Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for Flow and Message Confusion between PKMv1 and 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 flow and message confusion between the PKMv1 and 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 Flow and Message Confusion between PKMv1 and 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
There are many sub-messages in the PKM-REQ/RSP messages. Some of them are for the PKMv1, the other are for the PKMv2.

0.2 Problems
- Messages for the PKMv2 were obviously proposed for assuring more secure message transfer, safe key share, and so on. But, it is difficult to distinguish which messages are for the PKMv1 or PKMv2, e.g. Key-Request message, Key-Reply message, EAP-Transfer message.
- 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
We propose PKM-related flow and messages as follows.

a) The messages included in the PKMv1 are remained for backward compatibility with the PKMv1. In other words, the name and the attributes of messages are maintained.
   - SA Add, Auth Request, Auth Reply, Auth Reject, Key Request, Key Reply, Key Reject, Auth Invalid, TEK Invalid, and Auth Info messages

b) The messages included in the PKMv2 are changed under the PKMv2 procedure features. In other words, the names of messages are changed by procedure features. Their attributes are changed in case that some problems in the attribute occur. Moreover, code values for PKMv2 message type are re-numbered.
   - For the RSA-based Authorization procedure: The name of messages for the RSA-based Authorization procedure and a few attributes included in those messages are changed as follows:
     i. PKMv2 Auth-Request message → PKMv2 RSA-Request message (Name and attributes are changed: code # 13)
     ii. PKMv2 Auth-Reply message → PKMv2 RSA-Reply message (Name and attributes are changed: code # 14)
     iii. PKMv2 RSA-Reject message (New message is added: code # 15)
     iv. PKMv2 RSA-Acknowledgement message (New message is added: code # 16)
   - For the EAP-based Authorization procedure: The name of messages for the EAP-based Authorization procedure and a few attributes included in those messages are changed as follows:
     i. EAP Transfer message → PKMv2 EAP-Transfer message (Name is changed: code # 17)
     ii. Authenticated EAP message → PKMv2 Authenticated-EAP-Transfer message (Name and attributes are changed: code # 18)
     iii. PKMv2 EAP-Transfer-Complete message (New message is added: code # 19)
   - For the TEK exchange procedure: This procedure is for distributing TEK (or GTEK) in protecting replay-attack. The protecting function from replay-attack is added into the messages used for PKMv1 TEK exchange procedure. New messages for TEK exchange procedure are as follows:

i. PKMv2 Key-Request message (New message is added: code # 24)
ii. PKMv2 Key-Reply message (New message is added: code # 25)
iii. PKMv2 Key-Reject message (New message is added: code # 26)

- For the Dynamic SA addition procedure: This procedure is for adding new dynamic SA in protecting replay-attack The protecting function from replay-attack is added into the messages used for PKMv1 Dynamic SA addition procedure. New messages for Dynamic SA addition procedure are as follows:
  i. PKMv2 SA-Addition message (New message is added: code # 27)
- For the TEK Invalid procedure: This procedure is for informing MS of using the invalid TEK in protecting replay-attack. The protecting function from replay-attack is added into the messages used for PKMv1 TEK Invalid procedure. New messages for TEK Invalid procedure are as follows:
  i. PKMv2 TEK-Invalid message (New message is added: code # 28)
- For Group Key Update procedure: This procedure is for pushing Group keying material to MSs. The name of messages for Group Key Update procedure are changed as follows:
  i. Group Key Update Command message → PKMv2 Group-Key-Update-Command message (Name and attributes are changed: code # 29)

Proposed Changes into IEEE P802.16e/D7

[Change the Table 26 in sub-clause 6.3.2.3.9:]

6.3.2.3.9 Privacy key management (PKM) message (PKM-REQ/PKM-RSP)

Code	PKM message type	MAC Management message name
~~13~~	~~EAP Transfer~~	~~PKM-REQ/PKM-RSP~~
~~14~~	~~Pre-Auth Request~~	~~PKM-REQ~~
~~15~~	~~Pre-Auth Reply~~	~~PKM-RSP~~
~~16~~	~~Pre-Auth Reject~~	~~PKM-RSP~~
~~17~~	~~PKMv2 Auth Request~~	~~PKM-REQ~~
~~18~~	~~PKMv2 Auth Reply~~	~~PKM-RSP~~
~~19~~	~~Key Update Command~~	~~PKM-RSP~~
~~20~~	~~Authenticated EAP~~	~~PKM-REQ/PKM-RSP~~
~~21~~	~~SA-TEK-Challenge~~	~~PKM-RSP~~
~~22~~	~~SA-TEK-Request~~	~~PKM-REQ~~
~~23~~	~~SA-TEK-Response~~	~~PKM-RSP~~
~~24-255~~	~~reserved~~	
13	PKMv2 RSA-Request	PKM-REQ
14	PKMv2 RSA-Reply	PKM-RSP
15	PKMv2 RSA-Reject	PKM-RSP
16	PKMv2 RSA-Acknowledgement	PKM-REQ
17	PKMv2 EAP-Transfer	PKM-REQ/PKM-RSP
18	PKMv2 Authenticated EAP-Transfer	PKM-REQ/PKM-RSP
19	PKMv2 SA TEK Challenge	PKM-RSP
20	PKMv2 SA TEK Request	PKM-REQ
21	PKMv2 SA TEK Response	PKM-RSP
22	PKMv2 Key-Request	PKM-REQ
23	PKMv2 Key-Reply	PKM-RSP
24	PKMv2 Key-Reject	PKM-RSP
25	PKMv2 SA-Addition	PKM-RSP
26	PKMv2 TEK-Invalid	PKM-RSP
27	PKMv2 Group-Key-Update-Command	PKM-RSP
28-255	reserved	