Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Associated GKEK sequence number and GKEK-Parameters**
Data Submitted	**2006-09-21**

Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr

Re:	IEEE Std 802.16e-2005
Abstract	This contribution clarifies unstable usage of GKEK-related parameters for the MBRA.
Purpose	Adoption of proposed changes into Std. 802.16e-2005
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>.

Associated GKEK sequence number and GKEK-Parameters

Seokheon Cho, Sungcheol Chang and Chulsik Yoon

ETRI

Introduction

A commentary (# 5144) which was made a resolution at the TGe Chicago June meeting was accepted. But, some parts of the corresponding contribution (IEEE C802.16e-05/278, “Clarification of GKEK-related Parameters for the MBRA”) are not fully applied into the IEEE P802.16-2005.

The missing parts, which are descriptions of an Associated GKEK Sequence Number field and a GKEK-Parameters field, are really necessary.

This contribution contains only omitted part in the accepted contribution (IEEE C802.16e-05/278).

Proposed Changes into IEEE Std 802.16e-2005

[Insert new sections in the section 11.9:]

11.9.38 Associated GKEK Sequence Number

Description: This attribute indicates the GKEK Sequence Number of a GKEK-Parameters attribute under the same GSAID. When a BS transfers the GTEK, BS shall encrypt the GTEK using the GKEK corresponding to the Associated GKEK Sequence Number

Type	Length	Value(compound)
46	1	Associated GKEK sequence number

11.9.39 GKEK-Parameters

Description: This attribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all the security parameters relevant to a particular generation of a GSAID for encrypting the GTEK in the multicast or broadcast service. A summary of the GKEK-Parameters attribute format is shown below.

Type	Length	Value(compound)
47	variable	The Compound field contains the subattributes as defined in the following Table.

Table– GKEK-Parameters subattributes

Attributes	Contents
GKEK	Group Key Encryption Key, encrypted with KEK derived from AK
Key-Lifetime	GKEK's remaining lifetime
Key-Sequence-Number	GKEK's sequence number

The GKEK lifetime should be made by n times the GTEK lifetime as follows.

GKEK lifetime = n * GTEK lifetime

, where n is an integer (more than 1)