

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >	
Title	<b>HO consideration in PKMv2 security</b>	
Data Submitted	<b>2005-03-17</b>	
Source(s)	Sungcheol Chang Seokheon Cho Chulsik Yoon  ETRI  <a href="#">JunHyuk Song</a> <a href="#">Jicheol Lee</a> <a href="#">Yong Chang</a>  <a href="#">Samsung</a>  <a href="#">Sanjay Bakshi</a>  <a href="#">Intel</a>	Voice: +82-42-860-5456 Fax: +82-42-861-1966 <a href="mailto:scchang@etri.re.kr">scchang@etri.re.kr</a> <a href="mailto:chosh@etri.re.kr">chosh@etri.re.kr</a> <a href="mailto:csyoon@etri.re.kr">csyoon@etri.re.kr</a>
Re:	This is a response to Sponsor Ballot 16e on P802.16e/D6.	
Abstract	The document contains suggestions on the changes in IEEE P802.16e-D6 that would support PKMv2 security in HO procedure.	
Purpose	The document is submitted for review by 802.16 Working Group members.	
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 < <a href="http://ieee802.org/16/ipr/patents/policy.html">http://ieee802.org/16/ipr/patents/policy.html</a> >, 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 < <a href="mailto:chiar@wirelessman.org">mailto:chiar@wirelessman.org</a> > 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 < <a href="http://ieee802.org/16/ipr/patents/notices">http://ieee802.org/16/ipr/patents/notices</a> >.	

HO considerations in PKMv2 security  
*Sungcheol Chang, Seokheon Cho and Chulsik Yoon*  
 ETRI  
*JunHyuk Song, Jicheol Lee, and Yong Chang*  
 Samsung  
*Sanjay Bakshi*  
 Intel

## 1 Problem Statements

Additional authorization functionalities during handover are required to omit PKM-REQ/RSP in the network re-entry procedure. The draft specification P802.16e/D6 contains that the authenticator manages the PMK from the EAP authentication and the PAK from the RAS authentication.

- BSs involved during HO procedures may have different authentication. The authorization policy negotiation is required during before the network re-entry procedure.

~~To omit PKM-REQ/RSP in the target BS of different authentication, the way to exchange PKM-REQ/RSP messages is required before the network re-entry procedure.~~

~~To support the AK generation using random numbers, the random numbers has to be exchanged before the network re-entry procedure.~~

## 2 Overview of Proposed Solution

The draft specification P802.16e/D6 support three authentication cases; the EAP authentication, the RSA authentication, and both. When considering HO process between serving BS and target BS, 3x3 (=9) authentication cases exist as follows:

Authentication cases		Normal HO Process	HO Process optimization with the Omit PKM-REQ/RSP
Serving BS	Target BS		<del>HO</del> — Authorization Policy Support negotiated at BSHO-REQ and BSHO-RSP
RSA	RSA	OK	OK
RSA	EAP	OK	N/A
RSA	RSA&EAP	OK	N/A
EAP	RSA	OK	N/A
EAP	EAP	OK	OK
EAP	RSA&EAP	OK	N/A
RSA&EAP	RSA	OK	OK
RSA&EAP	EAP	OK	OK
RSA&EAP	RSA&EAP	OK	OK

Normal HO Process consists of RNG-REQ/RSP, PKM-REQ/RSP, and REG-REQ/RSP messages. The Normal HO Process may support all the types of authentication cases, which is marked as “OK”. HO Authorization is named when all the information about authentication is integrated to and carried on HO related messages : MOV\_BSHO-REQ, MOV\_MSSHO-REQ, MOV\_BSHO-RSP, and MOV\_MSSHO-IND. HO Process optimization with the Omit PKM-REQ/RSP can be supported by Pre-Authentication messages: Pre-Auth-Request and Pre-Auth-Reply. The mark of “Transfer” is that new authentication procedures with target BS are transferred by the Pre-Auth-Transfer, which is to be newly added.

