

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >
Title	<b>Reduction of Redundancy in TEK Delivery Related Management Message</b>
Date Submitted	<b>2005-07-14</b>
Source(s)	Jun Zhang, Yongmao Li, Phillip Barber, Jim Carlo, David Xiang, Duke Dang, Lucy Chen, John Lee <a href="mailto:john_lee@huawei.com">mailto:john_lee@huawei.com</a>  HUAWEI
Re:	<b>Call for contribution and comments.</b>
Abstract	Reduction of redundancy in TEK delivery related management message.
Purpose	<b>Adoption</b>
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 < <a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a> >, 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 < <a href="mailto:chair@wirelessman.org">mailto:chair@wirelessman.org</a> > 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 < <a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a> >.

## Reduction of Redundancy in TEK Delivery Related Management Message

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

### Background

In IEEE802.16e/D9, TEK updating and delivering procedure 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 its 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.

### Problem Definition

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 (TEK<sub>N</sub>, TEK<sub>N+1</sub>). In the same way, when MSS sent (N+1)th Key Request, BS shall response it with Key Reply (TEK<sub>N+1</sub>, TEK<sub>N+2</sub>). In the two sequent Key Reply messages, TEK<sub>N+1</sub> has been sent twice respectively, and the only difference between two TEK<sub>N+1</sub> is that the first TEK<sub>N+1</sub> is sent as a new keying material and the second as a old one. For the MSS, in a normal situation, the second TEK<sub>N+1</sub> 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 are still 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 losing synchronization.

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

### Proposed Text Changes

See the details as follows:

*[Change Table 37k in subclause 6.3.2.3.9.21 in page 53, line 1, PKMv2 Key-Request message, as follows]*

Table 37j—PKMv2 Key Request attributes

Attributes	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier -GSAID for multicast or broadcast service
Nonce	A random number generated in an MS
<u>New TEK Only</u>	<u>A indicator to inform BS</u>

HMAC Digest/CMAC Digest	Message Digest calculated using AK
-------------------------	------------------------------------

*[Change the second paragraph in subclause 7.2.2.1 Security Associations, as follows]*

The BS responds to a Key Request with a Key Reply message, containing [the newer or both of](#) the BS's active keying material for a specific SAID [depending on which keying material has been requested by MSS](#).

*[Change the fifth paragraph (page 222, line 15) in subclause 7.2.5 TEK state machine, as follows]*

For the unicast service, the BS includes in its Key Replies [the newer or both of](#) these TEKs [depending on which keying material has been requested by MSS](#), 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.

*[Change the seventh paragraph (page 222, line 31) in subclause 7.2.5 TEK state machine, as follows]*

Through operation of a TEK state machine, the SS attempts to keep its copies of an SAID's TEKs synchronized with those of its BS. A TEK state machine issues Key Requests to refresh copies of its SAID's keying material soon after the scheduled expiration time of the older of its two TEKs and before the expiration of its newer TEK. To accommodate for SS/BS clock skew and other system processing and transmission delays, the SS schedules its Key Requests a configurable number of seconds before the newer TEK's estimated expiration in the BS. With the receipt of the Key Reply, the SS shall always update its records with the TEK Parameters from [one or both](#) TEKs contained in the Key Reply message. [Before MSS sends Key Request, it should decide which TEK be to be requested, the newer or both, then informs BS by the indicator New TEK Only.](#) With the receipt of the two Key Update Command messages, the SS shall always update its records with the TEK Parameters contained in the two Key Update Command messages for the multicast service or the broadcast service.

*[Change the paragraph in subclause 7.2.5.2 Messages, in page 225 and line 34, as follows]*

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 or the GSAID's GTEK, encrypted with a GKEK randomly generated from the BS or the ASA server. The Key Reply message is authenticated with a keyed message digest; the authentication key is derived from the AK.

*[Change Table 370 in subclause 11.9 PKM-REQ/RSP management message encodings, as follows (only changed/new text is shown)]*

Table 370—PKM attribute types

Type	PKM attributes
22	<del>Reserved</del> <a href="#">New TEK Only</a>
28	EAP Payload
...	...

*[Change subclause 11.9.16 Version, 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 field is omissible, that is, a Key Request message may not include this indicator. When that happened, BS should act as New TEK Only = 0.

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	<i>Reserved</i>

Operator Operator  
Network Network