Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**TEK Transfer in Relay Systems**
Date Submitted	**2007-03-05**
Source(s)	Masato Okuda Fujitsu Laboratories LTD. Kamikodanaka 4-1-1, Nakahara-ku Kawasaki, Japan. 211-8588 Voice: +81-44-754-2811 Fax: +81-44-754-2786 okuda@jp.fujitsu.com Yuefeng Zhou, Mike Hart Fujitsu Laboratories of Europe Ltd. Hayes Park Central Hayes Middlesex., UB4 8FE, UK Voice: +44 (0) 20 8573 4444 FAX: +44 (0) 20 8606 4539 Yuefeng.zhou@uk.fujitsu.com Mike.hart@uk.fujitsu.com
Re:	IEEE802.16j-07/007r2: “Call for Technical Comments and Contributions regarding IEEE Project 802.16j”
Abstract	This contribution proposes a MS TEK Transfer mechanism.
Purpose	To propose text to describe a MS TEK Transfer mechanism
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:chair@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>.

TEK Transfer in Relay Systems

Masato Okuda, Yuefeng Zhou and Mike Hart
Fujitsu.

Introduction

This contribution describes necessity of decrypting MAC-PDUs at RS and proposes to transfer TEK to RS.

In the current 16e systems, Security Association would be established between (MR-)BS and MS. So, MR-BS and MS shares security keys, such as AK and TEK. In the same manner, it would be expected to establish SA and share security keys between MR-BS and RS in relay systems. However lack of MS's TEK knowledge at RS might cause several problems, especially in distributed scheduling model.

According to the current standards, subheaders are encrypted as a part of payload of MAC-PDU (see 6.3.2 and 6.3.3.6 in [1]). Therefore, when a relay station derives information from a subheader, it needs to decrypt the MAC-PDU.

An example of deriving information from subheader is "piggybacked bandwidth request". In distributed scheduling relay system, RS allocates bandwidth on its access link. So, the RS needs to know all BW request information. Therefore, RS needs to decrypt MAC-PDU (if encrypted) and get bandwidth request information from the Grant Management subheader.

In order to enable RS to decrypt MAC-PDUs, it is necessary for RS to be authenticated and allowed to have the TEKs shared by MR-BS and MS. Therefore, when MR-BS sends PKMv2 Key_Reply message to MS in response to PKMv2 Key_Request message, it sends another PKMv2 Key_Reply message to the RS. Integrity of this message shall be protected with HMAC/CMAC calculated with a key derived from the RS AK, to RS. The latter PKMv2 Key_Reply message contains MS's basic CID in addition to the same TEK parameters in the PKMv2 Key_Reply sent to the MS, and those parameters are encrypted with the KEK shared between MR-BS and RS.

Figure-1 shows concept of TEK Transfer. As shown in the figure, RS and MS have established security association with the MR-BS after authentication.

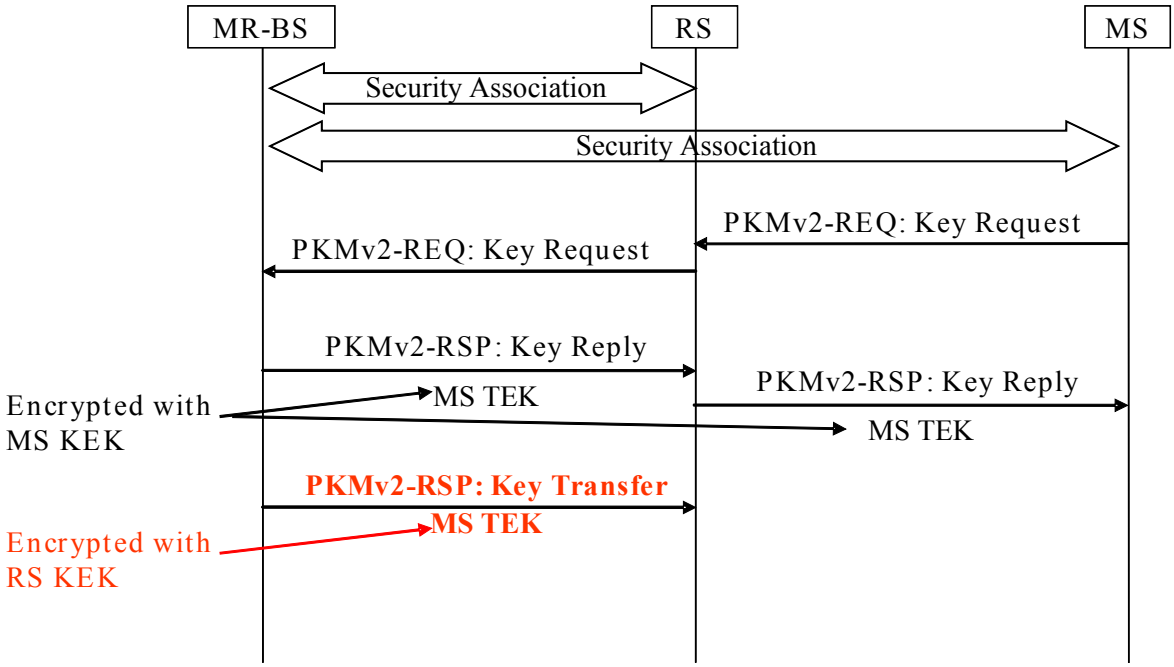

Figure-1 Concept of TEK Transfer

Specific Text Changes

Add the following row in the Table 26

Table 26 – PKM message codes

Code	PKM message Type	MAC Management message name
31	PKMv2 Key Transfer	PKM-RSP
32	PKMv2 Key Transfer Ack	PKM-RSP
33-255	*Reserved*	-

Intesert the following subclause 6.3.2.3.9.28

6.3.2.3.9.28 PKMv2 Key Transfer message

This message is sent by the MR-BS to notify RS of the MS' key information.

Table xx – PKMv2 Key Transfer attributes

Attribute	Contents
Key Sequence Number	RS AK sequence number
MS CID	MS's basic CID
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
CMAC Digest	Message Digest calculated using RS' AK.

6.3.2.3.9.29 PKMv2 Key Transfer Acknowledgement message

Table xx – PKMv2 Key Transfer attributes

Attribute	Contents
Key Sequence Number	RS AK sequence number
MS CID	MS's basic CID
SAID	Security association identifier
CMAC Digest	Message Digest calculated using RS' AK.

References

[1] IEEE802.16-2004

[2] IEEE802.16e-2005