Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Clarification of GKEK-related Parameters for the MBRA**
Data Submitted	**2005-06-08**

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 P802.16e/D8
Abstract	This contribution clarifies unstable usage of GKEK-related parameters for the MBRA.
Purpose	Adoption of proposed changes into P802.16e/D8

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>.

Clarification of GKEK-related Parameters for the MBRA

Seokheon Cho, Sungcheol Chang and Chulsik Yoon

ETRI

Introduction

The MBRA is used to refresh keying material efficiently for the multicast or broadcast service. The GTEK encrypts the multicast or broadcast traffic data. To transfer GTEK safely, a BS transmits the encrypted GTEK by the GKEK to an MS.

A proposal that both MS and BS maintain the GKEK lifetime being independent of the GTEK lifetime was accepted at #35 meeting. In other words, both MS and BS maintain the GTEK-related parameters and the GKEK-related parameters separately. To operate accepted concept, however, it is insufficient and needs to consider supplementary items as follows.

- It needs a field to associate the GTEK with the GKEK, because both an MS and BS maintain the GTEK-related parameters and the GKEK-related parameters separately.
- It needs a field to identify the GKEK, because both MS and BS should be able to support up to two GKEKs simultaneously.
- It needs that the GKEK-parameters should be included in the PKMv2 Key-Reply message for sharing the GKEK-parameters between an MS and BS.

This contribution provides a solution for above items.

Proposed Changes into IEEE P802.16e/D8

[Change sub-clauses 6.3.2.3.9.26 as follows]

6.3.2.3.9.26 Key Update Command messages

This message is sent by BS to push the GTEK and/or GKEK parameters to MSs served with the specific multicast service or broadcast service.

Code: 27

Attributes are shown in Table 37p.

Table 37p- PKMv2 Group Key ~~u~~Update ~~c~~Command attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
GSAID	Group Security Association ID
Key Push Modes	Usage code of Key Update Command message
Key Push Counter	Counter one greater than that of older generation
GTEK-Parameters	"Newer" generation of ~~key~~ GTEK-related parameters relevant to GSAID The GTEK-Parameters is the TEK-Parameters for multicast or broadcast service.
GKEK-Parameters	"Newer" generation of GKEK-related parameters for multicast or broadcast service. ~~Group Key Encryption Key protected by KEK derived from shared AK and other GKEK parameter e.g. Key lifetime.~~
CMAC/HMAC-Digest	Message integrity code of this message.

Key Sequence Number is the sequence number of the synchronized AK (Authorization Key) between an MS and a BS.

GSAID is SAID for the multicast group or the broadcast group. The type and length of the GSAID is equal to ones of the SAID.

There are two types in ~~the~~ a PKMv2 Group Key Update Command message, GKEK update mode and GTEK update mode. The former is used to update GKEK and the latter is used to update GTEK for the multicast service or the broadcast service. Key Push Modes indicates ~~this~~ the usage code of ~~the~~ a PKMv2 Group Key Update Command message. The PKMv2 Group Key Update Command message for the GKEK update mode is carried on the Primary Management connection, but one for the GTEK update mode is carried on the Broadcast connection. A few attributes in ~~the~~ a PKMv2 Key Update Command message shall not be used according this Key Push Modes attribute's value. See 11.9.33 for details.

Key Push Counter is used to protect for replay attack. This value is one greater than that of older generation.

~~The~~ A PKMv2 Group Key Update Command message contains only newer generation of key parameters, because this message inform an MSS of next traffic key material. The GTEK-Parameters attribute is a compound attribute containing all of the keying material corresponding to a newer generation of a GSAID's GTEK. This would include the GTEK, the GTEK's remaining key lifetime, the GTEK's key sequence number, the associated GKEK sequence number, and the cipher block chaining (CBC) initialization vector. The GTEK is TEK for the multicast group or the broadcast group. The type and length of the GTEK is equal to ones of the TEK. The GKEK (Group Key Encryption Key) can be randomly generated from a BS or a certain network node (i.e., an ASA server). The GKEK should be identically shared within the same multicast group or the broadcast group. The GTEK is encrypted with GKEK for the multicast service or the broadcast service. The GKEK-Parameters attribute contains the GKEK encrypted by the KEK, GKEK sequence number, and GKEK lifetime. See 7.5.4.4 for details.

The CMAC/HMAC-Digest attribute shall be the final attribute in the message's attribute list. Inclusion of the keyed digest allows the receiving client to authenticate the PKMv2 Group Key Update Command message. The CMAC/HMAC-Digest's authentication key is derived from the AK for the GKEK update mode and GKEK for the GTEK update mode. See 7.5.4.3 for details.

[Change sub-clauses 6.3.2.3.9.21 as follows]

6.3.2.3.9.21 PKMv2 Key-Request message

A MS sends a PKMv2 Key-Request message to the BS to request new ~~TEK (or GTEK) and traffic keying material~~ TEK and TEK-related parameters (GTEK and GTEK-related parameters for the multicast or broadcast service) or GKEK and GKEK-related parameters for the multicast or broadcast service.

Code: ~~22~~ 23

Attributes are shown in Table 37k.

Table 37k-PKMv2 Key Request attributes

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier - GSAID for multicast or broadcast service
Nonce	A random number generated in a MS
HMAC Digest/CMAC Digest	Message Digest calculated using AK

The HMAC-Digest attribute or the CMAC-Digest attribute shall be the final attribute in the message's attribute list.

