Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**A Key Management Method for the Multicast Service**
Data Submitted	**2004-03-09**
Source(s)	Seokheon Cho Ae Soon Park Chulsik Yoon SungCheol Chang Kyung Soo 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 Handoff/Sleep-mode Ad Hoc Group and/or 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 Soo Kim

ETRI

Introduction

1. Current Structure of the TEK Management for the multicast service

In order to provide a downlink multicast service safely, the key management for the multicast service is needed. The IEEE 802.16 considers that the multicast service and the unicast service is similarly managed by the TEK management

Current structure of the TEK management for the multicast service is shown as the <Figure 1>.

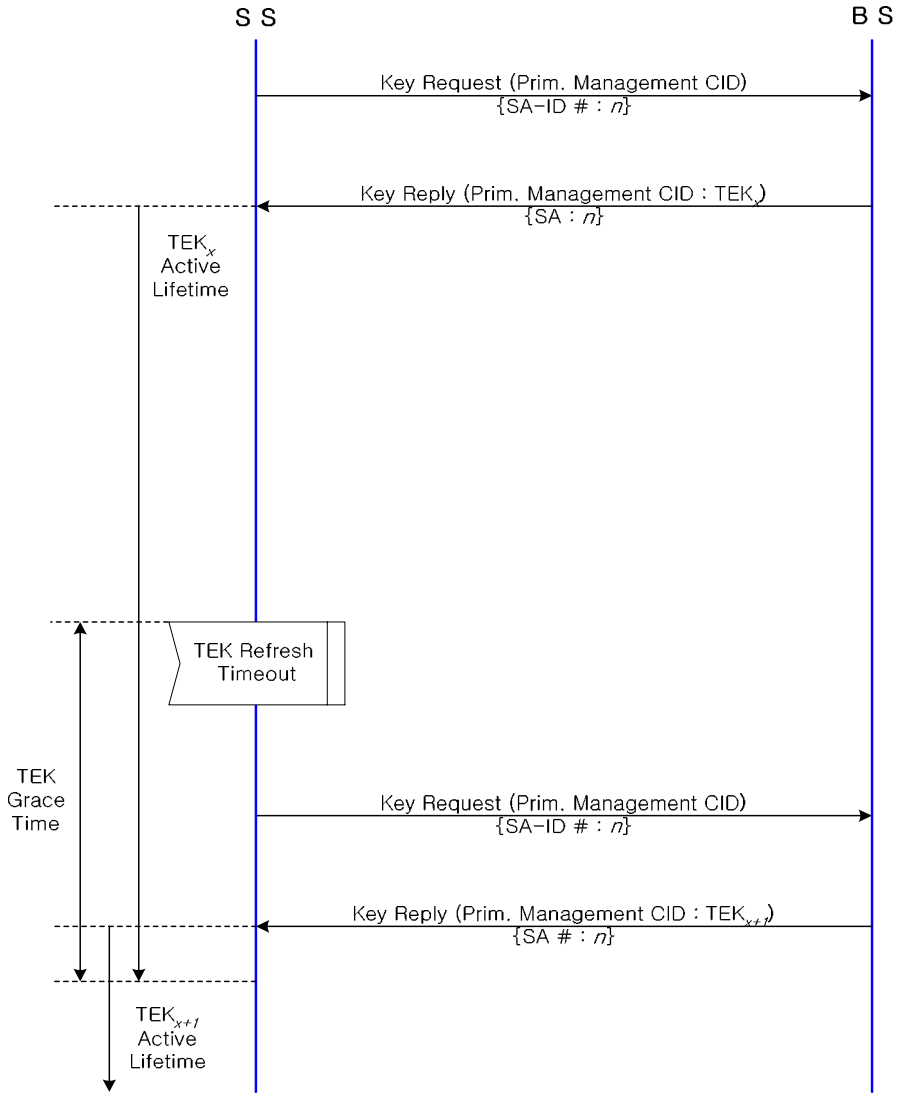

Figure 1 Current TEK distribution procedure

An SS tries to get the TEK before an SS is served with the specific multicast service. The SS sends the Key Request message to the BS through the primary management connection, requesting the new TEK for the specific multicast service. This Key Request message should contain the SA-ID (if being equal to *n*) related to the specific multicast service. Assuming that the SS get the TEK_x in the n^{th} SA (The TEK_x means the x^{th} assigned TEK for the n^{th} SA from the BS), the BS sends the Key Reply message, (including the n^{th} SA) response to this message. The Key Reply message is also carried on the primary management connection. By this procedure, the SS can get the updated TEK from the BS.

