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

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 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.

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 (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 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
New TEK Only	A indicator to inform BS

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 fifths paragraph(page222, 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(page222, 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 it's 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 page225 and line34, 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	~~Reserved~~ New TEK Only
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 filed 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	*Reserved*

Operator Network Operator Network