Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Security Context Transfer for fast Re-authentication**	
Date Submitted	**2004-07-08**	
Source(s)	Dongkie Lee, DongIl Moon, DongRyul Lee, JongKuk Ahn, Sungho Ha SK Telecom 15F, Seoul Finance Center, 84, Taepyungpro 1 ga, Chung-gu, Seoul, 100-768, Korea	Voice: +82-2-6323-3147 Fax: +82-2-6323-4493 [mailto: {galahad,dimoon,drlee,jgahn,ss23}@sktelecom.com]
Re:	Recirculation Ballot #14b Announcement	
Abstract	To minimize the handoff interruption time, fast authentication procedure is suggested and harmonized at handoff ad-hoc utilizing RNG-REQ with HMAC-Tuple. In order to send RNG-REQ with HMAC attached, security context shall be transferred from serving BS to target BS. In this contribution, informative text for security context transfer is proposed.	
Purpose	Discuss and Adopt	
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 h"Older"er 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>.	

Security Context Transfer for fast Re-authentication

Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn
SK Telecom

1. Problem Statements

If the normal PKM initial network entry process as defined in 7.2 is to be abridged or omitted, then the MSS shall include the HMAC Tuple as the last message item in the RNG-REQ management message. If the required HMAC Tuple is invalid or omitted in the RNG-REQ management message, than the full PKM REQ/RSP sequence must be completed and cannot be omitted. The Target BS shall include a valid HMAC Tuple as the last message item in the RNG-RSP if it instructs the MSS, through the HO Process Optimization TLV, that the PKM-REQ/RSP sequence may be omitted.

2. Overview of Proposed Solutions

In order to support fast authentication, security context from serving BS to target BS should be transferred during handover procedure. In this contribution "Newer" backbone messages for security context transfer messages are defined: MSS Security Context Transfer Request, MSS Security Context Transfer Response

Table 1 Security Context Information

Type	Content
AK Related	"Older"er/"Newer"er {AK, Remaining lifetime, Key Sequence Number}
TEK Related	"Older"er/"Newer"er {TEK Parameters(TEK, Remaining Key-Lifetime, Key-Sequence-Number, CBC-IV), SAID} per SAID

3. Proposed Changes to IEEE 802.16e/D3

[Add the following after Pre-authentication section if it's accepted:]

7.x.x.x Fast Re-Authentication with full security context transfer

After a HO-REQ/RSP exchange with the serving, an MSS may seek to use fast re-authentication to effect a fast handover with the target BS. If the full security context is transferred from the serving BS to the target BS and the normal PKM initial network re-entry is to be omitted, then the MSS shall include the HMAC Tuple as the last message item in the RNG-REQ management message. If the required HMAC Tuple is invalid or omitted in the RNG-REQ management message, than the full PKM REQ/RSP sequence must be completed and cannot be omitted. The target BS shall include a valid HMAC Tuple as the last message item in the RNG-RSP if it instructs the MSS, through the HO Process Optimization TLV, that the PKM-REQ/RSP sequence may be omitted.

[Add the following after D.2.13 BS-info-response message:]

D.2.14 MSS Security Context Transfer Request

This message is sent by a target BS to a serving BS or to an ASA server to request security context information of number of MSS' during handover process.

Field	Size	Notes
Global Header	152-bit	
Message Type=?	8-bit	
For(j=0;j<Num Records; j++){		
MSS Unique identifier	48-bit	48-bit unique identifier of the MSS
}		
Security field		A means to authenticate this message

D.2.15 MSS Security Context Transfer Response

This message is sent by a serving BS or ASA server to target BS to provide security context information of a MSS during handover process. This information maybe is used for fast re-authentication.

Field	Size	Notes
Global Header	152-bit	
Message Type=?	8-bit	
For(j=0;j<Num Records; j++){		
MSS Unique identifier	48-bit	48-bit unique identifier of the MSS
"Older" AK	160-bit	
"Older" AK Remaining key Lifetime	32-bit	
"Older" AK Key Sequence Number	8-bit	
"Newer" AK	169-bit	
"Newer" AK Remaining key Lifetime	32-bit	
"Newer" AK Key Sequence Number	8-bit	
N_SAIE	8-bit	Number of Security Association Information Elements
For(k=0;k<N_SAIE;k++){		
SA Descriptor	Variable	These properties include the SAID, the SA type, and the cryptographic suite employed within the SA.
}		
For(k=0;k<N_SAIE;k++){		
"Older" TEK		
"Older" TEK Remaining key Lifetime	32-bit	
"Older" TEK Key Sequence Number	8-bit	

“Older” TEK CBC Init Vector	Equal to Block length of cipher	
“NEWER” TEK		
“Newer” TEK Remaining key Lifetime	32-bit	
“Newer” TEK Key Sequence Number	8-bit	
“Newer” TEK CBC Init Vector	Equal to Block length of cipher	
}		
}		
Security field	TBD	A means to authenticate this message