An SS periodically informs the BS to refresh key material for the n^{th} SA-ID at the TEK Grace Time 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 also carried the specific primary management connection message between an SS and the BS. The TEK management for the multicast service and the unicast service follows this keying distribution procedure.

If the keying management for the multicast service follows this procedure, then there are some inefficient problems. Therefore, several problems are presented, meanwhile, two suggestions are proposed for the SA mapping and the TEK management of the multicast service.

2. Relationship between the multicast service and the SA

1). Mapping a multicast connection to different SAs

"Multicast Transport Connections may be mapped to any Static or Dynamic SA", mentioned in the IEEE 802.16 WirelessMAN Standard. This means that a multicast transport connection can be mapped to more than one static or dynamic SA. A multicast service may be mapped to different SAs or only one SA.

When a multicast service is mapped to different SAs, the key distribution flow is shown as the <figure 2>.

Assuming that several users (SS_1 ~ SS_z) are simultaneously served with a specific multicast service, "A." However, different SAs are assigned to individual SSs. In this case, the BS should encrypt the multicast traffic data with different SA, especially different TEK. Therefore, the BS is heavily burdened.

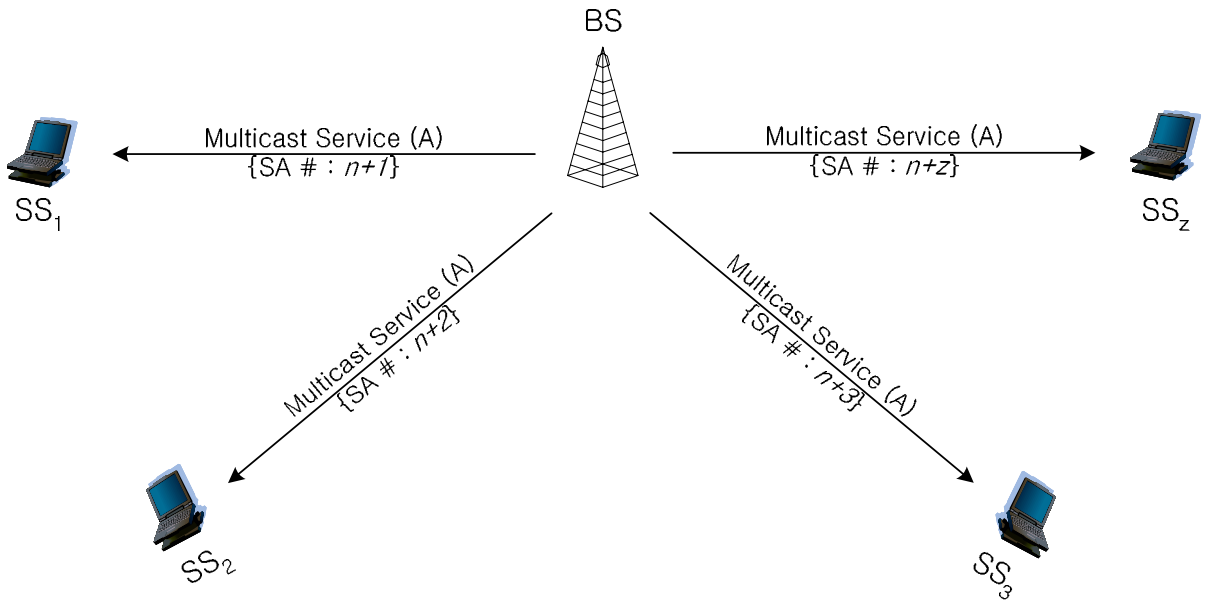

Figure 2 Multicast service example (A multicast service: different SAs)

2). Mapping a multicast connection to the same SA (Proposed solution)

We propose that a specific multicast service should be mapped to only one SA shown as <figure 3>.

