Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Secure Roaming of Key Association for Fast Handover**	
Date Submitted	**2004-10-30**	
Source(s)	Kihun Hong, Souhwan Jung Soongsil University 1-1 Sangdo-dong, Dongjak-ku, Seoul, 156-743, Korea Ki Jun Lee, Brian Lee, Jungwook Hwang DACOM 706-1, Yeoksam-Dong, Gangnam-Gu, Seoul 135-987, Korea	Voice: +82-2-820-0714 Fax: +82-2-821-7653 mailto: {kihun@cns., souhwanj@}ssu.ac.kr mobile95@dacom.net, lcm2000@chol.net, hjw33@chol.com
Re:	IEEE 802.16e Security Adhoc	
Abstract	Proposal to Secure Roaming of Key Association for Fast Handover.	
Purpose	To define Secure Roaming of Key Association procedure and messages for fast handover.	
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>.	

Secure Roaming of Key Association for fast handover

Kihun Hong, Souhwan Jung, Ki Jun Lee, Brian Lee, Jungwook Hwang
Soongsil University, DACOM

1. Problem Statements

IEEE P802.16e/D4 defines authorization via PKM extensible authentication protocol(eap) in 7.2.1.2. But in this authentication protocol, secure roaming of Key Association derived by PKM extensible authentication protocol is not defined. For fast handover, a serving BS should transfer Key Association including master key and $HMAC\_KEY_{serving}$ to the target BS. The master key is used to derive new TK, KCK, and AK. The $HMAC\_KEY_{serving}$ is used by the target BS to check or make a HMAC Tuple in the RNG-REQ and RNG-RSP messages. During handover, however, if the serving BS transfers his master key or AK, this scheme does not support perfect forward secrecy, because the target BS can derive the TK, KCK, AK, and KEK of the serving BS from the master key. Hence the protection of the master key is required before sending the master key.

Before a serving BS transmits Key Association to the target BS, a serving BS should know whether the target BS supports pre-authentication or not for fast handover. Because Key Association is important information to the MSS, the information should be transferred to the target BS in reply of the request of the MSS. If the serving BS sends Key Association by a request of the target BS, a compromised target BS can easily acquire Key Association information. These procedures should be defined in the HO-pre-notification messages and Key Association exchange messages.

2. Overview of Solution

After handover procedure, the Key Association should be transferred from the serving BS to the target BS for fast handover. The serving BS should know whether the target BS supports a pre-authentication or not before Key Association is transferred. Therefore the serving BS sends HO-pre-notification including Pre_Auth field to the target BS to ask whether target BS supports pre-authentication or not while the MSS is attempting to perform network re-entry or handover. The target BS replies with the Pre_Auth field in HO-pre-notification-response message. The security policy of the target BS may not allow pre-authentication.

After receiving a pre-authentication request from MSS, the serving BS transmits Key Association Inform message including SSID, MK_{target}, MKID, MK sequence number, MK lifetime, $HMAC\_KEY_{serving}$, $HMAC\_KEY_{serving}$ sequence number, SAID, and SA to the target BS. Through this procedure, the serving BS can prohibit that a compromised target BS acquires Key Association information. The target BS on receipt of a Key Association Inform message should reply with a Key Association Response message, or with a Key Association Reject message. After the exchange of Key Association messages, the serving BS transmits Pre-Authentication Reply message indicating that the chosen BS is populated with a PMK coupled to the identity of the requesting SS.

