Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**PKM EAP further developed on section 7**
Date Submitted	**2004-08-29**
Source(s)	Dongkie Lee, DongIl Moon, DongRyul Lee, JongKuk Ahn, KangIl Koh, Sihun Ryu, Sungho Ha SK Telecom 15F, Seoul Finance Center, 84, Taepyungpro 1 ga, Chung-gu, Seoul, 100-768, Korea Voice: +82-2-6323-3147 Fax: +82-2-6323-4493 [mailto: {galahad,dimoon,drlee,jgahn,ss23}@sktelecom.com]
Re:	Recirculation Ballot #14c Announcement
Abstract	Although PKM EAP was accepted and baseline procedure is defined, further details like state machine and call flow are not described in REVe/D4. In this contribution, PKM EAP text was developed in through section 7.
Purpose	Discuss and Adopt as the baseline text
Notice	
Release	
Patent Policy and Procedures	

PKM EAP further developed on Section 7

Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn, KangIl Koh, Sihun Ryu
SK Telecom

1. Problem Statements

Although PKM EAP was accepted and baseline procedure is defined, further details like state machine and call flow are not described in REVe/D4. In this contribution, PKM EAP text was developed in through section 7.

Although *EAP Establish-Key Reply* is quite similar to *Auth Request* and *EAP Establish-Key Confirm* is quite similar to *Auth Reply*, EAP state machine has to be separated with PKM RSA state machine due to the different procedure. So considering 3-step process of EAP rather than 2-step of PKM, two states are added to the state machine. And also the messages which trigger states change are renamed.

2 Proposed Changes

[Change the 6.3.2.3.9.15 as the following:]

6.3.2.3.9.15 EAP Establish-Key Reject message

The SS transmits the EAP Establish-Key Request message as the second step in the 4-step sequence of establishing an AK after EAP-based authentication.

Code: 17

Attributes are shown in Table 37f.

Table 37e—EAP Establish-Key Reject attributes

Attribute	Contents
~~Reject Reason~~	~~1 - Unrecognized MKID~~
Error Code	Error code identifying reason for rejection of authorization request.

11.9.10 Error Code

Type	Length	Value(uint8)	
16	1	Error-Code	Authorization Reject, Authorization Invalid, Key Reject, TEK Invalid, EAP Establish-Key Reject

Table 371—Error-code attribute code values

Error Code	Messages	Description
0	All	No information
1	Auth Reject, Auth Invalid, EAP Establish-Key Reject	Unauthorized SS
2	Auth Reject, Key Reject, EAP Establish-Key Reject	Unauthorized SAID

	Key Reject	
3	Auth Invalid	Unsolicited
4	Auth Invalid, TEK Invalid	Invalid Key Sequence Number
5	Auth Invalid	Message (Key Request) authentication failure
6	Auth Reject, EAP Establish-Key Reject	Permanent Authorization Failure
7	EAP Establish-Key Reject	Unrecognized MKID

[Change the 7.2.3 of REVd/D5 and put in REVe/D4 as the following:]

7.2.3 Security capabilities selection

As part of their authorization exchange, the SS provides the BS with a list of all the cryptographic suites (pairing of data encryption and data authentication algorithms) the SS supports. The BS selects from this list a single cryptographic suite to employ with the requesting SS's primary SA. The Authorization Reply and the EAP Establish-Key Confirm the BS sends back to the SS includes a primary SA-Descriptor which, among other things, identifies the cryptographic suite the BS selected to use for the SS's primary SA. A BS shall reject the authorization request or the EAP Establish-Key Reply if it determines that none of the offered cryptographic suites are satisfactory.

The Authorization Reply and the EAP Establish-Key Confirm also contains an optional list of static SA-Descriptors; each static SA-Descriptor identifies the cryptographic suite employed within the SA. The selection of a static SA's cryptographic suite is typically made independent of the requesting SS's cryptographic capabilities. A BS may include in its Authorization Reply or the EAP Establish-Key Confirm static SA-Descriptors identifying cryptographic suites the requesting SS does not support; if this is the case, the SS shall not start TEK state machines for static SAs whose cryptographic suites the SS does not support.