### 2.1 Remedy 1: Authorization policy negotiation when omitting PKM-REQ/RSP messages

HO process optimization allows to omit any of the network re-entry procedures. However REG-REQ/RSP could not be omitted if authentication is not omitted. That is, authorization negotiation between the MSS and new BS has to occur to omit the PKM-REQ/RSP procedure. The 16e/D6 document adapted the concept of pre-authentication, which results to the procedures HO-REQ/RSP, Pre-Auth-Request/Reply, HO-IND. The Remedy 1 handles ~~two~~ authentication negotiation procedures:

- HO authorization: MOV\_BSHO-REQ and MOV\_BSHO-RSP messages are sent by the serving BS. Those messages could carry authentication policies of the target BSs.

~~Pre-authentication: Pre-Auth-Reply message could carry authentication policies of the target BSs.~~

### 2.2 Remedy 2 : Pre-authentication transfer when PKM-REQ/RSP messages are required

~~To exchange PKM-REQ/RSP messages before the network re-entry procedure, a Pre-Auth-Transfer message is added. This~~

~~message encapsulates the authentication messages that are related to the EAP authentication or the RSA authentication and are exchanged between the MSS and the target BS. If the PKM-REQ/RSP procedure in the serving BS is compared to one in the target BS, the target BS does not provide services to the MSS when the PKM-REQ/RSP procedure in the target BS are.~~

### ~~2.3 Remedy 3 : AK generation support using random numbers~~

~~This remedy assumes AK generation using random numbers, which is submitted in other contribution. In the view of HO process optimization, it is required that the random numbers has to be exchanged before the network re-entry procedure. There are two possible ways:~~

~~IHO authorization: MOV\_BSHO-REQ and MOV\_BSHO-RSP messages carry the random number of RandomBS and MOV\_BSHO-IND carries the random number of NonceSS.~~

~~IPre-authentication: the Pre-Auth-Request message carries the RandomBS and the Pre-Auth-Reply message carries the NonceSS~~

### 3 Proposed changes to IEEE 802.16e/D6

[ Modify text in the section 6.3.2.3.51 as follows ]

#### 6.3.2.3.51 BS HO Request (MOB\_BSHO-REQ) message

The BS may transmit a MOB\_BSHO-REQ message when it wants to initiate an HO. An MS receiving this message may scan recommended neighbor BSs in this message. The message shall be transmitted on the basic CID.

**Table 108m—MOB\_BSHO-REQ message format**

Syntax	Size (bits)	Notes
MOB_BSHO-REQ_Message_Format() {		
Management Msg Type = 56	8	
<b>Network Assisted HO supported</b>	1	Indicates that the BS supports Network Assisted HO
Mode	3	000: HHO request 001: SHO/FBSS request: Anchor BS update with CID update 010: SHO/FBSS request: Anchor BS update without CID update 011: SHO/FBSS request: Active Set update with CID update 100: SHO/FBSS request: Active Set update without CID update 101: SHO/FBSS request: Active Set update with CID update for newly added BS 110: SHO/FBSS request: Active Set update with CID update and CQICH allocation for newly added BS 111: reserved
If (Mode == 000) {		
N_Recommended	8	
For (i=0 ; j<N_Recommended ; j++) {		N_Recommended can be derived from the known length of the message
Neighbor BSID	48	
Service level prediction	8	
HO process optimization	8	
HO_ID_included_indicator	1	To indicate if the field HO_IND is included
If (HO_ID_included_indicator == 1) {		
HO_ID	8	ID assigned for use in initial ranging to the target_BS once this BS is selected as the target BS
}		
<u>HO_authorization_policy_indicator</u>	<u>1</u>	<u>To indicate if authorization negotiation is used in HO procedure.</u> <u>0: EAP authorization and the value of the MAC mode field in the current BS (default)</u> <u>1: The authorization policy for the target BS is negotiated.</u>
<u>If (HO_authorization_policy_indicator == 1) {</u>		
<u>HO_authorization_policy_support</u>	<u>7</u> <del>8</del>	<u>Bit #0: RSA authorization</u> <u>Bit #1: EAP authorization</u> <u>Bit #2: Authenticated-EAP authorization</u> <u>Bit #3: HMAC supported</u> <u>Bit #4: OMAC supported</u> <u>Bit #5: 64-bit Short-HMAC</u> <u>Bit #6: 80-bit Short-HMAC</u> <u>Bit #7: 96-bit Short-HMAC</u>
<u>}</u>		
}		
}		
else if (Mode == 001) {		
.... All the context from here will be maintained in the table (skip rewriting the remained text).		