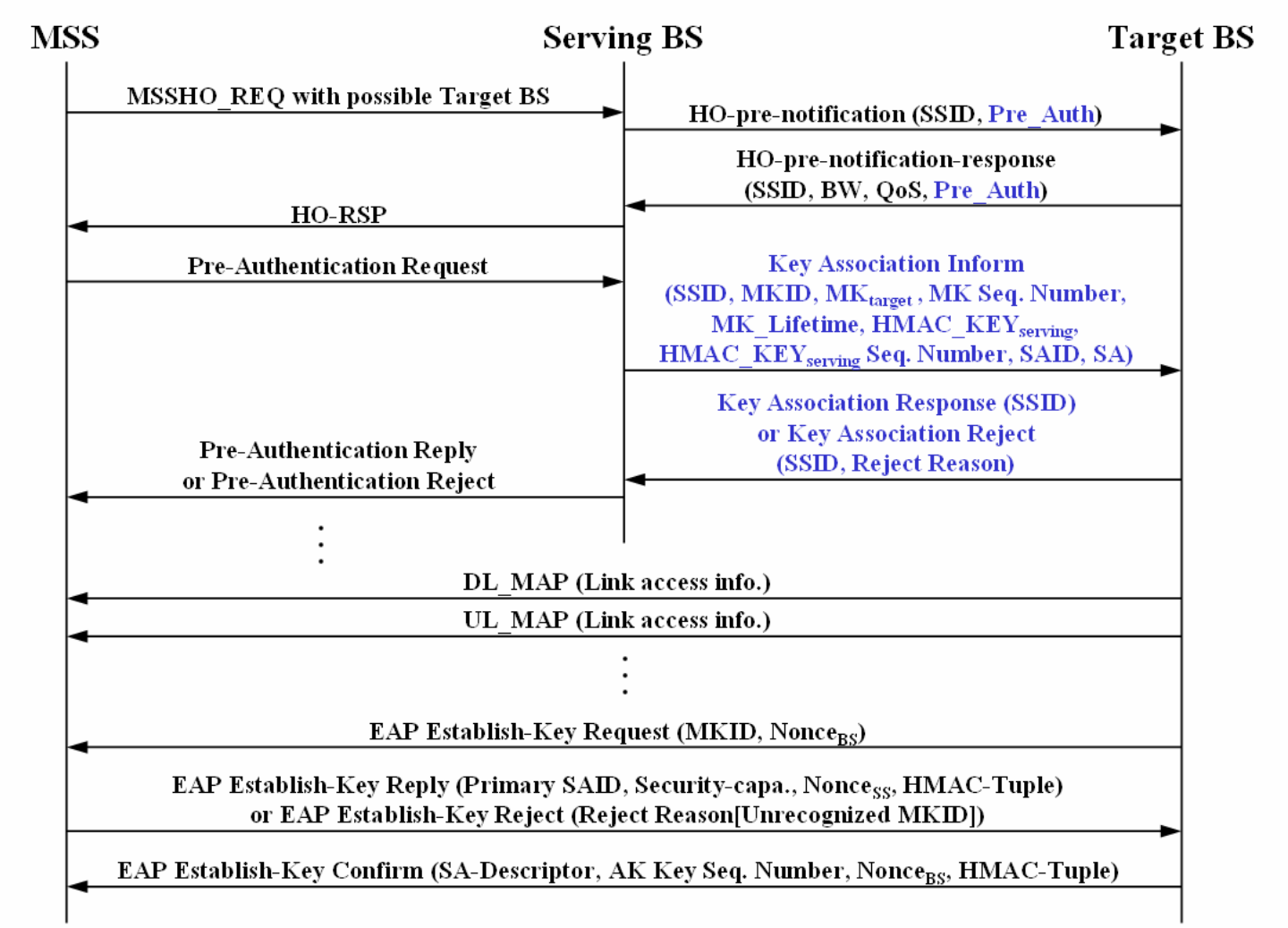
MK_{target} is generated in the serving BS as follows:

MK_{target} : Master key will be used by the target BS.

$MK_{serving}$: Master key was used by the serving BS.

$MK_{target} = PRF(MK_{serving})$

Through this process and sending MK_{target}, the serving BS can prohibit that the target BS acquires $MK_{serving}$ and derives TK, KCK, AK, KEK of the serving BS from $MK_{serving}$.



After a Key Association exchange, MSS and the target BS should perform an EAP-Establish-Key exchange. In this procedure, MSS and the target BS check MKID and share nonces. As a result of the EAP-Establish-Key exchange, they obtain the same new TK, KCK, AK, KEK, and $HMAC\_KEY_{target}$ from MK_{target}, BSID, SSID, and nonces. TEK is encrypted using a key derived from the AK.

3. Proposed Changes to 802.16e D4

[add entries to Table D8:]

Field	Size	Notes
Pre_Auth	1 bit	1 : Pre-authentication is required 0 : Pre-authentication is not required

Pre-Auth in HO-pre-notification indicates whether the pre-authentication is required or not.

[add entries to Table D9:]

Field	Size	Notes
Pre_Auth	1 bit	1 : Target BS supports pre-authentication 0 : Target BS does not support pre-authentication

Pre-Auth in HO-pre-notification-response indicates whether the target BS supports pre-authentication or not for fast handover.

D.2.16 Key Association Inform message

This message is sent by a serving BS to the target BS to provide Key Association information of a MSS after handover procedure. The target BS uses this information for fast authentication.

Field	Size	Notes
Global Header	152 bits	
Message Type = ?	8 bits	
for (j=0; j<NumRecords; j++) {		
MSS Unique identifier	48 bits	48-bit unique identifier used by MSS
MK_ID	128 bits	Master Key Identifier
MK_{target}	256 bits	Master Key will be used by the target BS
MK Remaining Lifetime	32 bits	
MK Sequence Number	16 bits	
HMAC_KEY	160 bits	
HMAC_KEY Sequence Number	4 bits	Number of MK_{target} generation
N_SAIE	8 bits	Number of Security Association Information Elements

for (k=0; i<N_SAIE; k++) {		
SA Descriptor	Variable	These properties include the SAID, the SA type, and the cryptographic suite employed within the SA.
}		
}		
Security field	TBD	A means to authenticate this message

D.2.17 Key Association Response message

This message is sent by the target BS to the serving BS to response to a Key Association Inform message.

Field	Size	Notes
Global Header	152 bits	
Message Type = ?	8 bits	
for (j=0; j<NumRecords; j++) {		
MSS Unique identifier	48 bits	48-bit unique identifier used by MSS
}		
Security field	TBD	A means to authenticate this message

D.2.18 Key Association Reject message

This message is sent by the target BS to the serving BS to reject Key Association information of the MSS.

Field	Size	Notes
Global Header	152 bits	
Message Type = ?	8 bits	
for (j=0; j<NumRecords; j++) {		
MSS Unique identifier	48 bits	48-bit unique identifier used by MSS
Reject Reason	8 bits	
}		
Security field	TBD	A means to authenticate this message