Project	IEEE 802.16 Broadband Wireless Access Working Group <***http://ieee802.org/16***>		
Title	TEK update procedure during HO and reentry		
Date Submitted	2-May-2007		
Source(s)	Kyeong-Tae Do	Samsung	Tel: +82-31-279-5748 *kyeongtae.do@samsung.com*
Re:	802.16, Corrigendum2 [Draft 3]		
Abstract	The contribution defines the TEK update procedure during HO and re-entry from Idle mode.		
Purpose	Resolve the TEK update procedure		
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 Update procedure during HO and reentry

Samsung Electronics

1. Background

The standard defines the TEK update procedure when the HO Process Optimization Bit #1 and #2 are both set to zero. In this case, the standard suggests using SA-TEK-Update TLV in the PKMv2 SA-TEK-Response message to update TEKs. When HO Process Optimization Bit #1 and #2 are both set to zero, it is not possible to update TEKs with SA-TEK-Update TLV.

The reasons why TEKs cannot be updated are
1) When the BS sets HO Process Optimization Bit #1 and #2 to zero, the BS may not have the previous authentication information of the MS. Thus, it may not possible to "update" without the previous information.
2) The MS initializes the authentication information and starts authentication when it receives a RNG-RSP message with HO Process Optimization Bit #1 and #2 set to zero. Thus, the MS cannot "update" the TEKs.

Therefore, when the bits are zeroes, MS and BS shall exchange the TEKs, the same procedure as the initial network entry, using PKMv2 Key-Request/Response messages.

2. Suggested remedy

Modify the standard to exchange the TEKs, the same procedure as the initial network entry, using PKMv2 Key-Request/Response messages when the HO Process Optimization Bit #1 and #2 are set to zero.

3. Proposed Text Changes

[In section 6.3.22.2.8.1.6.6, perform the indicated change to page 171 of P80216-Cor2_D3]

MS context with Serving BS: Maintained with resource retain timer.

MS context with Target BS: Context is handled per bit#1 and bit#2 settings.

Bit #1=0 AND bit#2=0:Perform re-authentication and SA-TEK 3-way handshake. BS shall not ~~should~~ include SA-TEK-Update TLV in the SA-TEK-Response message. In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV.
Bit #1=0 AND bit#2=1:Not used. MS shall silently ignore RNG-RSP message.

[In section 6.3.22.2.8.1.6.6, perform the indicated change to page 172 of P80216-Cor2_D3]

SAID update:
When re-authentication is not required and SAID_update TLV is excluded from the RNG-RSP message during network re-entry, it means that SAID value(s) will be the same value(s) as the value(s) used in previous serving BS and the value of Primary SAID will be implicitly updated because MS and BS use the same value as that of Basic CID.

[In section 11.6, perform the indicated change to Table 367, page 405of P80216-Cor2_D3]

Name	Type (1 byte)	Length	Value	PHY Scope
HO Process Optimization	21	2	… (Bit #1, Bit #2) = (0, 0): Perform re-authentication and SA-TEK 3-way handshake. BS ~~should~~ shall not include SA-TEK-Update TLV in the SA-TEK-Response message. In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV. …	All

[In section 6.3.2.3.9.20, perform the indicated change to Table 37j, page 34 of P80216-Cor2_D2]

(one or more) SA-Descriptor(s)	Each compound SA-Descriptor attribute specifies an SA identifier (SAID) and additional properties of the SA. This attribute is present at the initial network entry or reentry after receipt of a RNG-RSP message with HO Process

	Optimization bits (Bit#1, Bit#2)=(0, 0)~~only~~.