Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>
Title	**Multicast Key Update over IEEE 802.16.1a**
Date Submitted	**2012-01-09**
Source(s)	Eunkyung Kim, Sungcheol Chang, Won-Ik Kim, Seokki Kim, Sungkyung Kim, Miyoung Yun, Hyun Lee, Chulsik Yoon, Kwangjae Lim ETRI Voice: +82-42-860-5415 E-mail: ekkim@etri.re.kr scchang@etri.re.kr
Re:	"IEEE 802.16n-11/0029," in response to Call for Comments on GRIDMAN AWD
Abstract	Multicast key update on GRIDMAN Amendment Draft Standard
Purpose	To discuss and adopt the proposed text in the draft amendment document on GRIDMAN
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.
Copyright Policy	The contributor is familiar with the IEEE-SA Copyright Policy <http://standards.ieee.org/IPR/copyrightpolicy.html>.
Patent Policy and Procedures	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.

Multicast Key Update over IEEE 802.16.1a

Eunkyung Kim, Sungcheol Chang, Won-Ik Kim, Seokki Kim, Sungkyung Kim, Miyoung Yun, Hyun Lee, Chulsik Yoon, Kwangjae Lim
ETRI

1. Introduction

In IEEE 802.16.1a[3], multicast security key is described and hierarchy and how to derived MTEK and MCMAC key from the MAK. To support multicast operation, MAK is defined as a pre-shared key and shared by MSs in a multicast group. However, MTEK may be updated (or re-keyed) using PKM-RSP sent by HR-BS

Thus, this contribution provides some parameter in PKM-RSP to update security key of multicast communication.

2. References

[1] IEEE 802.16n-10/0048r3, 802.16n System Requirement Document including SARM annex, November 2011.
[2] IEEE 802.16n-11/0032, P802.16n Draft AWD, November 2011.
[3] IEEE 802.16n-11/0033, P802.16.1a Draft AWD, November 2011.
[4] EEE P802.16Rev3/D3, IEEE Draft Standard for Local and metropolitan area networks; Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," November 2011.
[5] IEEE P802.16.1^{TM}/D3, IEEE Draft for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems, November 2011.

3. Proposed Text on the IEEE 802.16.1a Amendment Draft Standard

[----------Start of Text Proposal----------]

[Remedy1: Change Table 70 - AAI-PKM-RSP message field description in line 2, page 40, in the 802.16.1a AWD as follows:]

6.2.3.43 Privacy key MAC Control messages (AAI-PKM-REQ/AAI-PKM-RSP)

[Modify Table 70, AAI-PKM-RSP message field description, as indicated:]

Table 70 - AAI-PKM-RSP message field description

Field	Size (bits)	Value/Description	Conditions
PKM v3 message type code	4	- PKMv3 EAP-Transfer; PKM v3 message code = 2 - PKMv3 Key_Agreement-MSG#1; PKM v3 message code = 3 - PKMv3 Key_Agreement-MSG#3; PKM v3 message code = 5 - PKMv3 TEK-Reply; PKM v3 message code = 7 - PKMv3 TEK-Invalid; PKM v3 message code = 8 ~~9-16:*Reserved*~~ - Peer_KeyAgreement_MSG #1; PKMv3 message code = 9 - Peer_KeyAgreement_MSG#3; PKMv3 message code = 11 - PKMv3 MTEK-Reply; PKMv3 message code = 12 ~~12~~13-16; *Reserved*	
.....	...	.....	...
if (PKMv3 message code == 12) {			
Multicast Group ID	12	Multicast Group ID to update METK	
FID	4	FID to update MTEK	
COUNTER_MTEK	16	COUNTER_MTEK used for deriving current MTEK	
MEKS	2	Encryption key sequence number for current MTEK	
}			

[*Remedy2: Change Table 71 - PKMv3 message types in line 3, page 42, in the 802.16.1a AWD as follows:*]

[Modify Table 71, PKMv3 message types, as indicated:

Table 71- PKM v3 message types

Code	PKM message type	MAC control message name
1	PKMv3 Reauth-Request	AAI-PKM-REQ
2	PKMv3 EAP-Transfer	AAI-PKM-REQ/AAI-PKM-RSP
3	PKMv3 Key_Agreement-MSG#1	AAI-PKM-RSP
4	PKMv3 Key_Agreement-MSG#2	AAI-PKM-REQ
5	PKMv3 Key_Agreement-MSG#3	AAI-PKM-RSP
6	PKMv3 TEK-Request	AAI-PKM-REQ
7	PKMv3 TEK-Reply	AAI-PKM-RSP
8	PKMv3 TEK-Invalid	AAI-PKM-REQ/AAI-PKM-RSP
9	~~PKMv3 MulticastKey-Update~~Peer_KeyAgreement_MSG #1	AAI-PKM-RSP
10	Peer_KeyAgreement_MSG #2	AAI-PKM-REQ
11	Peer_KeyAgreement_MSG #3	AAI-PKM-RSP
12	PKMv3 MTEK-Reply	AAI-PKM-RSP
~~9~~10~~10~~13-16	*Reserved*	-

[*Remedy3: Insert the following text into the end of 6.2.3.43.9 in the 802.16.1a AWD.*]

Add new section after 6.2.3.43.8 as indicated:

6.2.3.43.9 PKMv3 MTEK-Reply message

The HR-BS transmits the PKMv3 MTEK-Reply message to update MTEK of HR-MSs in a multicast group.

Code: 12

Attributes are shown in Table 79a.

Table 79a - PKMv3 MTEK-Reply message attributes

Attribute	Contents
Multicast Group ID	The identifier of the multicast group of which HR-MS is a member of
FID	The FID of the multicast group of which HR-MS is a member of
COUNTER_MTEK	The counter of MTEK that the HR-MS uses to derive the MTEK
MEKS	Encryption key sequence number for MTEK
MCMAC digest	Message digest calculated using MAK

[----------End of Text Proposal----------]