[Add the 7.2.X at the appropriate section separate with the PKM RSA Authorization state machine:]

7.2.X Authorization state machine for PKM EAP

The Authorization state machine consists of eight states and nine distinct events (including receipt of messages) that can trigger state transitions. The Authorization finite state machine (FSM) is presented below in a graphical format, as a state flow model (Figure 131), and in a tabular format, as a state transition matrix (Table 131).

The state flow diagram depicts the protocol messages transmitted and internal events generated for each of the model's state transitions; however, the diagram does not indicate additional internal actions, such as the clearing or starting of timers, that accompany the specific state transitions. Accompanying the state transition matrix is a detailed description of the specific actions accompanying each state transition; the state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

The following legend applies to the Authorization State Machine flow diagram depicted in Figure 131.

a) Ovals are states.
b) Events are in *italics*.
c) Messages are in normal font.
d) State transitions (i.e., the lines between states) are labeled with <what causes the transition>/<messages and events triggered by the transition>. So "*timeout*/EAP Establish-Key Reply" means that the state received a "timeout" event and sent an Establish-Key Reply message. If there are multiple events or messages before the slash "/" separated by a comma, *any* of them can cause the transition. If there are multiple events or messages listed after the slash, *all* of the specified actions shall accompany the transition.

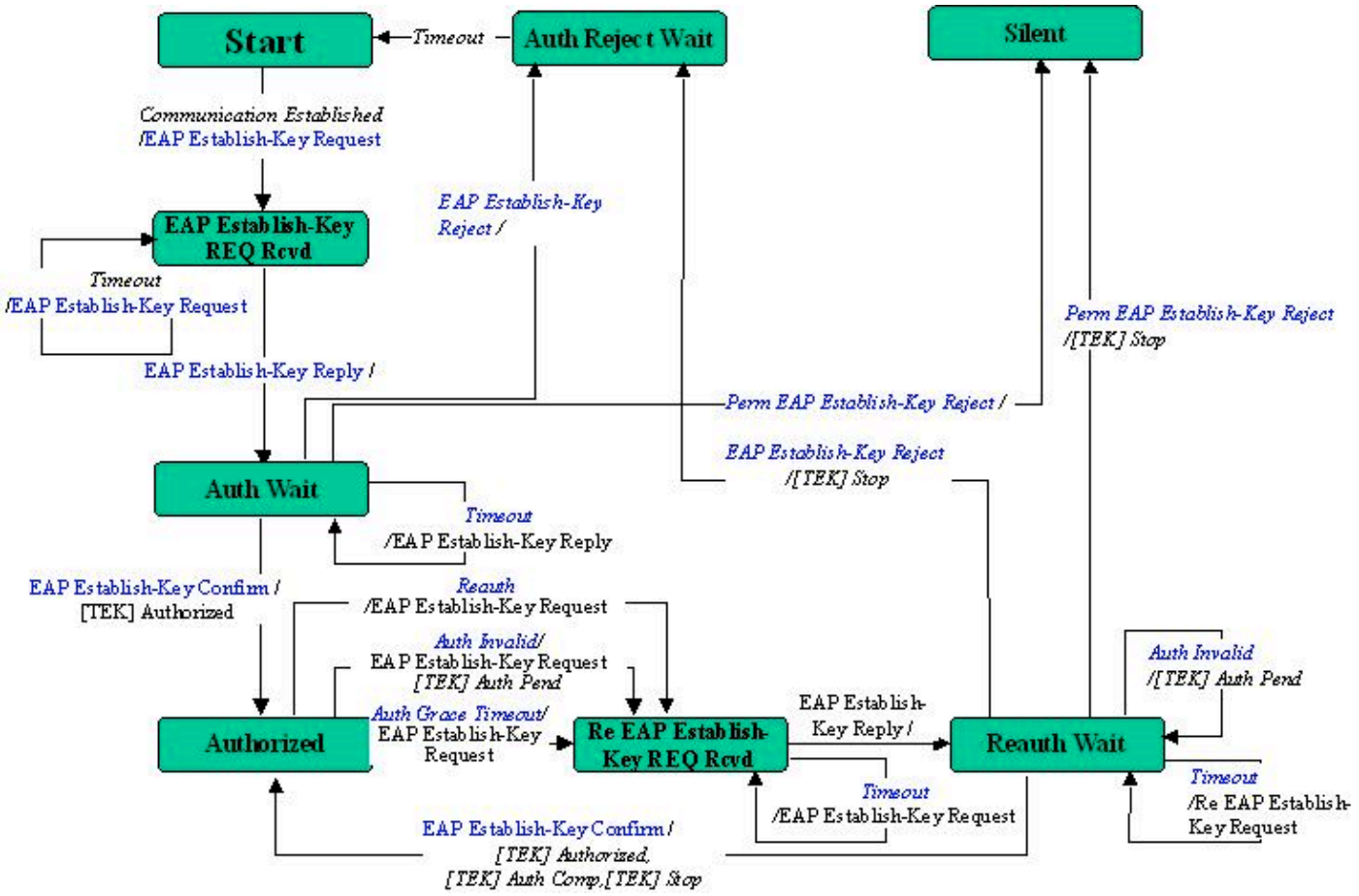

Figure 131 Authorization state machine flow diagram

Table 131 Authorization FSM state transition matrix

State Event or Rcvd Message	(A) Start	(B) EAP Establish-Key Request Rcvd	(C) Auth Wait	(D) Authorized	(E) Re EAP Establish-Key Request Rcvd	(F)Reauth Wait	(G) Auth Reject Wait	(H) Silent
(1)Communication Established	EAP Establish-Key Request Rcvd							
(2)EAP Establish-Key Reject			Auth Reject Wait			Auth Reject Wait		
(3)Perm EAP Establish-Key Reject			Silent			Silent		
(4)EAP Establish-Key Confirm			Authorized			Authorized		
(5)EAP Establish-Key Reply		Auth Wait			Reauth Wait			
(6)Timeout		EAP Establish-Key Request Rcvd	Auth Wait		Re EAP Establish-Key Request Rcvd	Reauth Wait	Start	
(7)Auth Grace Timeout				Re EAP Establish-Key Request Rcvd				
(8)Auth Invalid				Re EAP Establish-Key Request Rcvd		Reauth Wait		
(9)Reauth				Re EAP Establish-Key				

State Event or Rcvd Message	(A) Start	(B) EAP Establish-Key Request Rcvd	(C) Auth Wait	(D) Authorized	(E) Re EAP Establish-Key Request Rcvd	(F)Reauth Wait	(G) Auth Reject Wait	(H) Silent
