Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	comment on Secure Roaming of Key Association for Fast Handover(C80216e-04_407)	
Date Submitted	**2005-01-14**	
Source(s)	[Feng Tian] [DongXin Lu] [Rui Li] [zte] [ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057]	Voice: [86-0755-26772017] Fax: [86-0755-26772004] [mailto:tian.feng2@zte.com.cn]
Re:	802.16e/D5	
Abstract	comment on Secure Roaming of Key Association for Fast Handover(C80216e-04_407)	
Purpose	comment on Secure Roaming of Key Association for Fast Handover(C80216e-04_407)	
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>.	

comment on Secure Roaming of Key Association for Fast Handover(C80216e-04_407)

Feng Tian , Dongxin Lu , Rui Li

The Secure Roaming of Key Association for Fast Handover document only be applied to EAP-only mode , and need some enhancement . The following are the modified document .

1.Problem Statements

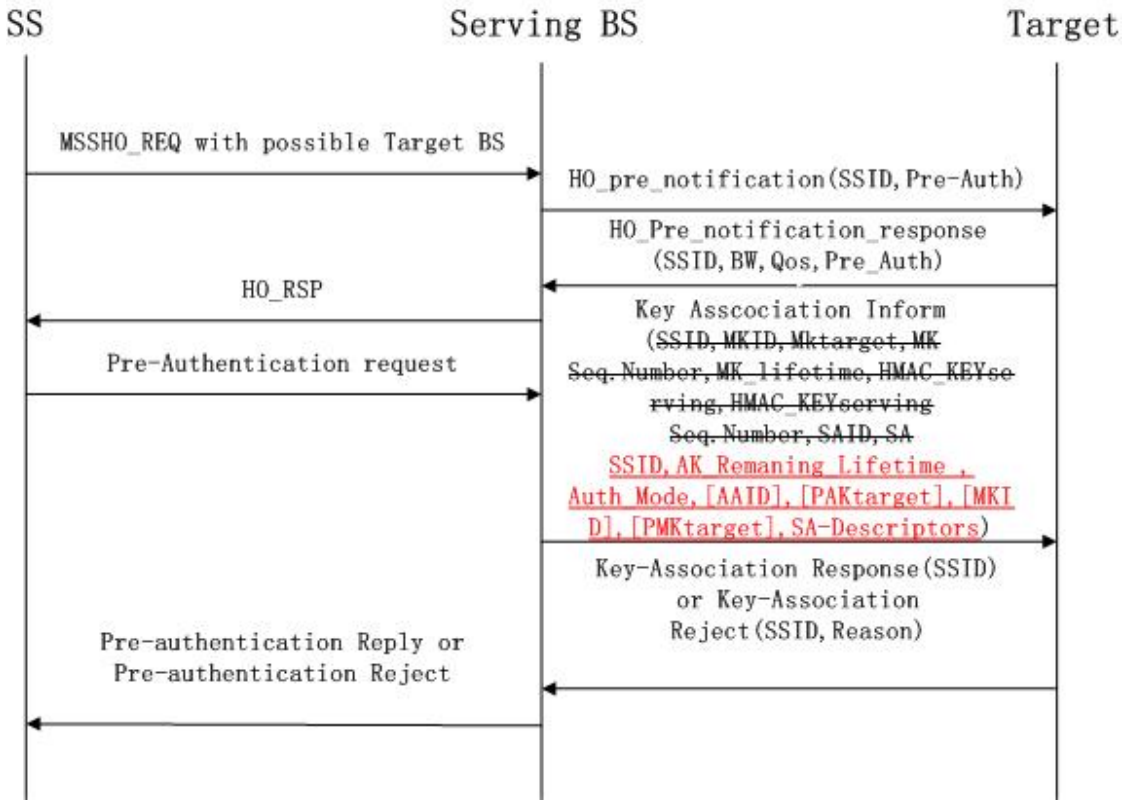
IEEE P802.16e/D4 defines authorization via PKM extensible authentication protocol(eap) in 7.2.1.2. But in this authentication protocol, secure roaming of Key Association derived by PKM extensible authentication protocol is not defined. For fast handover, a serving BS should transfer Key Association including ~~master key and HMAC_KEYserving~~ PAK and PMK to the target BS. The ~~master key~~ PAK and PMK 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~~ PAK and PMK, 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~~ PAK and PMK is required before sending the ~~master key~~ PAK and PMK. 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-notificationresponse 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, MKtarget, MKID, MK sequence number, MK lifetime, HMAC_KEYserving, HMAC_KEYserving sequence number, SAID, and SA~~ SSID , AK_Remaning_Lifetime , Auth_Mode , PAKtarget , PMKtarget , AAID , MKID , SA-Descriptors 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 and PAK coupled to the identity of the requesting SS.

~~MKtarget is generated in the serving BS as follows:~~
~~MKtarget : Master key will be used by the target BS.~~
~~MKserving : Master key was used by the serving BS.~~
~~MKtarget = PRF(MKserving)~~
PAKtarget and PMKtarget is generated in the serving BS as follows:
PAKtarget : Primary Authorization key will be used by the target BS.
PAKserving : Primary Authorization key will be used by the serving BS.
PAKtarget = PRF(PAKserving)
PMKtarget : Pairwise Master key will be used by the target BS.
PMKserving : Pairwise Master key was used by the serving BS.
PMKtarget = PRF(PMKserving)
Through this process and sending ~~Mktarget~~ PAKtarget and PMKtarget , the serving BS can prohibit that the target BS acquires ~~MKserving~~ PAKserving , PMKserving and derives ~~TK, KCK,~~ AK, KEK of the serving BS from ~~Mkserving~~ PAKserving and PMKserving.



~~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_KEYtarget from Mktarget, BSID, SSID, and nonces .TEK is encrypted using a key derived from the AK.~~
After a Key Association exchange , they obtain the same new AK from PAKtarget , PMktarget, BSID, SSID .

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~~
~~Mktarget~~	~~256 bits~~	~~Master Key will be used by the target BS~~
~~MK Remaning Lifetime~~	~~32 bits~~	
~~MK Sequence Number~~	~~16bits~~	
~~HMAC_KEY~~	~~160 bits~~	
~~HMAC_KEY Sequence Number~~	~~4 bits~~	~~Number of Mktarget generation~~
AK_Remaning_Lifetime	32bits	The remaning lifetime of the AK
Auth_Mode	8 bits	The field indicates the authorization policy used by the MSS and serving BS 1 : the authorization exchange has been used yielding a PAK and the EAP authentication exchange has been used, yielding an MSK 2 : the authorization exchange has been used yielding a PAK and the

		EAP authentication exchange has been used, but not yielding an MSK 3 : only the EAP authentication exchange has been used, yielding an MSK 4 : only the authorization exchange has been used
If (Auth_Mode = 1) {		
AAID		Authorization Association ID
PAKtarget	128 bits	PAK will be used by the target BS
MKID	128 bits	Master key identifier
PMKtarget	256 bits	PMK will be used by the target BS
}		
Eles If (Auth_Mode = 2) {		
AAID		
PAKtarget	128 bits	
}		
Eles If (Auth_Mode = 3) {		
MKID	128 bits	Master key identifier
PMKtarget	256 bits	
}		
Eles If (Auth_Mode = 4) {		
AAID		
PAKtarget	128 bits	
}		
N_SAIE	8 bits	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
}		
}		
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