

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >
Title	Correct Figure for TEK management in BS and MS
Date Submitted	2005-07-19
	Sangwoo Doe, Sungsoo Oh, SungHo Yoo POSDATA Co. LTD
	doeing@posdata.co.kr
Re:	Response to Sponsor Ballot on IEEE802.16e/D8 document
Abstract	This contribution corrects the figure for TEK management in BS and MS.
Purpose	To incorporate the figure changes proposed in this contribution into the 802.16e/D9 draft.
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 (Version 1.0) < http://ieee802.org/16/ipr/patents/policy.html >, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org > as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site < http://ieee802.org/16/ipr/patents/notices >.

Correct Figure for TEK management in BS and MS

*Sangwoo Doe, Sungsoo Oh, Sungho Yoo,
POSDATA Co. LTD*

1. Problem Statements

IEEE 802.16-2004 describes TEK management as follows:

“Through operation of its TEK state machines, an SS shall request a new set of traffic keying material a configurable amount of time, the *TEK Grace Time* [see points (x) and (y) in Figure 134], **before the MS's latest TEK is scheduled to expire.**”

“TEK Refresh Timeout: The TEK refresh timer timed out. This timer event signals the TEK state machine to issue a new Key Request in order to refresh its keying material. The refresh timer is set to fire a configurable duration of time (*TEK Grace Time*) **before the expiration of the newer TEK the SS currently holds.** This is configured via the BS to occur after the scheduled expiration of the older of the two TEKs.”

However, Figure 134 of 802.16-2004 is incorrect, **as the current figure shows that an SS sends Key Request message to the BS when TEK0 Refresh Timer is fired [see points (x)]. Also, it shows that the BS receives Key Request message after TEK0 Lifetime expires. Therefore, SS and BS cannot synchronize TEKs. Figure 134 of 802.16-2004 needs correction so it can comply with the texts in IEEE 802.16-2004.**

