Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Corrections for Adaptation of the PKMv1 Messages to PKMv2**	
Data Submitted	**2005-05-05**	
Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon, ETRI Jicheol Lee and Yong Chang SAMSUNG Yongjoo Tcha KT Li Rui and Tian Feng ZTE corporation Yigal Eliaspur Intel Corp.	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea
Re:	IEEE P802.16e/D7	
Abstract	The existing PKMv2 is somewhat unorganized and insecure security framework. This contribution provides a resolution for adaptation the PKMv1 messages to the PKMv2.	
Purpose	Adoption of proposed changes into P802.16e/D7	
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>.	

Corrections for Adaptation of the PKMv1 Messages to PKMv2

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon
ETRI

Jicheol Lee and Yong Chang
SAMSUNG

Yongjoo Tcha
KT

Li Rui and Tian Feng
ZTE corporation

Yigal Eliaspur
Intel Corp.

Introduction

The existing PKMv2 is somewhat in disorder and provides unorganized and insecure security framework.
This contribution supports the backward compatibility with the PKMv1 and security framework of the PKMv2.

This contribution provides a resolution for those problems in the PKMv2.

0.1 IEEE P802.16e/D7 Status
Some messages defined in the PKMv1 are still used in the PKMv2.

0.2 Problems

- Some messages included in the PKMv1 are needed for full operation of the PKMv2. Those messages need to be changed to satisfy the aim of PKMv2 and backward compatibility with PKMv1.

0.3 Solutions

a) For TEK exchange procedure:
   - The messages used in the PKMv1 should be added some attributes to protect replay-attack.
     i. PKMv2 Key-Request message: Key Sequence Number (AK), SAID, Nonce, OMAC Digest (from AK)
     ii. PKMv2 Key-Reply message: Key Sequence Number (AK), SAID, TEK-Parameters (for old), TEK-Parameters (for new), Nonce, OMAC Digest (from AK)
     iii. PKMv2 Key-Reject message: Key Sequence Number (AK), SAID, Error-Code, Display-String, Nonce, OMAC Digest (from AK)

b) For Dynamic SA addition procedure:
   - The messages used in the PKMv1 should be added some attributes to protect replay-attack.
     i. PKMv2 SA-Addition message: Key Sequence Number (AK), (one or more) SA-Descriptor(s), Nonce, OMAC Digest (from AK)

c) For TEK Invalid procedure:
   - The messages used in the PKMv1 should be added some attributes to protect replay-attack.
     i. PKMv2 TEK Invalid message: Key Sequence Number (AK), SAID, Error-Code, Display-String, Nonce, OMAC Digest (from AK)

Proposed Changes into IEEE P802.16e/D7

[Delete sub-clauses 6.3.2.3.9.5 and 6.3.2.3.9.6]

~~**6.3.2.3.9.5 Key Request message**~~

~~**Table 31-Key Request attributes**~~

~~Attribute~~	~~Contents~~
~~Key Sequence Number~~	~~AK sequence number~~
~~AKID~~	~~This identifies the AK to the BS that was used for protecting this message.~~
~~NonceSS~~	~~A number chosen by the SS (once per protocol run). It can be counter or a random number.~~
~~SAID~~	~~Security association identifier.~~
~~HMAC-Digest~~	~~Keyed SHA message digest.~~

~~**6.3.2.3.9.6 Key Reply message**~~

~~**Table 31-Key Reply attributes**~~

~~Attribute~~	~~Contents~~
~~Key Sequence Number~~	~~AK sequence number~~
~~AKID~~	~~This identifies the AK to the BS that was used for protecting this message.~~
~~NonceSS~~	~~A number chosen by the SS (once per protocol run). It can be counter or a random number. This is returned by BS to MS.~~
~~SAID~~	~~Security association identifier.~~
~~TEK-Parameters~~	~~"Older" generation of key parameters relevant to SAID.~~
~~TEK-Parameters~~	~~"Newer" generation of key parameters relevant to SAID.~~
~~HMAC-Digest~~	~~Keyed SHA message digest.~~

6.3.2.3.9.20 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.