.... All the context from here will be maintained (skip rewriting the remained text)

[ Modify text in the section 6.3.2.3.53 as follows ]

#### 6.3.2.3.53 BS HO Response (MOB\_BSHO-RSP) message

The BS shall transmit an MOB\_BSHO-RSP message upon reception of MOB\_MSHO-REQ message. The message shall be transmitted on the basic CID.

**Table 108o—MOB\_BSHO-RSP message format**

Syntax	Size (bits)	Notes
MOB_BSHO-RSP_Message_Format() {		
Management Msg Type = 58	8	
Mode	3	0b000: HHO request 0b001: SHO/FBSS request: Anchor BS update with CID update 0b010: SHO/FBSS request: Anchor BS update without CID update 0b011: SHO/FBSS request: Active Set update with CID update 0b100: SHO/FBSS request: Active Set update without CID update 0b101: SHO/FBSS request: Active Set update with CID update for newly added BS 0b110: : SHO/FBSS request: Active Set update with CID update and CQICH allocation for newly added BS 0b111: <i>reserved</i>
If (Mode == 0b000) {		
N_Recommended	8	
For (i=0 ; j<N_Recommended ; j++) {		Neighbor base stations shall be presented in an order such that the first presented is the one most recommended and the last presented is the least recommended.
Neighbor BSID	48	
Preamble index/ Preamble Preserved Subchannel Index	8	For the SCA and OFDMA PHY this parameter defines the PHY specific preamble for the neighbor BS. For the OFDM PHY the 5 LSB contain the active DL subchannel index for the neighbor BS. The 3 MSB shall be Reserved and set to '0b000'.
Service level prediction	8	
HO process optimization	8	
HO_ID_included_indicator	1	To indicate if the field HO_IND is included
If (HO_ID_included_indicator == 1) {		
HO_ID	8	ID assigned for use in initial ranging to the target BS once this BS is selected as the target BS
}		
HO_authorization_policy_indicator	1	<a href="#">To indicate if authorization negotiation is used in HO procedure.</a> 0: EAP authorization and the value of the OMAC Supported field in the current BS (default) 1: The authorization policy for the target BS is negotiated.
If (HO_authorization_policy_indicator == 1) {		
HO_authorization_policy_support	78	<a href="#">Bit #0: RSA authorization</a> <a href="#">Bit #1: EAP authorization</a> <a href="#">Bit #2: Authenticated-EAP authorization</a> <a href="#">Bit #23: HMAC supported</a> <a href="#">Bit #34: OMAC supported</a> <a href="#">Bit #45: 64-bit Short-HMAC</a> <a href="#">Bit #56: 80-bit Short-HMAC</a> <a href="#">Bit #67: 96-bit Short-HMAC</a>
}		
}		
}		
else if (Mode == 0b001) {		
.... All the context from here will be maintained in the table (skip rewriting the remained text).		

.... All the context from here will be maintained (skip rewriting the remained text)

~~[-Modify text in the section 6.3.2.3.54 as follows-]~~

#### 6.3.2.3.54 HO Indication (MOB\_HO\_IND) message

~~An MS shall transmit a MOB\_HO\_IND message for final indication that it is about to perform a HO. When the MS cancels or rejects the HO, the MS shall transmit a MOB\_HO\_IND message with appropriate HO\_IND type field. The message shall be~~

transmitted on the basic CID.

