Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Correction to Construction of Prepended CMAC data**	
Date Submitted	**2005-10-06**	
Source(s)	David Johnston Intel Corporation Hillsboro, OR USA	Voice: 502 264 3855 Fax: mailto:dj.johnston@ieee.org
Re:	802.16e late comment by Pieter-Paul Giesberts	
Abstract	The padding of the prepended CMAC data is meant to align to 128 bits, but it doesn't. At some point the AKID using in the computation of the CMAC value was change to the 4 bit AK Sequence Number, thus breaking the secuity properties of using the AKID. This proposal restored the AKID makes the fields of the CMAC computation align to 128 bits and aligns all the fields to a byte boundary.	
Purpose	Consider and adopt this text into the 802.16e draft as a resolution of late comment by Pieter-Paul Giesberts.	
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>.	

Correcting Construction of 802.16e CMAC Prepended Data

David Johnston
Intel Corporation(optional)

Introduction

The following text amends the 802.16e CMAC management frame protection text to revert to the insertion of the AKID in the computation of the CMAC instead of the 4 bit AK Sequence number. This aligns the prepended data to 128 bits, consistent with the AES block size and aligns the internal fields to 8 bit boundaries.

Background

The AKID is included in the computation of the CMAC as a unique identifier to prevent classes of replay that rely on different AKIDs with the same key sequence number. There are only 16 key sequence numbers so collision is inevitable.

The 4 bit key sequence number is used in the SA-TEK-Challenge message to allow a mapping of AK key sequence to AKID so that the full AKID does not need to be sent in the CMAC tuple, only the 4 bit sequence number. However the full AKID can be included in the CMAC computation which is a purely local process.

Proposal

Adopt the following text in place of the existing text of 7.5.4.4.1 in 802.16e.

[Change the text of 7.5.4.4.1 as indicated:]

7.5.4.4.1 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 AKID~~CMAC key sequence number~~ used in the computation of the CMAC value~~tuple~~ shall be the 64 bit AKID~~equal to the 4-bit AK sequence number~~ of the AK from which the CMAC_KEY_x was derived. See 6.3.2.3.9.18 for the SA-TEK-Challenge message attributes in which the

mapping between the AK Sequence number and the AKID is communicated and see 7.2.2.4.1 for a description of the AK context that contains the AK and AKID.

The CMAC Packet Number Counter (CMAC_PN_*) is a 4 byte sequential counter that is incremented in the context of UL messages by the SS, 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 reauthentication process should be initiated (by BS or SS) to establish a new AK before the CMAC_PN_* reaches the end of its number space.

The digest shall be calculated over a field consisting of the AKID~~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_*, AKID~~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.