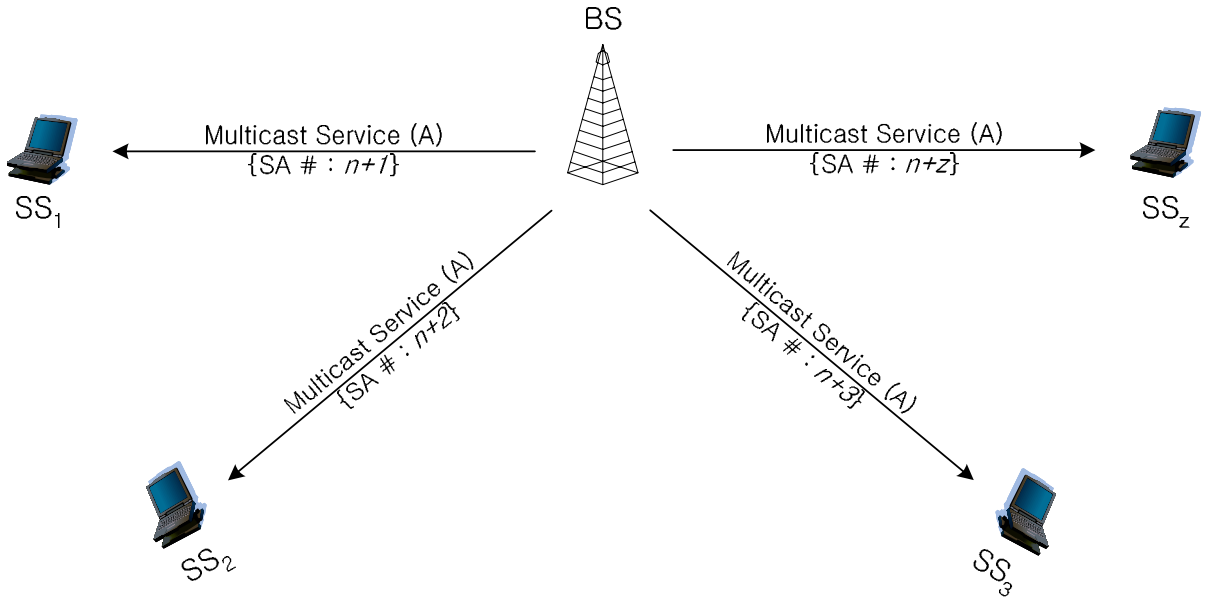

Figure 3 Multicast service example (A multicast service: equal SA)

The BS can mitigate the processing of encrypting multicast traffic data by using the equal SA. In this mapping, since the same SA

is shared with multiple SSs and the BS, the TEK itself should be also encrypted.

3. The Key Refreshment and Distribution for the Multicast Service

1). Carried on the primary management connection (general method)

The TEK distribution method is specified shown as <figure 1> in the IEEE 802.16. The Key Request and Key Reply messages used for the TEK distribution are carried on the primary management connection. The TEK updating and distribution procedure is shown as the <figure 4>.