				Request Rcvd				

The Authorization state transition matrix presented in Table 131 lists the eight Authorization machine states in the topmost row and the nine Authorization machine events (includes message receipts) in the leftmost column. Any cell within the matrix represents a specific combination of state and event, with the next state (the state transitioned to) displayed within the cell. For example, cell 4-C represents the receipt of an EAP Establish-Key Confirm message when in the Authorize Wait (Auth Wait) state. Within cell 4-C is the name of the next state, "Authorized." Thus, when an SS's Authorization state machine is in the Auth Wait state and an Auth Reply) or EAP Establish-Key Confirm message is received, the Authorization state machine will transition to the Authorized state. In conjunction with this state transition, several protocol actions shall be taken; these are described in the listing of protocol actions, under the heading 4-C, in 7.2.4.5.

A shaded cell within the state transition matrix implies that either the specific event cannot or should not occur within that state, and if the event does occur, the state machine shall ignore it. For example, if an EAP Establish-Key Confirm message arrives when in the Authorized state, that message should be ignored (cell 4-D). The SS may, however, in response to an improper event, log its occurrence, generate an SNMP event, or take some other vendor-defined action. These actions, however, are not specified within the context of the Authorization state machine, which simply ignores improper events.

7.2.4.1 States

a) *Start:* This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state—e.g., all timers are off, and no processing is scheduled.

b) *EAP Establish-Key Request Rcvd*: The SS has received the "Communication Established" event indicating that it has completed basic capabilities negotiation with the BS. In response to receiving the event, the BS has sent EAP Establish-Key Request and SS has received EAP Establish-Key Request.

c) *Authorize Wait (Auth Wait):* In response to receiving the EAP Establish-Key Request, the SS has responded with EAP Establish-Key Reply to the BS and is waiting for the reply. At this point, the SS has AK and KEK derived from the EAP Master Key which is to validated after receiving EAP Establish-Key Confirm.

d) *Authorized:* The SS has received an EAP Establish-Key Confirm message which contains a list of valid SAIDs for this SS. At this point, the SS has a valid AK and SAID list. Transition into this state triggers the creation of one TEK FSM for each of the SS's privacy-enabled SAIDs.

