Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**A Key Management Method for the Multicast Service**	
Data Submitted	**2004-03-05**	
Source(s)	Seokheon Cho Ae Soon Park Chulsik Yoon SungCheol Chang Kyung Su Kim ETRI 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr aspark@etri.re.kr
Re:	This is a response to a Ballot #14 Announcement IEEE 802.16-04/06 on IEEE P802.16e-D1.	
Abstract	The document contains suggestions on the changes in IEEE P802.16e-D1 that would support to negotiate authorization policy between the existing device authentication and the user authentication.	
Purpose	The document is submitted for review by 802.16 Working Group members	
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>.	

A Key Management Method for the Multicast Service

Seokheon Cho, Ae Soon Park, Chulsik Yoon, SungCheol Chang, and Kyung Su Kim
ETRI

Introduction

In order for a downlink multicast service to be safely provided, the key management for the multicast service is needed. The IEEE 802.16 considers the TEK management for the multicast service and for the unicast service as one and the same thing.

An SS periodically asks the BS to refresh of key material for respective SA-ID by sending the Key Request message. BS responds to this message with the Key Reply message, containing the BS's active keying material for a specific SA-ID. The Key Request and Key Reply messages are carried on the specific primary management connection between an SS and the BS. The TEK management for the multicast service as well as for the unicast service follows this keying distribution procedure.

If the key management for the multicast service follows the above procedure, however, the key management meets some problems. First, the BS should instantaneously have excessive processing capacity. The BS shall receive simultaneously so many Key Request messages at the TEK Grace Time. In addition, the BS has to refresh and distribute new TEK to individual SSs through the primary management connection for a moment. Second, signalling resources are unnecessarily used to refresh TEK which is the same between the BS and multiple SSs being provided with a multicast service.

Therefore, we propose an alternative key method to solve those mentioned problems. The BS shall periodically begin to refresh TEK for the multicast service at the Multicast TEK Grace Time. The BS shall send only one Key Reply message, containing updated TEK, to all SSs being provided with the relevant service through the broadcast connection. The BS doesn't need to have excessive processing capacity and only a few resources are needed to distribute the new TEK in the proposed key method.
In sending the Key Reply message, the newly updated TEK should be encrypted, because a downlink multicast service is safely provided SSs. The TEK shall be encrypted using two-key triple DES in the encrypt-decrypt-encrypt mode. Two input keys in the 3-DES are old distributed TEKs.

Proposed changes to IEEE 802.16-REVd/D3-2004

6.2.2.3 MAC Management Messages
[Change to Table 14]

Table 14 - MAC Management Messages

Type	Message name	Message description	Connection
10	PKM-RSP	Privacy Key Management Response	Primary Management, Basic

NOTE: The Key Reply PKM message of the PKM-RSP message can be carried on the Basic connection.

7.1.4 Mapping of connections to SAs
[Change the second particulars]

2) Multicast Transport Connections may be mapped to Static or Dynamic SA. However, each of Multicast Transport Connections should be mapped to only one SA.