Code: 22

Attributes are shown in Table 37j.

Table 37l-PKMv2 Key Request attributes

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier
Nonce	A random number generated in a MS
HMAC Digest/OMAC Digest	Message Digest calculated using AK

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

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

6.3.2.3.9.21 PKMv2 Key-Reply message

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

Code: 23

Attributes are shown in Table 37k.

Table 37k-PKMv2 Key-Reply attributes

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier
TEK-Parameters	"Older" generation of key parameters relevant to SAID
TEK-Parameters	"Newer" generation of key parameters relevant to SAID
Nonce	A same random number included in the PKMv2 Key Request message
HMAC-Digest/OMAC Digest	Message Digest calculated using AK

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

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

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

6.3.2.3.9.22 PKMv2 Key-Reject message

The BS responds to a MS's PKMv2 Key-Request message with a PKMv2 Authorization-Reject message if the BS rejects the MS's traffic keying material request.

Code: 24

Attributes are shown in Table 37l.

Table 37l-PKMv2 Key-Reject attributes

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier
Error-Code	Error code identifying reason for rejection of the PKMv2 Key-Request message
Display-String (optional)	Display string containing reason for the PKMv2 Key-Request message
Nonce	A same random number included in the PKMv2 Key Request message
HMAC-Digest/OMAC Digest	Message Digest calculated using AK

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

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

6.3.2.3.9.23 PKMv2 SA-Addition message

This message is sent by the BS to the SS to establish one or more additional SAs.

Code: 25

Attributes are shown in Table 37m.

Table 37m-PKMv2 SA-Addition attributes

Attribute	Contents
Key Sequence Number	AK sequence number
(one or more) SA-Descriptor(s)	Each compound SA-Descriptor attribute specifies an SA identifier (SAID)

	and additional properties of the SA
Nonce	A random number generated in a BS
HMAC-Digest/OMAC Digest	Message Digest calculated using AK

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

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

6.3.2.3.9.24 PKMv2 TEK-Invalid message

The BS sends a PKMv2 TEK-Invalid message to a client MS if the BS determines that the MS encrypted an uplink PDU with an invalid TEK (i.e., an SAID's TEK key sequence number), contained within the received packet's MAC Header, is out of the BS's range of known, valid sequence numbers for that SAID.

Code: 26

Attributes are shown in Table 37n.

Table 37n-PKMv2 TEK-Invalid attributes

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security Association Identifier
Error-Code	Error code identifying reason for PKMv2 TEK-Invalid message
Display-String (optional)	Display string containing reason for the PKMv2 TEK-Invalid message
Nonce	A random number generated in a BS
HMAC-Digest/OMAC Digest	Message Digest calculated using AK

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

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

[Change sub-clauses 6.3.2.3.9.17 as follows]

~~**6.3.2.3.9.17 Group Key Update Command message**~~

6.3.2.3.9.25 PKMv2 Group-Key-Update-Command message

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 37o.

Table ~~37g~~ 37o ~~– Key update command attributes~~ PKMv2 Group Key Update Command attributes

Attribute	Contents
Key-Sequence-Number	AK 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 parameters relevant to GSAID
GKEK-Parameters	Group Key Encryption Key protected by KEK derived from shared AK and other GKEK parameter e.g. Key lifetime.
OMAC/HMAC-Digest	Message integrity code of this message

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 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 usage code of the Group Key Update Command message. The 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 Group 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 Group Key Update Command message contains only newer generation of key parameters, because this message inform an MSS 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, 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 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. GKEK parameters contain the GKEK encrypted by the KEK and GKEK lifetime. See 7.5.4.4 for details.

The OMAC/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 Group Key Update Command message. The OMAC/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.