Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**The Clarification of AK Context and Calculation of CMAC Digest**
Date Submitted	**2005-07-14**
Source(s)	Zhengfei Xiao, Yongmao Li, Phillip Barber, Jim Carlo, David Xiang, Duke Dang, Lucy Chen, John Lee mailto:john_lee@huawei.com HUAWEI Seokheon Cho Taeyong Lee ETRI
Re:	Call for contribution and comments.
Abstract	The Clarification of AK Context and Calculation of CMAC Digest.
Purpose	Adoption
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>.

The Clarification of AK Context and Calculation of CMAC Digest

Zhengfei Xiao, Yongmao Li, Phillip Barber, Jim Carlo, David Xiang, Duke Dang, Lucy Chen, John Lee
HUAWEI

Problem Definition

To avoid replay attack, it should be ensured that the CMAC_PN_* in the management message received by the BS or MS is always incremented and never repeated。 So the standard should stress that MS shall complete the re-authentication with BS and obtain a new AK before the CMAC_PN_* is expired.

Proposed Text Changes

[Remedy 1]

[Modify sub-clause 7.5.4.1, in page230 line36 as follows:]

7.5.4.1 Calculation of CMAC Value

The calculation of the keyed hash value contained in the CMAC-Digest attribute and the CMAC Tuple shall use the CMAC Algorithm with AES. The downlink authentication key CMAC_KEY_D shall be used for authenticating messages in the downlink direction. The uplink authentication key CMAC_KEY_U shall be used for authenticating messages in the uplink direction. Uplink and downlink message authentication keys are derived from the AK (see 7.5.4 below for details).

For authentication multicast messages (in the DL only) a CMAC_KEY_GD shall be used (one for each group), group authentication key is derived from GKEK The CMAC-Digest and CMAC-Tuple attributes shall be only applicable to the PKM version 2. In the PKM version 2 protocol, the CMAC key sequence number in the CMAC tuple shall be equal to the 4-bit AK
sequence number of the AK from which the CMAC_KEY_x was derived.

The CMAC Packet Number Counter (CMAC_PN_*) is a 4 byte sequential counter that is incremented in the context of UL messages by the MS, and in the context of DL messages by the BS,. The BS will also maintain a separate CMAC_PN_* for multicast packets per each GSA and increment that counter in the context of each multicast packet from the group. For MAC messages that have no CID e.g. RNG-REQ message, the CMAC_PN_* context will be the same as used on the basic CID. If basic CID is unknown (e.g. in network reentry situation) then CID 0 should be used.

The CMAC Packet Number Counter, CMAC_PN_*, is part of the CMAC security context and must be unique for each MAC management message with the CMAC tuple or digest. Any tuple value of {CMAC_PN_*, AK} shall not be used more than once. The MS shall initiate re-authentication when the CMAC_PN_U reaches the half of its number space to obtain a new AK before it expires. The BS shall send the Auth-Invalid message to MS when the CMAC_PN_D reaches the half of its number space.

The digest shall be calculated over a field consisting of the CMAC key sequence number followed by the CMAC Packet Number Counter, expressed as an unsigned 32-bit number, followed by the 16-bit Connection ID on which the message is sent, followed by 16-bit of zero padding (for the header to be aligned with AES block size) and followed by the entire MAC management message with the exception of the CMAC TLV.

The least significant bits of the digest shall be truncated to yield a 64-bit length digest. The CMAC key sequence number shall be equal to the 4-bit AK sequence number of the AK from which the CMAC_KEY_x was derived.

I.e.,:

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

If the digest is included in an MPDU that has no CID, e.g. A RNG-REQ message, the CID used shall take the value of the basic CID. If basic CID is unknown (e.g. in network reentry situation) then CID 0 should be used.

