Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**HO consideration in PKMv2 security**	
Data Submitted	**2005-03-09**	
Source(s)	Sungcheol Chang Seokheon Cho Chulsik Yoon ETRI	Voice: +82-42-860-5456 Fax: +82-42-861-1966 scchang@etri.re.kr chosh@etri.re.kr csyoon@etri.re.kr
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 <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:chiar@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>.	

HO considerations in PKMv2 security

Sungcheol Chang, Seokheon Cho and Chulsik Yoon

ETRI

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 nework 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 nework re-entry procedure.
- To support the AK generation using random numbers, the random numbers has to be exchanged before the nework 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		HO Authorization	Pre-Authentication
RSA	RSA	OK	OK	OK
RSA	EAP	OK	N/A	Transfer
RSA	RSA&EAP	OK	N/A	Transfer
EAP	RSA	OK	N/A	Transfer
EAP	EAP	OK	OK	OK
EAP	RSA&EAP	OK	N/A	Transfer
RSA&EAP	RSA	OK	OK	OK
RSA&EAP	EAP	OK	OK	OK
RSA&EAP	RSA&EAP	OK	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 nework 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 nework re-entry procedure. Threre are two possible ways:

- HO 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.
- Pre-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	
Network Assisted HO supported	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
}		
HO_authorization indicator	1	To indicate if authorization negotiation is used in HO procedure.
If (HO_authorization indicator == 1) {		
HO_authorization_policy_support	4	Bit #0: RSA authorization Bit #1: EAP authorization Bit #2: OMAC supported (if set to 0, HMAC is the default) Bit #3: Different RandomBS supported (if set to 0, common RandomBS is default)
If (Different RandomBS supported) {		
RandomBS	64	A freshly generated random number of 64 bits (BS-specific)
}		
}		
}		
If (any of the recommended BSs use common RandomBS) {		
RandomBS	64	A freshly generated random number of 64 bits that is common to the recommented BSs with HO_authorization_indicator == 1 and the common RandomBS
}		
}		
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: *reserved*
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 Presen 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 indicator	1	To indicate if authorization negotiation is used in HO procedure.
If (HO_authorization indicator == 1) {		
HO_authorization_policy_support	4	Bit #0: RSA authorization Bit #1: EAP authorization Bit #2: OMAC supported (if set to 0, HMAC is the default) Bit #3: Different RandomBS supported (if set to 0, common RandomBS is default)
If (Different RandomBS supported) {		
RandomBS	64	A freshly generated random number of 64 bits (BS-specific)
}		
}		
}		
If (any of the recommended BSs use common RandomBS) {		
RandomBS	64	A freshly generated random number of 64 bits that is common to the recommented BSs with HO_authorization_indicator == 1 and the common RandomBS
}		
}		
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.
}		
HO_authorization indicator	1	To indicate if authorization negotiation is used in HO procedure.
If (HO_authorization_indicator == 1) {		
NonceSS	64	A 64-bit number chosen by the SS (once per protocol run). It can be a counter or a random number.
}		
}		
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	Pre-Auth-Transfer	PKM-REQ/PKM-RSP
~~17~~18	PKMv2 Auth-Request	PKM-REQ
~~18~~19	PKMv2 Auth-Reply	PKM-RSP
~~19~~20	Key Update Command	PKM-RSP
~~20~~21	Protected EAP	PKM-REQ/PKM-RSP
~~21~~22	SA-TEK-Challenge	PKM-RSP
~~22~~23	SA-TEK-Request	PKM-REQ
~~23~~24	SA-TEK-Response	PKM-RSP
~~24~~25–255 *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~~ Primary Master Key (PMK) with the target BS for handoff.

Code: 18

Attributes are shown in Table 37b.

Table 37b—PKM Pre-Auth-Request attributes

Attribute	Contents
Target BSID	The BSID to which an MS will connect after HO
NonceSS	A 64-bit number chosen by the SS (once per protocol run). It can be a counter or a random number.
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMAC_KEY

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

The OMAC/HMAC 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/HMAC tuple. The number of Authorization Polocy Support and the RandomBS attributes are matched with the number of target BSID attributes.

Code: 19

Attributes are shown in Table 37c.

Table 37c—PKM Pre-Auth-Reply attributes

Attribute	Contents
Target BSID	BSID that MS will connect after HO
Authorization Policy Support	Authorization policies supported in the target BS
RandomBS	A freshly generated random number of 64 bits.
NonceSS	The 64-bit number from the Pre-Auth-Request.
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMC_KEY

The OMAC/HMAC 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 **and/or a valid PAK**.

Code: 20

Attributes are shown in Table 37d.

Table 37d—PKM Pre-Auth-Reject attributes

Attribute	Contents
Target BSID	BSID that MS will connect after HO
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMAC_KEY

The OMAC/HMAC 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.

6.3.2.3.9.15 Pre-Auth-Transfer message

The Pre-Auth-Transfer message is sent by the MS or the serving BS to exchange PKM messages between the MS and the target BS.

Code: 21

Attributes are shown in Table 37e.

Table 37e—PKM Pre-Auth-Transfer attributes

Attribute	Contents
Target BSID	BSID that MS will connect after HO
PKM authorization protocol	Contains the PKM authorization data, interpreted not in the serving BS but in the target BS
OMAC/HMAC Tuple	Message Digest calculated using OMAC_KEY/HMAC_KEY

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

Inclusion of the keyed digest allows the receiving MS or BS to authenticate the Pre-Auth-Transfer.