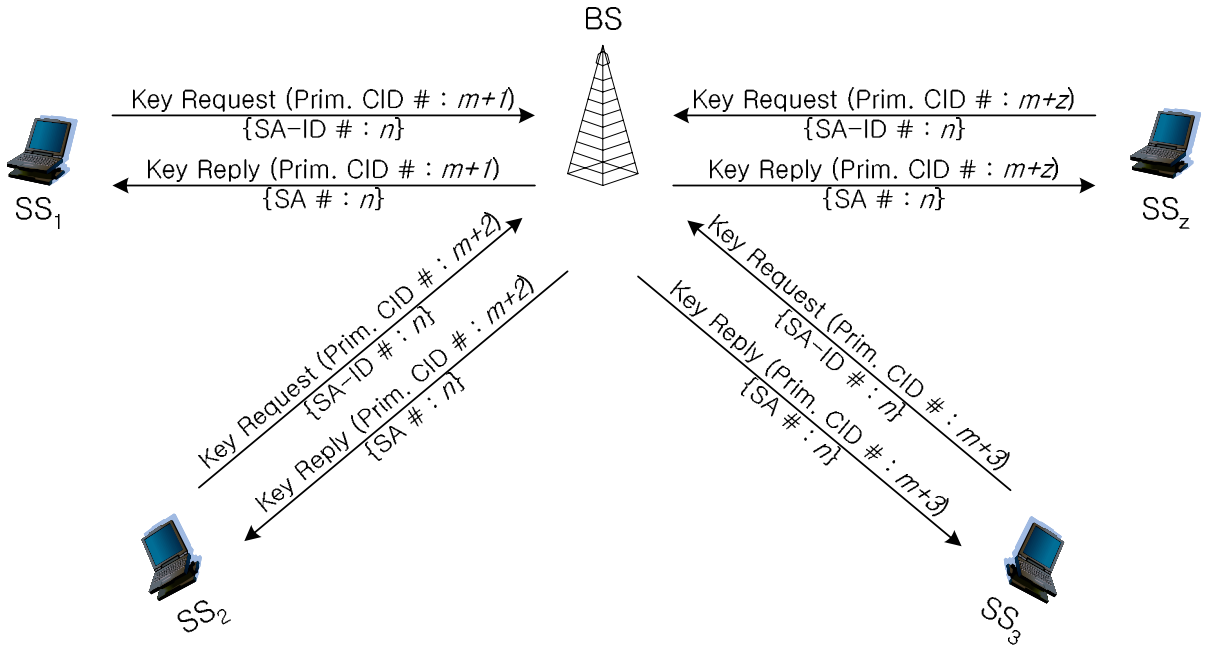

Figure 4 TEK updating and distribution procedure (primary management connection)

All SSs (SS_1 ~ SS_z) and the BS share the same n^{th} SA, because the BS provides a specific multicast service.

If the key management for the multicast service follows the above procedure, however, the key management encounters some problems. First, the BS should instantaneously waste excessive processing capacity. Because 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, unnecessary signalling resources are used to refresh TEK which shall be the same between the BS and multiple SSs (SS_1 ~ SS_z). In order to share new TEK with *z* SSs, the individual total size of the Key Request and the Key Reply messages on wireless channel are shown as the <table 1>,.

Table 1 Message total size (primary management connection)

Message	Size (bytes)	Total size (bytes)
Key Request	32 * z	106 * z
Key Reply	74 * z	

2). Carried on the broadcast connection (Proposed method)

Therefore, an alternative key method is proposed to solve those mentioned problems.

The proposed structure of the TEK management for the multicast service is shown as the <Figure 5>.