[Remedy 2]

[Modify sub-clause 7.5.4.1, in page230 line36 as follows:]

7.5.4.1 Calculation of CMAC Value

The calculation of the keyed hash value contained in the CMAC-Digest attribute and the CMAC Tuple shall use the CMAC Algorithm with AES. The downlink authentication key CMAC_KEY_D shall be used for authenticating messages in the downlink direction. The uplink authentication key CMAC_KEY_U shall be used for authenticating messages in the uplink direction. Uplink and downlink message authentication keys are derived from the AK (see 7.5.4 below for details).

For authentication multicast messages (in the DL only) a CMAC_KEY_GD shall be used (one for each group), group authentication key is derived from GKEK The CMAC-Digest and CMAC-Tuple attributes shall be only applicable to the PKM version 2. In the PKM version 2 protocol, the CMAC key sequence number in the CMAC tuple shall be equal to the 4-bit AK
sequence number of the AK from which the CMAC_KEY_x was derived.

The CMAC Packet Number Counter (CMAC_PN_*) is a 4 byte sequential counter that is incremented in the context of UL messages by the MS, and in the context of DL messages by the BS,. The BS will also maintain a separate CMAC_PN_* for multicast packets per each GSA and increment that counter in the context of each multicast packet from the group. For MAC messages that have no CID e.g. RNG-REQ message, the CMAC_PN_* context will be the same as used on the basic CID. If basic CID is unknown (e.g. in network reentry situation) then CID 0 should be used.

The CMAC Packet Number Counter, CMAC_PN_*, is part of the CMAC security context and must be unique for each MAC management message with the CMAC tuple or digest. Any tuple value of {CMAC_PN_*, AK} shall not be used more than once. The MS shall initiate re-authentication when the

CMAC_PN_U reaches the allowed maximum PN number for signaling message to obtain a new AK before it expires. The BS shall send the Auth-Invalid message to MS when the CMAC_PN_D reaches the allowed maximum PN number for signaling message.

The digest shall be calculated over a field consisting of the CMAC key sequence number followed by the CMAC Packet Number Counter, expressed as an unsigned 32-bit number, followed by the 16-bit Connection ID on which the message is sent, followed by 16-bit of zero padding (for the header to be aligned with AES block size) and followed by the entire MAC management message with the exception of the CMAC TLV.

The least significant bits of the digest shall be truncated to yield a 64-bit length digest. The CMAC key sequence number shall be equal to the 4-bit AK sequence number of the AK from which the CMAC_KEY_x was derived.

I.e.,:

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

If the digest is included in an MPDU that has no CID, e.g. A RNG-REQ message, the CID used shall take the value of the basic CID. If basic CID is unknown (e.g. in network reentry situation) then CID 0 should be used.

[Change Talbe 37g in sub-clauses 6.3.2.3.9.18: as follows]

6.3.2.3.9.18 PKMv2 SA-TEK-Challenge message

Table 37g – PKMv2 SA-TEK-Challenge message attributes

Attribute	Contents
BS_Random	A freshly generated random number of 64bits
AKID	BS transmits newly assigned AKID.
CMAC Tuple/HMAC Tuple	Message integrity tuple for this message
Key lifetime	PMK lifetime, this attribute shall include only follows EAP-based authorization or EAP-based re-authorization procedures.
Allowed maximum PN number	Allowed maximum PN number for signaling connection

[Change the Table 370 in sub-clause 11.9:]
11.9 PKM-REQ/RSP management message encodings

Table 370-PKM attribute types

Type	PKM attribute
32	~~Reserved~~ Allowed Maximum PN Number
33	SS_RANDOM
	… **Rest of the attributes of this table remains the same.**

[Add the following sub-clause in the section 11.9:]
11.9.x Allowed maximum PN number

Description: This attribute indicates the maximum PN number which the MS can use when CMAC-value or short-HMAC digest is generated. The MS shall initiate re-authentication when the CMAC_PN_* reaches the allowed maximum PN number.

Type	Length	Value
32	1	Operator-specific

Operator Operator
Network Network