~

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple attribute contains a keyed message digest (to authenticate the sender). The HMAC Tuple attribute shall be the final attribute in the DSx message's attribute list.

6.3.2.3.14 DSC Response (DSC-RSP) message

Change the last paragraph as indicated:

~~***Change the explanation text of the "HMAC" field as indicated:***~~

Whether successful or unsuccessful, the message shall include the following if authentication is supported:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple attribute contains a keyed message digest (to authenticate the sender). The HMAC Tuple attribute shall be the final attribute in the DSx message's attribute list.

6.3.2.3.22 SS basic capability request (SBC-REQ) message

Change the last paragraph as indicated:

The RES-CMD shall include the following parameter~~s~~ encoded as TLV tuple~~s~~ if authentication is supported:

~~***Change the explanation text of the "HMAC" field as indicated:***~~

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[Add following text below the Table 55, 6.3.2.3.26, p.32 of IEEE 802.16 Cor2/D2]

Change the first paragraph below Table 55 as follows:

The DREG-CMD shall include the following parameters encoded as TLV tuples if authentication is supported:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[Add following text above the section 6.3.2.3.42 p.34 of IEEE 802.16 Cor2/D2]

6.3.2.3.28 Config File TFTP Complete (TFTP-CPLT) message

Change the last paragraph as indicated:

~~***Change the explanation text of the "HMAC" field as indicated:***~~

The TFTP-CPLT shall include the following parameter~~s~~ encoded as TLV tuple~~s~~ if authentication is supported:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[Add following text below the table 87, 6.3.2.3.42 p.34 of IEEE 802.16 Cor2/D2]

Change the paragraph below Table 87 as indicated:

The DREG-REQ shall include the following parameter~~s~~ encoded as TLV tuple~~s~~ if authentication is supported:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

Change the text on the page 25 as follows;

[from]

The REG-RSP ~~shall~~may contain the following TLVs:

SS management support (11.7.2)

Response to REG-REQ indicating the mode of SS management operation.

Secondary Management CID (11.7.5)

Present only if the SS has indicated in the REG-REQ that it is a managed SS.

When the Secondary Management CID is present, the following uplink QoS parameters may be also included in the message:

Traffic priority (11.13.5)

Maximum sustained traffic rate (11.13.6)

Minimum reserved traffic rate (11.13.8)

Maximum latency (11.13.14)

IP management mode (11.7.3)

Response to REG-REQ indication of whether or not the requester wishes to accept IP-based traffic

on the Secondary Management Connection, once the initialization process has completed.

To:

In the OFDM, the REG-RSP shall contain the following TLVs:

SS management support (11.7.2)

Response to REG-REQ indicating the mode of SS management operation.

Secondary Management CID (11.7.5)

Present only if the SS has indicated in the REG-REQ that it is a managed SS.

When the Secondary Management CID is present, the following uplink QoS parameters may be also included in the message:

Traffic priority (11.13.5)

Maximum sustained traffic rate (11.13.6)

Minimum reserved traffic rate (11.13.8)

Maximum latency (11.13.14)

IP management mode (11.7.3)

Response to REG-REQ indication of whether or not the requester wishes to accept IP-based traffic

on the Secondary Management Connection, once the initialization process has completed.