e) *Re EAP Establish-Key Request Rcvd* : The SS has received the "EAP Establish-Key Request" message sent by the BS when the BS was either about to expire (see Authorization Grace Time in Table 341) current authorization for the SS or received an indication that authorization for the SS is no longer valid.

f) *Reauthorize Wait (Reauth Wait):* The SS has an outstanding EAP Establish-Key Reply. The SS sent an EAP Establish-Key Reply following EAP Establish-Key Request message to the BS and is waiting for a response.

g) *Authorize Reject Wait (Auth Reject Wait):* The SS received an EAP Establish-Key Reject message in response to its last EAP Establish-Key Reply. The EAP Establish-Key Reject's error code indicated the error was not of a permanent nature. In response to receiving this reject message, the SS set a timer and transitioned to the Auth Reject Wait state. The SS remains in this state until the timer expires.

h) *Silent:* The SS received an EAP Establish-Key Reject message in response to its last EAP Establish-Key Reply following EAP Establish-Key Request. The EAP Establish-Key Reject's error code indicated the error was of a permanent nature. This triggers a transition to the Silent state, where the SS is not permitted to pass subscriber traffic. The SS shall, however, respond to management messages from the BS issuing the Perm EAP Establish-Key Reject.

7.2.4.2 Messages

Note that the message formats are defined in detail in 6.3.2.3.9.

EAP Establish-Key Request: Forward a nonce and MKID optionally to utilize the cached MK. Sent from BS to SS.

EAP Establish-Key Reply: Forward a nonce and security capabilities of SS. Sent from SS to BS.

EAP Establish-Key Confirm: Receive Key Sequence Number of authorized SAIDs and SA descriptors. Sent from the BS to the SS.

EAP Establish-Key Reject: Attempt to authorize was rejected. Sent from the BS to the SS.

Authorization Invalid (Auth Invalid): The BS may send an Authorization Invalid message to a client SS as follows:

a) an unsolicited indication, or
b) a response to a message received from that SS.

In either case, the Auth Invalid message instructs the receiving SS to re-authorize with its BS. The Auth Invalid message is followed by EAP Establish-Key Request, which is also sent by the BS.

The BS responds to a Key Request with an Auth Invalid message if (1) the BS does not recognize the SS as being authorized (i.e., no valid AK associated with SS) or (2) verification of the Key Request's keyed message digest (in HMAC-Digest attribute) failed. Note that the Authorization Invalid *event*, referenced in both the state flow diagram and the state transition matrix, signifies either the receipt of an Auth Invalid message or an internally generated event.

7.2.4.3 Events

Communication Established: The Authorization state machine generates this event upon entering the Start state if the MAC has completed basic capabilities negotiation. If the basic capabilities negotiation is not complete, the SS sends a Communication Established event to the Authorization FSM upon completing basic capabilities negotiation. The Communication Established event triggers the SS to begin the process of getting its AK and TEKs.

Timeout: A retransmission or wait timer timed out. Generally a request is received from the BS.

Authorization Grace Timeout (Auth Grace Timeout): The Authorization Grace timer timed out. This timer fires a configurable amount of time (the Authorization Grace Time) before the current authorization is supposed to expire, signalling the SS to reauthorize before its authorization actually expires. The Authorization Grace Time takes the default value from Table 341 or may be specified in a configuration setting within the EAP Establish-Key Confirm message.

Reauthorize (Reauth): SS's set of authorized static SAIDs may have changed. This event is generated in response to an SNMP set and meant to trigger a reauthorization cycle.

Authorization Invalid (Auth Invalid): This event is internally generated by the SS when there is a failure authenticating a Key Reply or Key Reject message, or externally generated by the receipt of an Auth Invalid message, sent from the BS to the SS. A BS responds to a Key Request with an Auth Invalid if verification of the request's message authentication code fails. Both cases indicate BS and SS have lost AK synchronization.

A BS may also send to an SS an unsolicited Auth Invalid message, forcing an Auth Invalid event.

