Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**AK transfer in a distributed security model**	
Date Submitted	**2007-07-05**	
Source(s)	Sergey Seleznev, Hyoung Kyu Lim, Jungje Son Samsung Electronics Rep. of Korea, Gyonggi-do, Suwon	Voice: +82312795968 E-mail: s.sergey@samsung.com
Re:	IEEE 802.16j-07/019: “Call for Technical Comments Regarding IEEE Project 802.16j”	
Abstract	This contribution proposes text for Authorization Key (AK) transfer in a distributed security model.	
Purpose	Discuss and adopt proposed text.	
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the “Source(s)” field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

AK transfer in a distributed security model

Sergey Seleznev
Samsung Electronics

Problem description

In this contribution we propose text changes to enable authorization key (AK) transfer in a distributed security model. We define relevant message format and procedure.

Text proposal

[*Insert the following section 7.2.2.6*]:

7.2.2.6 AK transfer

In a distributed security model, upon successful authorization of MS or RS, MR-BS shall send PKMv2 AK Transfer message conveying a set of AK parameters to the relevant AR-RS (i.e. AR-RS which runs PKM protocol with that MS or RS). PKMv2 AK Transfer message may also include multicast/broadcast GSAIDs and associated GTEK-Parameters pairs.

AK parameters shall include AK key material, AK Sequence Number and AK Lifetime. GKEK parameters shall include GKEK key material, GKEKID and GKEK Lifetime for the relevant MS. AR RS shall use them during PKMv2 SA-TEK 3-way handshake with MS.

AR RS shall send PKMv2 AK Transfer ACK message to MR-BS in order to acknowledge successful reception of PKMv2 AK Transfer message.

For SAs using a ciphersuite employing DES-CBC, the AK in the AK Transfer message is triple DES (3-DES) encrypted, using a two-key, 3-DES KEK derived from the AR-RS AK. For SAs using a ciphersuite employing 128 bits keys, such as AES-CCM mode, the TEK in the AK Transfer message is AES encrypted using a 128-bit key derived for the AR RS AK and a 128-bit block size.

[*Insert the following section 7.5.2.5.*]:

7.5.2.5 Encryption of AK with AES Key Wrap

This method of encrypting the AK shall be used for SAs with the TEK encryption algorithm identifier in the cryptographic suite equal to 0x04. MR-BS encrypts the value fields of the AK in the AK Transfer messages it sends to AR RS. This field is, first, padded with 32-bit nonce and then encrypted using AES Key Wrap Algorithm.

Encryption: $C, I = E_k [P||N]$

Decryption: $P||N, I = D_k [C]$

P = 160-bit plaintext AK

N = 32-bit random value

C = 192-bit ciphertext

I = Integrity Check Value

k = the 128-bit KEK

E_k [ ] = AES Key Wrap encryption with key k

D_k [ ] = AES Key Wrap decryption with key k

The AES key wrap encryption algorithm accepts both a ciphertext and integrity check value. The decryption algorithm returns a plaintext key and the integrity check value. The default integrity check value in the NIST AES Key Wrap algorithm shall be used.

[*Insert the following section 6.3.2.3.9.xx*]:

6.3.2.3.9.xx PKMv2 AK Transfer message

Attribute	**Contents**
Key Sequence Number	AR RS AK sequence number
SAID	AR RS primary SAID
SAID	MS/RS’s primary SAID
AK	MS/RS’s authorization key
Key Sequence Number	MS/RS’s AK sequence number
Key Lifetime	MS/RS’s AK lifetime
Group SA Descriptor	TLV that specifies GSAID and additional properties of that SA
Nonce	A random number generated in an MR-BS
HMAC/CMAC Digest	Message authentication digest

6.3.2.3.9.xx PKMv2 AK Transfer ACK

Attribute	**Contents**
Key Sequence Number	AR RS AK sequence number
SAID	AR RS primary SAID
Key Sequence Number	MS/RS’s AK sequence number
SAID	MS/RS’s primary SAID
Nonce	A same random number included in the PKMv2 AK Transfer message
HMAC/CMAC Digest	Message authentication digest