
Project **IEEE 802.16 Broadband Wireless Access Working Group** <<http://ieee802.org/16>>

Title **The MBRA for the MBS**

Data **2005-06-16**

Submitted

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

Re: IEEE P802.16e/D8

Abstract The existing PKMv2 is somewhat unorganized and insecure security framework. This contribution provides a resolution for the efficient keying distribution for the MBS service.

Purpose Adoption of proposed changes into P802.16e/D8

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>>.

The MBRA for the MBS

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon

ETRI

Jicheol Lee, Junhyuk Song

Samsung Electronics

Introduction

0.1 IEEE P802.16e/D8 Status and Problems

Even though the MBS is defined, the keying distribution method for the encryption of the MBS traffic data is not defined.

There are several keys for the MBS, e.g., MAK (MBS Authorization Key), MGTEK (MBS Group Traffic Encryption Key), and MTK (MBS Transport Key).

The MAK may be generated and transported from the MBS application layer.

The MGTEK is used to derive the MTK, but the generation and transport methods of this key are not defined. Therefore, that method needs to be obviously specified.

In addition, the MTK used to encrypt the MBS traffic data is defined in the IEEE P802.16e/D7 as follows.

$$\text{MTK} \leftarrow \text{Dot16KDF}(\text{MAK}, \text{MGTEK}, 128)$$

The current derivation method for the MTK is not related to the SS's AK (Authorization Key). Since the MTK should be transmitted to the only authorized SS, the MTK should have relationship with the AK. It is reasonable that the MTK should be derived from a child key of the AK, such as the GTEK.

0.2 Proposed Solutions

Both an SS and BS have to share a new specific key, e.g., the MTK, to be used for encrypting the MBS traffic data. An SS shall send the Key-Request message to derive the MTK. A BS shall respond to the requesting SS with a PKMv2 Key Reply message. By exchanging these two messages, an SS can get a GTEK to be used for the derivation of the MTK. The MGTEK doesn't need any more.

In addition, the wrong current derivation method for the MTK shall be changed as follows:

$MTK \leftarrow \text{Dot16KDF}(MAK, GTEK, 128)$

0.3 MBS GSA Clarification

MGTEK's key encryption algorithm and key transport mechanism is same as those of GTEK.

This contribution clarifies such mechanism.

Proposed Changes into IEEE P802.16e/D8

[Modify sub-clause 7.2.2.2.8 as follows:]

7.2.2.2.8 MBS Transport Key (MTK)

The generation and transport of the MAK (MBS AK) is outside the scope of the 802.16 standard. It is provided through means defined at higher layers. However the ~~keying~~ key such as the MTK is used in the link cipher, therefore its existence needs to be defined in layer 2.

The MTK is used to ~~protect MBS data~~ encrypt the MBS traffic data. It is defined as follows:

$MTK \leq \text{Dot16KDF}(MAK, MGTEK, 128)$

The MGTEK is the GTEK for the MBS. An SS can get the GTEK by exchanging the PKMv2 Key Request message and the PKMv2 Key Reply message with a BS or by receiving the PKMv2 Group Key Update Command message from a BS. The generation and transport of the GTEK is defined as in section 6.3.2.3.9 and 7.9.

[Insert red text below 7.2.2.3.3 as follows:]

7.2.2.3.3 MBS Group Security Association

The primary keying material in the MBS Group Security Association is the MAK. This serves the same function as the AK in the Authorized Association, however the MAK is provisioned by an external entity, such as an MBS server. The MAK may be common among members of an MBS group.

The contents of an MBSGSA are:

The MAK, a 160-bit MBS AK, serves the same function as the AK but local to the MBSGSA.

The MGTEK, a 128-bit MBS Group Traffic Encryption Key, used indirectly to protect MBS traffic. It is updated more frequently than the MAK.

The MTK (MBS Traffic Key) a 128-bit key used to protect MBS traffic, derived from the MAK and MGTEK.

The MGTEK is a random number provisioned by the access network such as a BS as an access network authorization key. It is only used for generating MTK together with MAK.

In MBS Group Security Association, the usage of MGTEK is same as that of GTEK.

Key encryption algorithm and key transport mechanism of GTEK shall be also applied for MGTEK.

[Insert red text below 7.2.2.4.2 as follows:]

7.2.2.4.2 GKEK context

The GKEK is the head of the group key hierarchy. There is a separate GKEK for each group (each GSA). This key is randomly generated by the BS and transferred to the SS encrypted with KEK. It is used to encrypt group TEKs (GTEK) when broadcasting them to all SSs. The GKEK context is described in the table:

GKEK or KEK can be used for encrypting MGTEK for MBS GSA.