

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >	
Title	Comments on SDD Security Key Exchange	
Date Submitted	2009-04-24	
Source(s)	Yih-Guang Jan, Yang-Han Lee, Hsien-Wei Tseng, Ming-Hsueh Chuang Tamkang University (TKU)	yihjan@yahoo.com
	Youn-Tai Lee, Chun-Yen Hsu Institute for Information Industry (III)	lyt@nmi.iii.org.tw
	Shiann-Tsong Sheu National Central University (NCU)	stsheu@ce.ncu.edu.tw
	Whai-En Chen National Ilan University (NIU)	wechen@niu.edu.tw
Re:	Category: SDD comments / Area: Chapter 10 (MAC) "Comments on SDD 10 MAC"	
Abstract	Comments on SDD Security Key Exchange	
Purpose	To be discussed and adopted by TGM for the 802.16m SDD.	
Notice	<i>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.</i>	
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 >.	

Comments on SDD Security Key Exchange

*Yih-Guang Jan, Yang-Han Lee, Hsien-Wei Tseng, Ming-Hsueh Chuang
 Tamkang University (TKU)
 Youn-Tai Lee, Chun-Yen Hsu
 Institute for Information Industry (III)
 Shiann-Tsong Sheu
 National Central University (NCU)
 Whai-En Chen
 National Ilan University (NIU)*

1. Introduction

This contribution provides the corrected SDD text proposal to Key Exchange. In Figure 18 and Figure 19, they have some errors and are corrected.

2. Proposed SDD Text Modification

[In IEEE 80216m-08_003r8, Section 10.6.3.2, Replaced by the following corrected text]

=====Start of Proposed Text=====

10.6.3.2 Key Exchange

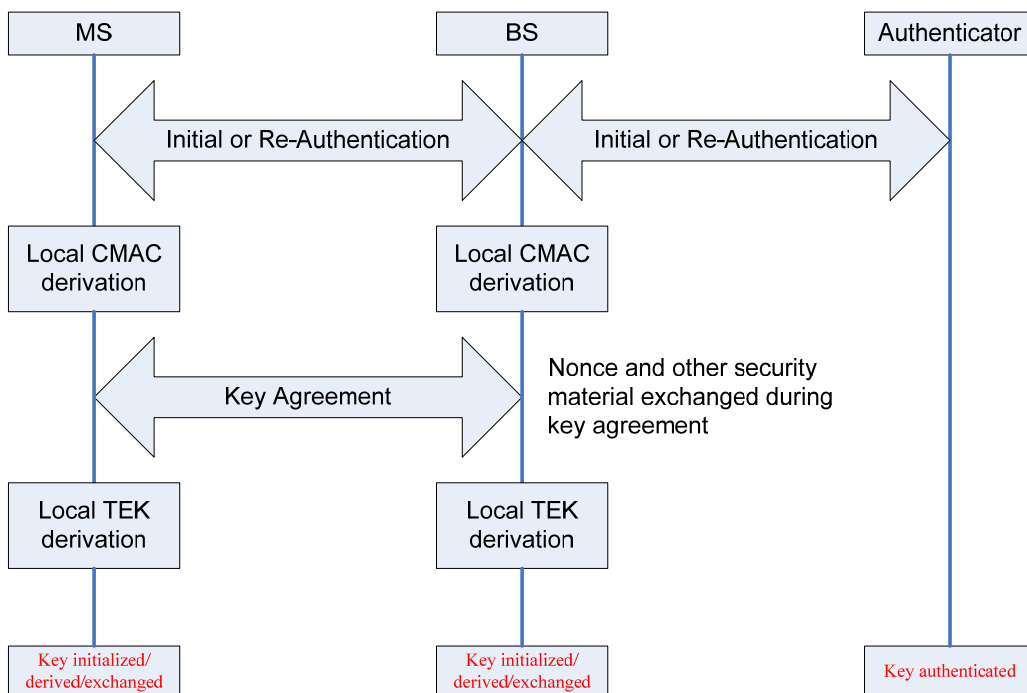
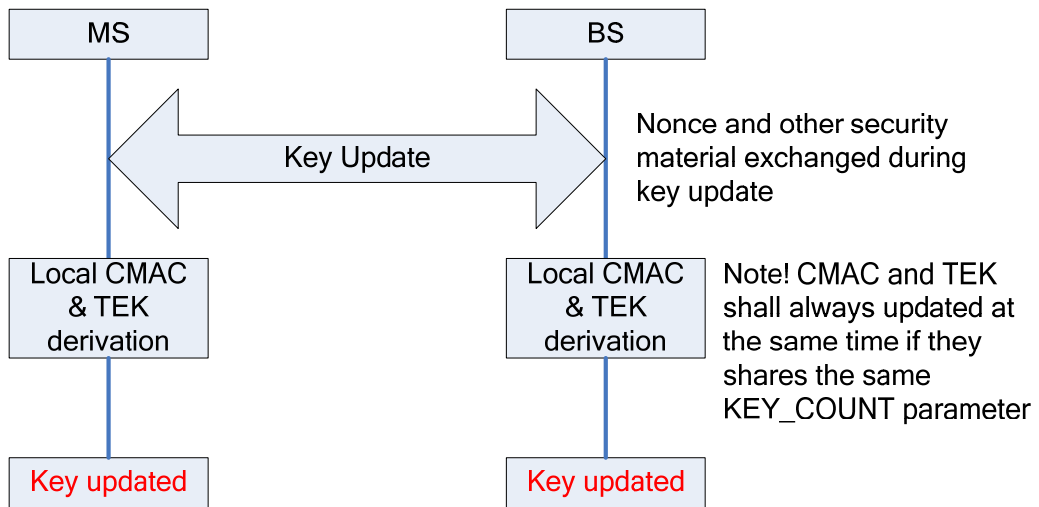


Figure 1 Initial or Re-authentication - Key Derivation and Exchange



=====*End of Proposed Text*=====