Inclusion of the HMAC-Digest or the CMAC digest allows the MS and BS to authenticate the PKMv2 Key-Request message. The HMAC-Digest or the CMAC-Digest's authentication key is derived from the AK.

[Change sub-clauses 6.3.2.3.9.22 as follows]

6.3.2.3.9.22 PKMv2 Key-Reply message

The BS responds to a MS's PKMv2 Key-Request message with a PKMv2 Key-Reply message.

Code: ~~23~~ 24

Attributes are shown in Table 37l.

Table 37l-PKMv2 Key-Reply attributes

Attribute	Contents
Key Sequence Number	AK sequence number

SAID	Security association identifier - GSAID for multicast or broadcast service
TEK-Parameters	"Older" generation of key parameters relevant to SAID - GTEK-Parameters for the multicast or broadcast service
TEK-Parameters	"Newer" generation of key parameters relevant to SAID - GTEK-Parameters for the multicast or broadcast service
GKEK-Parameters	"Older" generation of GKEK-related parameters for multicast or broadcast service.
GKEK-Parameters	"Newer" generation of GKEK-related parameters for multicast or broadcast service.
Nonce	A same random number included in the PKMv2 Key Request message
HMAC-Digest/CMAC Digest	Message Digest calculated using AK

The TEK-Parameters and the SAID attributes are as defined in 6.3.2.3.9.5.

The GKEK-Parameters attribute is a compound attribute containing all of the GKEK-related parameters corresponding to a GSAID. This would include the GKEK, the GKEK's remaining key lifetime, and the GKEK's key sequence number. The older generation of GKEK-Parameters is valid within the current lifetime and the newer generation of GKEK-Parameters is valid within the next lifetime.

The HMAC-Digest or the CMAC-Digest attribute shall be the final attribute in the message's attribute list.

Inclusion of the HMAC-Digest or the CMAC digest allows the MS and BS to authenticate the PKMv2 Key-Reply message. The HMAC-Digest or the CMAC-Digest's authentication key is derived from the AK.

[Change the Table 370 in sub-clause 11.9:]

11.9 PKM-REQ/RSP management message encodings

Table 370-PKM attribute types

Type	**PKM attribute**

	… **The above attributes of this table remains the same.**
45	AKID
46	Associated GKEK Sequence Number
47	GKEK-Parameters
~~46~~48-255	reserved

[Change the Table 370 in the section 11.9.8 as follows]

11.9.8 TEK parameters

Description: This attribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all security parameters relevant to a particular generation of an SAID's TEK. A summary of the TEK-Parameters attribute format is shown below. The GTEK and GKEK are defined only for the multicast service or the broadcast service. The GTEK is the TEK for the multicast service or the broadcast service.

Type	Length	Value(compound)
13	variable	The Compound field contains the subattributes as defined in Table ~~370~~ 372

Table 372 - TEK-parameters subattributes

Attributes	Contents

TEK	TEK, encrypted with the KEK GTEK, encrypted with the GKEK
~~GKEK~~	~~Group Key Encryption Key, encrypted with GKEKEK derived from AK~~
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	CBC Initialization Vector
Associated GKEK Sequence Number	Associated GKEK sequence number with this TEK-Parameters

[Change the section 11.9.30 as follows]

11.9.30 Key Push Modes

Description: The field, key push modes, is used to distinguish usage code of ~~the~~ a PKMv2 Group Key Update Command message.

Type	Length	Value
41	1	0, GKEK update mode 1, GTEK update mode 2-255, reserved

~~The~~ A PKMv2 Group Key Update Command message for the GKEK update mode is to distribute new GKEK to each SS carried on the Primary Management connection. The BS transmits this message before the M&B TEK Grace Time starts.

~~The~~ A PKMv2 Group Key Update Command message for the GTEK update mode is to distribute new GTEK to all SS carried on the Broadcast connection. The BS transmits this message after the M&B TEK Grace Time starts.

Attributes of a PKMv2 Group Key Update Command message are different according to the value of the Key Push Modes as shown in the following Table.

Attribute	GKEK update mode	GTEK update mode
Key-Sequence-Number	Yes	~~No~~ Yes
GSAID	Yes	Yes
Key Push Modes	Yes	Yes
Key Push Counter	Yes	Yes
GTEK-Parameters	No	Yes
~~> GKEK~~	~~o~~	~~x~~
~~> GTEK~~	~~x~~	~~o~~
~~> Key-Lifetime~~	~~x~~	~~o~~
~~> Key-Sequence-Number~~	~~o~~	~~o~~
~~> CBC-IV~~	~~x~~	~~o~~
GKEK-Parameters	Yes	No
HMAC/CMAC-Digest	Yes	Yes

AK's Key-Sequence-Number, GSAID, Key Push Modes, and HMAC/CMAC-Digest fields are included in two PKMv2 Group Key Update Command messages regardless of the value of the Key Push Modes. ~~Some subattributes of TEK-Parameters, GKEK and GTEK's Key-Sequence-Number, should be contained in the Key Update Command message for the GKEK update mode. And, GTEK, GTEK's Key-Lifetime, GTEK's Key-Sequence-Number, and CBC-IV should be contained in the Key Update Command message for the GTEK update mode.~~

GKEK-Parameters attribute should be included in a PKMv2 Group Key Update Command message for the GKEK update mode. And GTEK-Parameters attribute should be included in that message for the GTEK update mode.

[Insert new sections in the section 11.9:]

11.9.35 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

[Insert new sections in the section 11.9:]

11.9.36 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)

ttribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all the security parameters relev