Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	TEK delivery problem fix for related management message
Date Submitted	**2005-07-09**
Source(s)	Jun Zhang, Yongmao Li, John Lee, Thomas Lee(Li Li) Huawei / FutureWei (Huawei North America Division) 3255-4 Scott Blvd.Suite 101, Santa Clara, CA 95054 Voice: 408-7129326 mailto: john_lee@huawei.com
Re:	IEEE P802.16-2004Cor1/D3
Abstract	TEK delivery problem fix for related management message.
Purpose	For 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>.

TEK delivery problem fix for related management messages

Jun Zhang, Li Yongmao, John Lee, Thomas Lee
HUAWEI

1. Background

In IEEE802.16D-2004, a procedure of TEK updating and delivering has been defined as follow: at all times the BS maintains two active sets of keying material per SAID. The lifetimes of the two generations overlap such that each generation becomes active halfway through the life of it predecessor and expires halfway through the life of its successor. An MSS shall periodically refresh its TEK by reissuing a Key Request. The Key Reply sent by BS provides the requesting MSS both of an SAID's active generations of keying material, which includes the TEK, the CBC initialization vector, and the remaining lifetime of the keying material.

2. Problem statement

In the Key Reply, sent by BS to response the MSS's Key Request, BS will always include both of an SAID's active generations of keying material, but it is not necessary. In detail, when MSS sent Nth Key Request, BS shall response it with Key Reply (TEKn, TEKn+1). In the same way, when MSS sent (N+1)th Key Request, BS shall response it with Key Reply (TEKn+1, TEKn+2). In the two sequent Key Reply messages, TEKn+1 has been sent twice respectively, and the only difference between two TEKn+1 is that the first TEKn+1 is sent as a new keying material and the second as a old one. For the MSS, in a normal situation, the second TEKn+1 is a redundancy. So BS doesn't need to do so every time, and in most cases, only needs to reply with the new keying material.

But there is stilly other two situations where BS needs to response MSS's Key Request by sending a Key Response including two active generations of keying material. The one situation is where MSS sends its initial Key Request. And the other situation is where MSS sends a Key Request to re-synchronize its TEK state machine with BS after a period of loss of synchronization.

So, it is a reasonable and efficient way that BS makes different response according to different situation which MSS is in.

3. Proposed Solution

While MSS definitely knows which situations it is in, BS has no way to know which situation the requesting MSS is in. We propose that a new indicator, named as New TEK Only, be added into Key Request message. MSS can use this indicator to inform BS which operations should be taken, to response with two active generations of keying material or to response with only the new one.

Before it is about to send a Key Request message to request TEK, a MSS should estimate which situation it be in, then makes a decision that is to request a new TEK only or both. If just request a new TEK only, MSS should set indicator New TEK Only = 1, otherwise New TEK Only = 0.

When BS received a Key Request, it should read the value of indicator New TEK Only first then decide which action should be taken. If New TEK Only = 1, BS should response with the new TEK only, otherwise with both of active TEK.

In addition, the indicator New TEK Only is omissible, that is a Key Request message may not include this indicator. When that happened, BS should act as New TEK Only = 0.

Proposed Text Changes

See the details as follows:

[Insert a subclause 6.3.2.3.9.5 Key Request message, as follows]

6.3.2.3.9.5 Key Request message

change the Table 31 and Table 32 as follows

Table 31— Key Request attributes

Attributes	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier
New TEK Only	A indicator to inform BS
HMAC Digest/CMAC Digest	Message Digest calculated using AK

Table 32— Key Request attributes for Mesh Mode

Attributes	Contents
SS Certificate	X.509 Certificate of the Node.
SAID	SA identifier.
New TEK Only	A indicator to inform BS
HMAC-Digest	HMAC using HMAC_KEY_S

[Insert a subclause 6.3.2.3.9.6 Key Replyt message, as follows]

6.3.2.3.9.6 Key Reply message

change the fourth paragraph as follow

The BS distributes to a client SS one or both generations of active keying material depending on which keying material SS has requested. Thus, the Key Reply message contains one or two TEK-Parameters attributes, each containing the keying material for one of the SAID's two active sets of keying material.

[Insert a subclause 7.2.5 TEK state machine, as follows]

7.2.5 TEK state machine

change the fourth paragraph as follow

As mentioned in 7.2.2, the BS maintains two active TEKs per SAID. The BS includes in its Key Replies one or two ~~both~~ of these TEKs, along with their remaining lifetimes. The BS encrypts

downlink traffic with the older of its two TEKs and decrypts uplink traffic with either the older or newer TEK, depending upon which of the two keys the SS was using at the time. The SS encrypts uplink traffic with the newer of its two TEKs and decrypts downlink traffic with either the older or newer TEK, depending upon which of the two keys the BS was using at the time. See 7.4 for details on SS and BS key usage requirements.

[Insert a subclause 7.2.5.2 Messages, as follows]

7.2.5.2 Messages

Change the third paragraph as follow

Key Reply: Response from the BS carrying the one or two active sets of traffic keying material for this SAID. Sent by the BS to the SS, it includes the SAID's TEKs, encrypted with a KEK derived from the AK. The Key Reply message is authenticated with a keyed message digest; the authentication key is derived from the AK.

[Insert a subclause 7.4.1.4 TEK lifetime, as follows]

7.4.1.4 TEK lifetime

Change the second paragraph as follow

The Key Reply messages sent by a BS contain TEK parameters for the one or two active TEKs. The TEKs' active lifetimes a BS reports in a Key Reply message shall reflect, as accurately as an implementation permits, the remaining lifetimes of these TEKs at the time the Key Reply message is sent.

[change subclause 11.9 PKM-REQ/RSP management message encodings, as follows]

11.9 PKM-REQ/RSP management message encodings

Change the Table 370 as follow, the unchanged is omitted

Table 370—PKM attribute types

Type	PKM attributes
22	~~Version~~New TEK Only
23	SA-Descriptor
…	…

[Insert a new subclause 11.9.16 Version, as follows]

11.9.16 Version

change the entire subclause as follows:

11.9.16 New TEK Only
Description: An indicator to inform BS which action shall be taken: to response with only new TEK or to response with both active TEK. This filed is omissible, that is, a Key Request message may not include this indicator. When that happened, BS should act as New TEK Only =

Table 379—New TEK Only attribute values

Type	Length	Value
22	1	1 byte indicator to inform BS which keying material has been requested by MSS

Table 380—New TEK Only attribute values

Value	Description
0	MSS request both active TEK
1	MSS only request the new TEK
2-255	*Reserved*