7.2.5 TEK state machine
[Change the Figure 127]

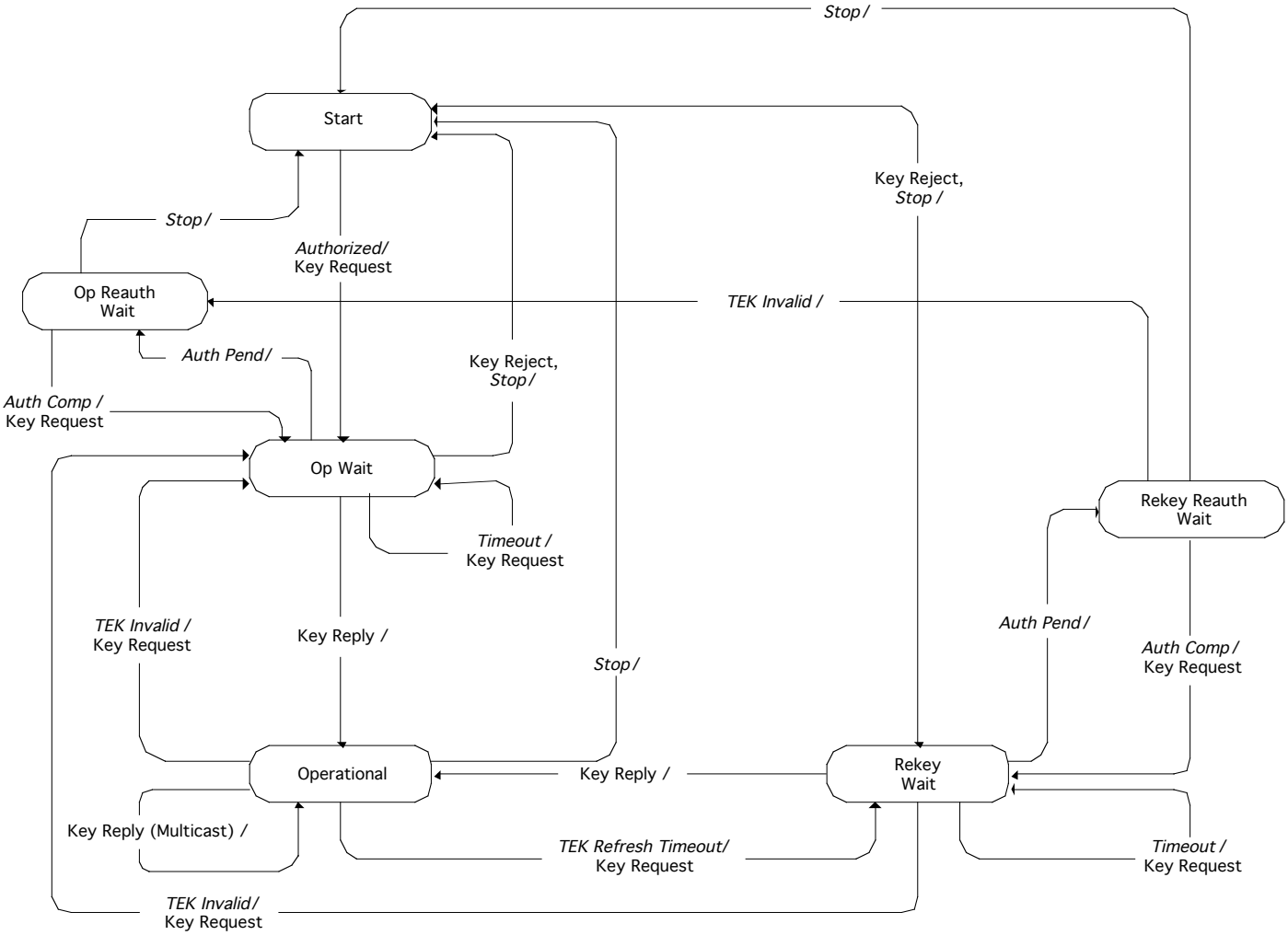

Figure 127 - TEK state machine flow diagram

[Change the Table 111]

Table 111 - TEK FSM state transition matrix

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait			Rekey Wait	
(7) TEK Refresh Timeout				Rekey Wait		
(8) Key Reply		Operational		Operational	Operational	
(9) Key Reject		Start			Start	

NOTE: The state, Operational (D), can be transited to the "Operational" state by receiving the Key Reply message for the multicast transport service such as "8-D".

7.2.5.3 Events
[Insert at the end of this section]

Multicast TEK Refresh Timeout: This event is defined only for the multicast service in BS. The TEK refresh timer for the multicast service timed out. This timer event signals the MAC in BS to refresh new keying material. The refresh timer is set to fire a configurable duration of time (*Multicast TEK Grace Time*) before the expiration of the newer TEK the BS currently holds.

7.2.5.4 Parameters
[Insert at the end of this section]

Multicast TEK Grace Time: This parameter is defined only for the multicast service in BS. Time interval, in seconds, before the estimated expiration of a TEK that the BS starts rekeying for a new TEK. This parameter is vendor-specific and is the same across all SAIDs related to the multicast service.

7.2.5.5 Actions
[Insert between "8-B" and "8-E"]

8-D Operational (Key Reply: Multicast) → Operational
a) process contents of Key Reply message and incorporate new keying material into key database
b) set the TEK refresh timer to go off "TEK Grace Time" seconds prior to the key's scheduled expiration

7.5.2 Encryption of TEK with 3-DES
[Insert after the second paragraph]

The Key Reply message is generally carried on the primary management connection. When the BS periodically begins to refresh

keying and distributes this TEK only for the multicast service, the Key Reply message is carried on the basic connection. The method of encrypting the TEK is differently used by connection carrying the Key Reply message.

Encryption: C = Ek1[Dk2[Ek1[P]]]
Decryption: P = Dk1[Ek2[Dk1[C]]]
P = Plaintext 64-bit TEK
C = Ciphertext 64-bit TEK
k1 = left-most 64 bits of the 128-bit KEK (primary management connection)
= an old distributed TEK (basic connection)
k2 = right-most 64 bits of the 128-bit KEK (primary management connection)
= an old distributed TEK (basic connection)
E[] = 56-big DES ECB(electronic code block) mode encryption
P[] = 56-bit DES ECB decryption

10.2 PKM parameter values
[Change to Table 270]

Table 270 – Operational ranges for privacy configuration settings

System	Name	Description	Minimum value	Default value	Maximum value
BS	Multicast TEK Grace Time	Time prior to TEK (for the multicast service) expiration BS begins rekeying. This time is bigger than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value