Table 108p—MOB\_HO\_IND message format

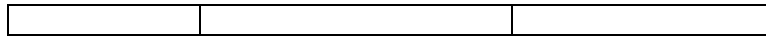
Syntax	Size (bits)	Notes
MOB_BSHO_IND_Message_Format() {		
-Management Msg Type = 59	8	
-reserved	6	Reserved; shall be set to zero
-Mode	2	0b00: HHO request 0b01: SHO/FBSS request: Anchor BS update 0b10: SHO/FBSS request: Active Set update 0b11: reserved
If (Mode == 0b00) {		
-HO_IND_type	2	0b00: serving BS release 0b01: HO cancel 0b10: HO reject 0b11: reserved
-If (HO_IND_type == 0b00) {		
-Target_BS_ID	48	Applicable only when HO_IND_type is set to 0b00.
}		
else if (Mode == 0b01) {		
..... All the context from here will be maintained in the table (skip rewriting the remained text):		

..... All the context from here will be maintained (skip rewriting the remained text)

{ Modify Table 26 as follows }

Table 26—PKM message codes

Code	PKM message type	MAC Management message name
0-2	reserved	—
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	EAP Transfer	PKM-REQ/PKM-RSP
14	Pre-Auth Request	PKM-REQ
15	Pre-Auth Reply	PKM-RSP
16	Pre-Auth Reject	PKM-RSP
17	PKMv2 Auth Request	PKM-REQ
18	PKMv2 Auth Reply	PKM-RSP
19	Key Update Command	PKM-RSP
20	Protected EAP	PKM-REQ/PKM-RSP
21	SA-TEK Challenge	PKM-RSP
22	SA-TEK Request	PKM-REQ
23	SA-TEK Response	PKM-RSP
24-255 reserved		



~~[Modify text from the section 6.3.2.3.9.12 to the section 6.3.2.3.9.14 as follows]~~

~~6.3.2.3.9.12 Pre-Auth-Request message~~

~~The Pre-Auth-Request message is sent by the MS to the BS to establish Pairwise Master Key with the target BS for handoff.~~

~~Code: 18~~

~~Attributes are shown in Table 37b.~~

~~Table 37b—PKM Pre-Auth-Request attributes~~

<del>Attribute</del>	<del>Contents</del>
<del>Target BSID</del>	<del>The BSID to which an MS will connect after HO</del>
<del>OMAC Tuple</del>	<del>Message Digest calculated using OMAC_KEY</del>

~~The target BSID attribute contains one or more target BSIDs. The MS notified the serving BS of these BSID(s) for handoff.~~

~~The OMAC Tuple attribute shall be the final attribute in the message's attribute list.~~

~~Inclusion of the keyed digest allows the receiving MS to authenticate the Pre-Auth-Request.~~

~~6.3.2.3.9.13 Pre-Auth-Reply message~~

~~Sent by the BS to a client SS in response to Pre-Auth-Request or in an unsolicited manner, the Pre-Auth-Reply message contains one or more target BSIDs and an OMAC tuple.~~

~~Code: 19~~

~~Attributes are shown in Table 37c.~~

~~Table 37c—PKM Pre-Auth-Reply attributes~~

<del>Attribute</del>	<del>Contents</del>
<del>Target BSID</del>	<del>BSID that MS will connect after HO</del>
<del>OMAC Tuple</del>	<del>Message Digest calculated using OMAC_KEY</del>

~~The OMAC Tuple attribute shall be the final attribute in the message's attribute list.~~

~~Inclusion of the keyed digest allows the receiving MS to authenticate the Pre-Auth-Request.~~

~~6.3.2.3.9.14 Pre-Auth-Reject message~~

~~Sent by the BS to a client MS, receipt of a Pre-Auth-Reject message indicates to the receiving MS, that the BS identified by the BSID in the associated Pre-Auth-Request message and repeated in the response, is not populated with a valid PMK.~~

~~Code: 20~~

~~Attributes are shown in Table 37d.~~

~~Table 37d—PKM Pre-Auth-Reject attributes~~

<del>Attribute</del>	<del>Contents</del>
<del>Target BSID</del>	<del>BSID that MS will connect after HO</del>
<del>OMAC Tuple</del>	<del>Message Digest calculated using OMAC_KEY</del>

~~The OMAC Tuple attribute shall be the final attribute in the message's attribute list.~~

~~Inclusion of the keyed digest allows the receiving MS to authenticate the Pre-Auth-Request.~~