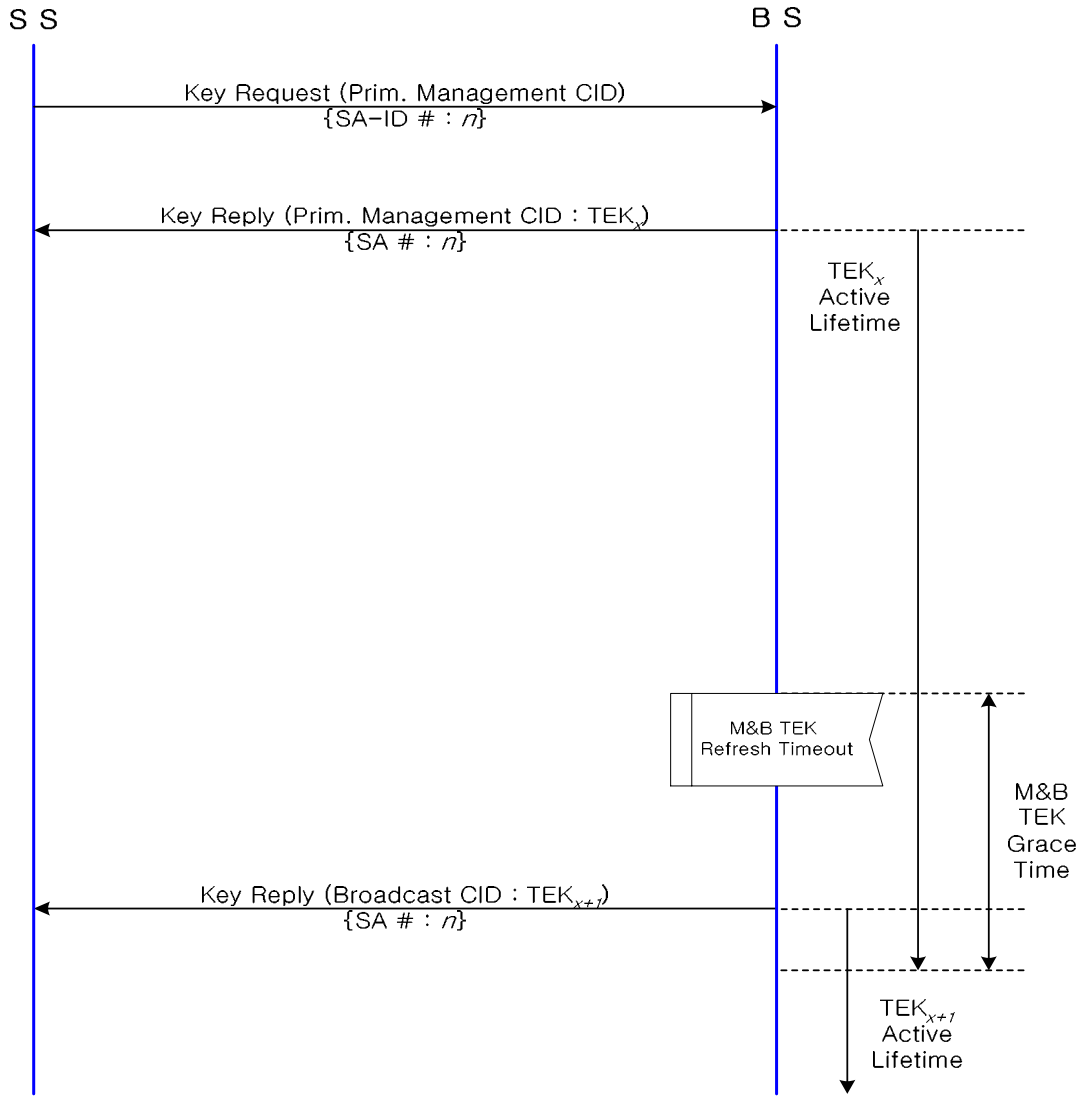

Figure 5 Proposed TEK distribution procedure

An SS tries to get the TEK before an SS is served with the specific multicast service. The first TEK distribution procedure is equal to that of the <figure 1>. Both the SS and the BS share the new TEK_x in the n^{th} SA by using the Key Request and Key Reply messages which are carried on the primary management connection.

The BS manages the Multicast TEK Grace Time for the respective SA-ID. This Multicast TEK Grace Time is defined only for the multicast service in the BS. This parameter means time interval, in seconds, before the estimated expiration of an old distributed TEK. Since the Multicast TEK Grace Time is longer than the TEK Grace Time in an SS, the BS starts rekeying for a new TEK.