Perm EAP Establish-Key Reject: The SS receives an EAP Establish-Key Reject in response to an EAP Establish-Key Reply. The error code in the EAP Establish-Key Reject indicates the error is of a permanent nature. What is interpreted as a permanent error is subject to administrative control within the BS. EAP Establish-Key Reply processing errors that can be interpreted as permanent error conditions include:

a) incompatible security capabilities

When an SS receives an EAP Establish-Key Reject indicating a permanent failure condition, the Authorization State machine moves into a Silent state, where the SS is not permitted to pass subscriber traffic. The SS shall, however, respond to management messages from the BS issuing the Perm EAP Establish-Key Reject. The SS shall also issue an SNMP Trap upon entering the Silent state.

Perm EAP Establish-Key Reject: The SS receives an EAP Establish-Key Reject in response to an EAP Establish-Key Reply. The error code in the EAP Establish-Key Reject does not indicate the failure was due to a permanent error condition. As a result, the SS's Authorization state machine shall set a wait timer and transition into the Auth Reject Wait State. The SS shall remain in this state until the timer expires, at which time it shall reattempt authorization.

NOTE—The following events are sent by an Authorization state machine to the TEK state machine:

[TEK] Stop: Sent by the Authorization FSM to an active (non-START state) TEK FSM to terminate the FSM and remove the corresponding SAID's keying material from the SS's key table.

[TEK] Authorized: Sent by the Authorization FSM to a nonactive (START state), but valid TEK FSM.

[TEK] Authorization Pending (Auth Pend): Sent by the Authorization FSM to a specific TEK FSM to place that TEK FSM in a wait state until the Authorization FSM can complete its reauthorization operation.

[TEK] Authorization Complete (Auth Comp): Sent by the Authorization FSM to a TEK FSM in the Operational Reauthorize Wait (Op Reauth Wait) or Rekey Reauthorize Wait (Rekey Reauth Wait) states to clear the wait state begun by a TEK FSM Authorization Pending event.

7.2.4.4 Parameters

All configuration parameter values take the default values from Table 341 or may be specified in the EAP Establish-Key Confirm message.

Authorize Wait Timeout (Auth Wait Timeout): Timeout period between sending EAP Establish-Key Reply messages from Auth Wait state (see 11.9.19.2).

Authorization Grace Timeout (Auth Grace Timeout): Amount of time before authorization is scheduled to expire that the BS starts reauthorization (see 11.9.19.3.

Authorize Reject Wait Timeout (Auth Reject Wait Timeout): Amount of time an SS's Authorization FSM remains in the Auth Reject Wait state before transitioning to the Start state (see 11.9.19.7).

EAP Establish-Key Request Rcvd Timeout: Timeout period between receiving EAP Establish-Key Request message from EAP Establish-Key Rcvd state.

7.2.4.5 Actions

Actions taken in association with state transitions are listed by <event> (<rcvd message>) --> <state> below:

1-A Start (*Communication Established*)_EAP Establish-Key Request Rcvd

a) receive EAP Establish-Key Request from BS
b) set EAP Establish-Key Request retry timer to EAP Establish-Key Request Rcvd Timeout

2-C Auth Wait (*EAP Establish-Key Reject*) _→ Auth Reject Wait

a) clear EAP Establish-Key Request retry timer
b) set a wait timer to Auth Reject Wait Timeout

2-F Reauth Wait (*EAP Establish-Key Reject*) _→ Auth Reject Wait

a) clear EAP Establish-Key Request retry timer
b) generate TEK FSM Stop events for all active TEK state machines
c) set a wait timer to Auth Reject Wait Timeout

3-C Auth Wait (*Perm Establish-Key Reject*) _→ Silent

a) clear EAP Establish-Key Request retry timer
b) disable all forwarding of SS traffic

3-F Reauth Wait (*Perm Establish-Key Reject*) _→ Silent

a) clear EAP Establish-Key Request retry timer
b) generate TEK FSM Stop events for all active TEK state machines
c) disable all forwarding of SS traffic

4-C Auth Wait (EAP Establish-Key Confirm) _→ Authorized

a) clear EAP Establish-Key Request retry timer
b) activate AK confirmed by EAP Establish-Key Confirm
c) start TEK FSMs for all SAIDs listed in EAP Establish-Key Confirm(provided the SS supports the cryptographic suite that is associated with an SAID) and issue a TEK FSM Authorized event for each of the new TEK FSMs
d) set the Authorization Grace timer to go off "Authorization Grace Time" seconds prior to the supplied AK's scheduled expiration