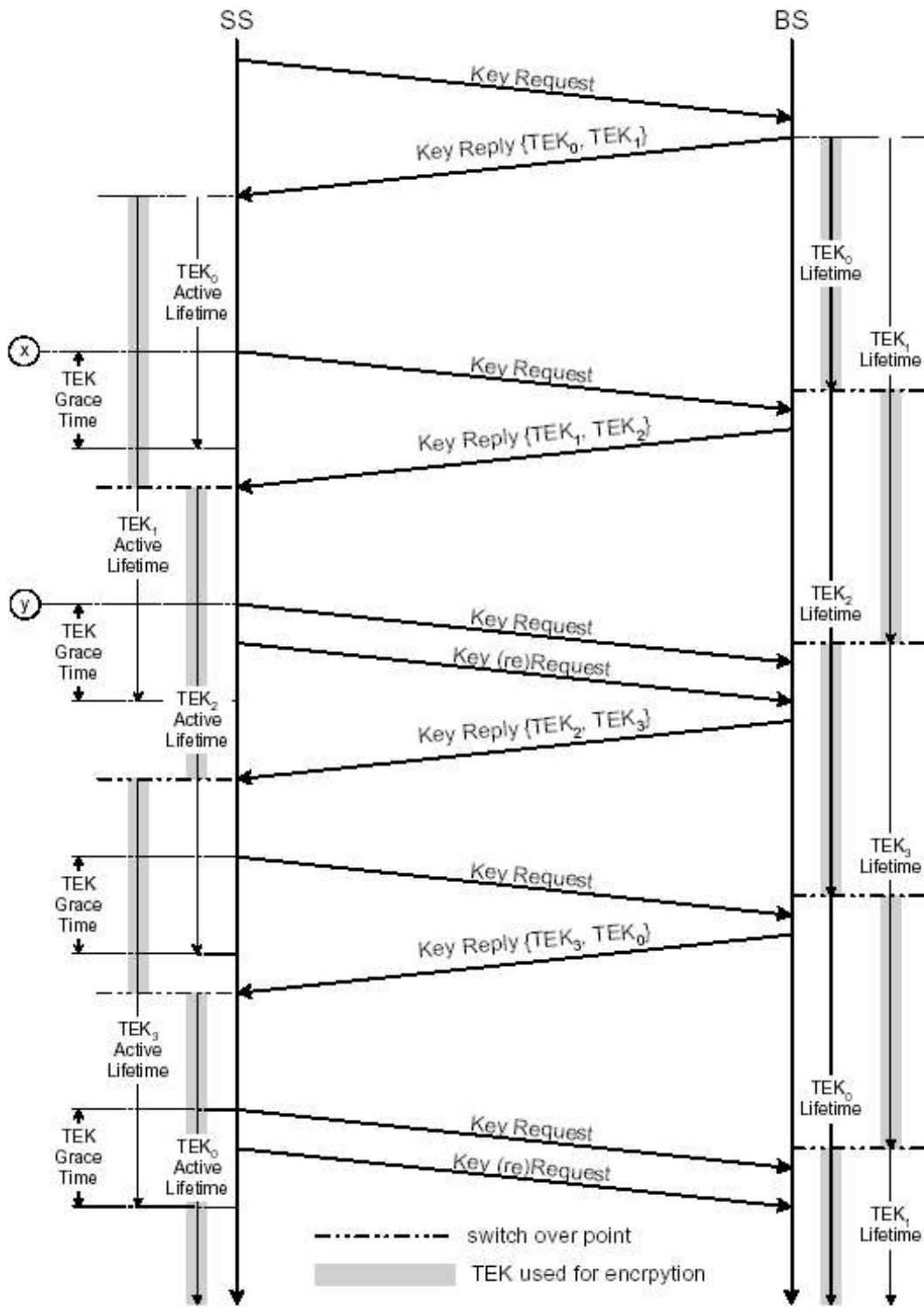


Figure 134—TEK management in BS and SS

2. Proposed Solution

We propose a correct figure in the below. In the proposed figure, an SS sends Key Request message to the BS when TEK1 Refresh Timer is fired [see points (x)] and the BS receive Key Request message before TEK1 Lifetime expires.

3. Specific Changes

[Insert the following changes in line 26, page 67 of 802.16d Cor1/D3 as indicated and include a new figure in the next page :]

7.4.1.5 BS usage of TEK

[Replace Figure 134 of 802.16-2004 with a new figure:]

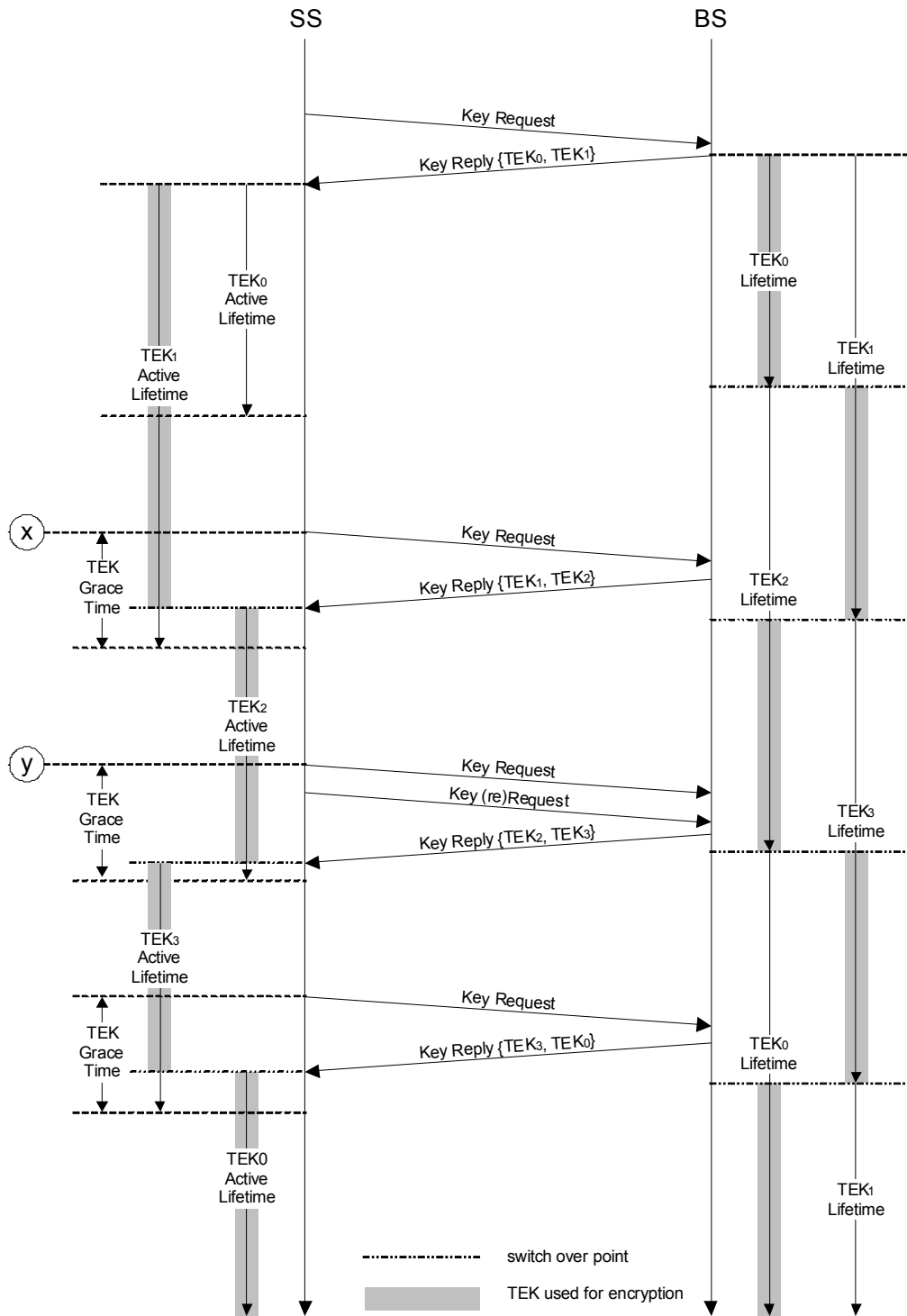


Figure 134 -TEK management in BS and SS

4. References

- [1] IEEE 802.16-2004 IEEE Standards for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems
- [2] DOCSIS1.1 SP-BPI+I10-030730 Cable Television Laboratories Specification to describe MAC layer security services for DOCSIS® CMTS