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_{x+1} in the n^{th} SA, to all SSs being provided with the relevant multicast service through not the primary management connection but the broadcast connection.

The proposed TEK updating and distribution procedure between multiple SSs and the BS is shown as the <figure 6>.

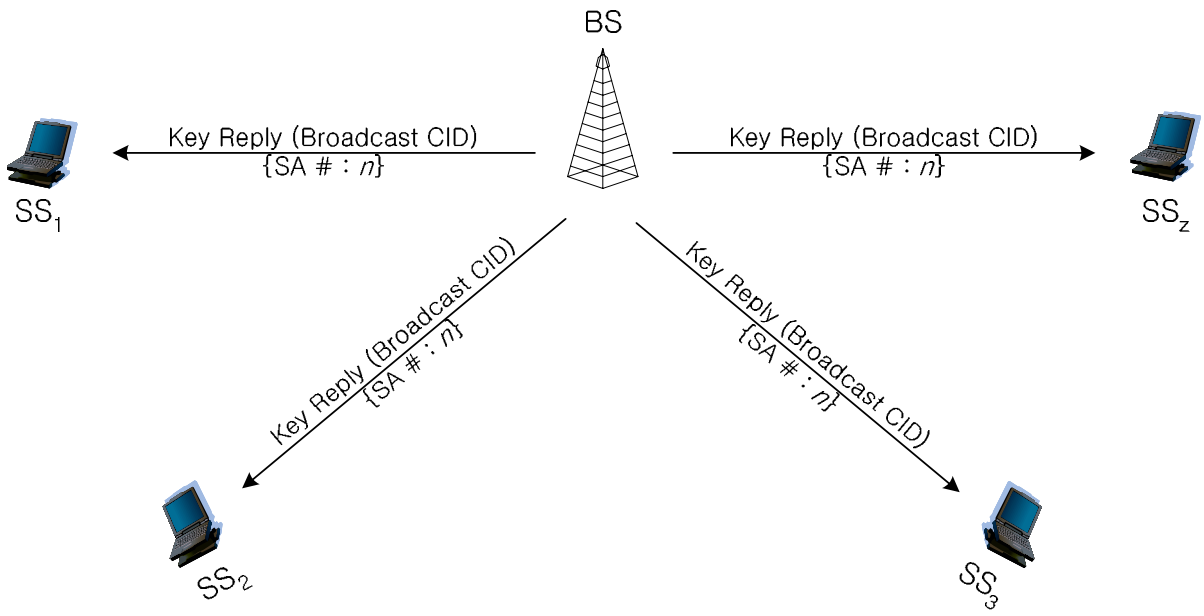

Figure 6 TEK updating and distribution procedure (broadcast connection)

The BS can distribute the new TEK to all served SSs with the specific multicast service by sending the Key Reply message though the broadcast connection. The Key Request messages from all SSs are not needed in this scheme. In addition, the new TEK can be sent by only one Key Reply message. Accordingly, 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 the sent Key Reply message, the newly updated TEK should be encrypted, because a downlink multicast service is safely provided by 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 the KEK, when the Key Reply message is carried on the primary management connection. Moreover, two input

keys are two old distributed TEKs, when the Key Reply message is carried on the broadcast connection. The common input keys should be used to encrypt the new TEK, because a new identical TEK is transmitted to all served SSs (SS_1 ~ SS_z) with the specific multicast service. In addition, these common input keys should be known to only served SSs with the specific multicast service, because the new encrypted TEKs are transmitted to the authorized SSs as well as the unauthorized SSs for that service. Owing to satisfaction of these requirements, old distributed TEKs for the multicast service is proper as the input keys of the 3-DES.

