Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**AES Based Cryptographic Functions for PKMv2**
Date Submitted	**2004-6-23**

Source(s)	David Johnston Intel Corporation 2111 NE 25th Ave. Hillsboro 97124	Voice: +1 (503) 264-3855 [mailto:dj.johnston@intel.com]

Re:	IEEE 802.16e Security Adhoc
Abstract	Proposal for cryptographic functions that are all based on AES
Purpose	Enable implementations with a minimum of crypto primitive acceleration hardware through reduction in the number of underlying primitives used in PKMv2
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>.

AES Based Cryptographic Functions for PKMv2

David Johnston, Intel
Junhyuk Song, Samsung
Donnie Dongkie Lee, SK Telecom
YoungMan Park, Korea Telecom

Cryptographic primitives are typically compute intensive in software, however they tend to be easily accelerated using digital logic acceleration hardware. For systems where there is a need to accelerate the cryptographic primitives, each new primitive imposes a further implementation cost in terms of acceleration hardware.

With the introduction of a new negotiated PKM version (PKMv2) we are given the opportunity to invoke a set of cryptographic functions that are based on a single underlying AES primitive. This will allow an implementation to accelerate all security functions with only an expoentiator for RSA and an AES accelerator for the link cipher, key exchange and authentication functions.

This document contains draft text changes to 802.16e-D3 to achieve this.

Remedy 1:
*[Add new subsection after 7.5.3, **7.5.4 Calculation of OMAC Digests**.]*

7.5.4 Calculation of OMAC-Digests

The calculation of the keyed hash in the OMAC-Digest attribute and the OMAC Tuple shall use the OMAC Algorithm [1] with AES. The downlink authentication key OMAC_KEY_D shall be used for authenticating messages in the downlink direction. The uplink authentication key OMAC_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).

In the PKM version 2 protocol, The OMAC Sequence number in the OMAC Tuple shall be equal to the 48 bit AK Sequence Number of the AK from which the OMAC_KEY_x was derived. In the PKM version 1 protocol, The 4 least significant bits of the OMAC Sequence number in the OMAC Tuple shall be equal to the 4 bit AK Sequence Number and the 44 most significant bits shall be equal to 0.

The digest shall be calculated over a field consisting of the OMAC key sequence number followed by the frame number, expressed as an unsigned 32 bit number, followed by the 16 bit connection ID on which the message is sent followed by the entire MAC management message with the exception of the OMAC-Digest but including the OMAC Tuple attributes.

The least significant bits of the digest shall be truncated to yield a 64 bit length digest.

I.E.:

OMAC digest <= Truncate64(OMAC(OMAC_KEY_*, OMAC sequence number | Frame number | CID | MAC_Management_Message | OMAC_TLV_Attributes))

If the message is included in an MPDU that has no CID, E.G. A RNG-REQ message, the CID used shall take the value 0.

The frame number in which a message containing an OMAC tuple may be fragmented and so be transmitted in more than one frame number. In this case, the frame number used in the OMAC calculation shall take the value of the frame number of the frame in which the first fragment is transmitted.

[If the ETRI proposal 'Authentication Policy Support' is accepted into 16e, there will be a policy bit to determine whether or not the equipment supports the inclusion of the frame number. So if this ETRI proposal is accepted, then insert the following text:]

If the frame_number_in_authentication_tuple bit is set to zero in the authentication policy bits, then the frame number used in the OMAC calculation shall take the value 0 expressed as a 32 bit integer.

[Insert a new level 3 section before 11.1.2 HMAC Tuple and change 11.1.2 to 11.1.2.1]

11.1.2 Authentication Tuples

11.1.2.1 HMAC Tuple

[Insert section 11.1.2.2 OMAC Tuple, and number the type numbers appropriately]

11.1.2.2 OMAC Tuple

This parameter contains the OMAC Key Sequence Number concatenated with an OMAC-Digest used for message authentication. The OMAC Key Sequence Number is stored in the 48 least significant bits of the OMAC Tuple. The OMAC-Tuple attribute format is shown in Table 347 and Table 348.

When included in a MAC management message, the OMAC tuple shall always be the final tuple in the message.

A message received, that contains an OMAC tuple, shall not be considered authentic if the length field of the tuple is not 17, or if the locally computed value of the digest does not match the digest in the message.

Non authentic messages shall be discarded.

Informative note: It would be appropriate for a MIB to increment an error count on receipt of a non authentic message, so that management can detect an active attack.

Table 347—HMAC Tuple definition

Type	Length	Value	Scope
[tbd]	14	See table 348	DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT

Table 348—HMAC Tuple definition

Field	Length	Note
OMAC key sequence number	48 bits	
OMAC Digest	64 bits	OMAC with AES 128

[Renumber table numbering as appropriate]

[Add the following to the references and update the reference number as required]

[1] http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/omac/omac-spec.pdf , Tetsu Iata, Kaoru Kurosawa, Dec 20th 2002.