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]

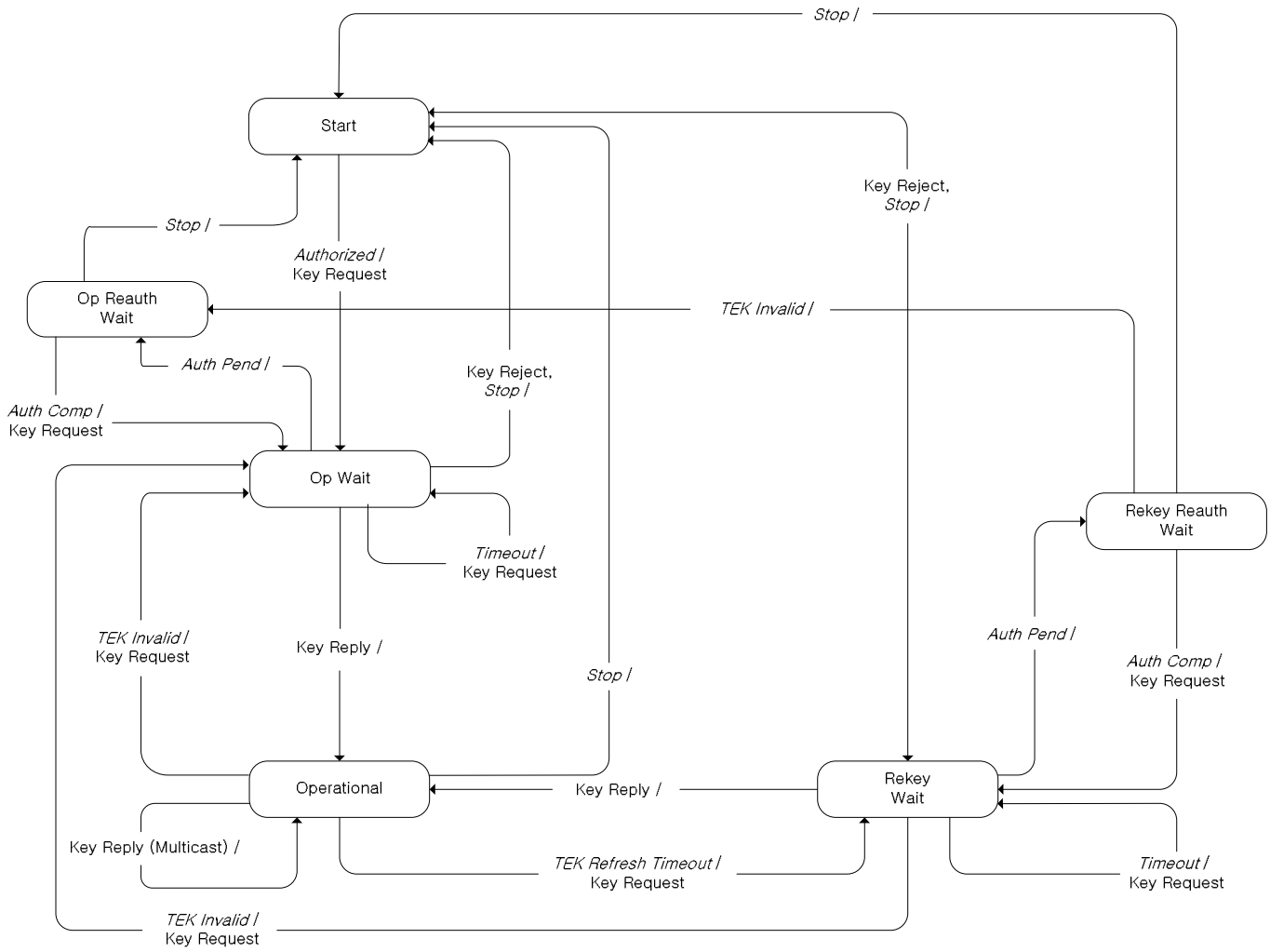

Figure 127 - TEK state machine flow diagram

[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