4-F Reauth Wait (EAP Establish-Key Confirm) _→ Authorized

a) clear EAP Establish-Key Request retry timer
b) activate AK confirmed by EAP Establish-Key Confirm
c) start TEK FSMs for any newly authorized SAIDs listed in EAP Establish-Key Confirm(provided the SS supports the cryptographic suite that is associated with the new SAID) and issue TEK FSM Authorized event for each of the new TEK FSMs
d) generate TEK FSM Authorization Complete events for any currently active TEK FSMs whose corresponding SAIDs were listed in EAP Establish-Key Confirm
e) generate TEK FSM Stop events for any currently active TEK FSMs whose corresponding SAIDs were not listed in EAP Establish-Key Confirm
f) set the Authorization Grace timer to go off "Authorization Grace Time" seconds prior to the supplied AK's scheduled expiration

5-B EAP Establish-Key Request Rcvd (EAP Establish-Key Reply) → Auth Wait

a) send EAP Establish-Key Reply message to BS
b) set EAP Establish-Key Reply retry timer to Auth Wait Timeout

5-E Re EAP Establish-Key Request Rcvd (EAP Establish-Key Reply) _→ ReAuth Wait

a) send EAP Establish-Key Reply message to BS
b) set EAP Establish-Key Reply retry timer to Auth Wait Timeout

6-B EAP Establish-Key Request Rcvd (*Timeout*) → EAP Establish-Key Request Rcvd

a) receive EAP Establish-Key Request message from BS
b) set EAP Establish-Key Request retry timer to EAP Establish-Key Request Rcvd Timeout

6-C Auth Wait (*Timeout*) _→ Auth Wait

a) send EAP Establish-Key Reply message to BS
c) set EAP Establish-Key Reply retry timer to Auth Wait Timeout

6-E Re EAP Establish-Key Request Rcvd (*Timeout*) → Re EAP Establish-Key Request Rcvd

a) receive EAP Establish-Key Request message from BS
b) set EAP Establish-Key Request retry timer to EAP Establish-Key Request Rcvd Timeout

6-F Reauth Wait (*Timeout*) _→ Reauth Wait

a) send EAP Establish-Key Reply message to BS
b) set EAP Establish-Key Request retry timer to Reauth Wait Timeout

6-G Auth Reject Wait (*Timeout*) _→ Start

a) no protocol actions associated with state transition

7-D Authorized (*Auth Grace Timeout*) _→ Re EAP Establish-Key Request Rcvd

a) receive Establish-Key Request message from BS
b) set Establish-Key Request retry timer to Reauth Wait Timeout

8-D Authorized (*Auth Invalid*) _→ Re EAP Establish-Key Request Rcvd

a) clear Authorization Grace timer
b) receive Establish-Key Request message from BS
c) set Establish-Key Request retry timer to Reauth Wait Timeout
d) if the Auth Invalid event is associated with a particular TEK FSM, generate a TEK FSM Authorization Pending event for the TEK state machine responsible for the Auth Invalid event (i.e., the TEK FSM that either generated the event, or sent the Key Request message the BS responded to with an Auth Invalid message)

8-F Reauth Wait (*Auth Invalid*) _→ Re EAP Establish-Key Request Rcvd

a) if the Auth Invalid event is associated with a particular TEK FSM, generate a TEK FSM Authorization Pending event for the TEK state machine responsible for the Auth Invalid event (i.e., the TEK FSM that either generated the event, or sent the Key Request message the BS responded to with an Auth Invalid message)

9-D Authorized (*Reauth*) _→ Re EAP Establish-Key Request Rcvd

a) clear Authorization Grace timer
b) receive Establish-Key Request message from BS
c) set Establish-Key Request retry timer to Reauth Wait Timeout

[Change the 7.4 of REVd/D5 and put in REVe/D4 as the following:]

7.4 Key usage

7.4.1 BS key usage

The BS is responsible for maintaining keying information for all SAs. The PKM protocol defined in this specification describes a mechanism for synchronizing this keying information between a BS and its client SS.

7.4.1.1 AK key lifetime

After an SS completes basic capabilities negotiation, it shall initiate an authorization exchange with its BS. The BS's first receipt of an Auth Request or EAP Establish-Key Reply following EAP Establish-Key Request message from the unauthorized SS shall initiate the activation of a new AK, which the BS sends back to the requesting SS in an Auth Reply or EAP Establish-Key Confirm message. This AK shall remain active until it expires according to its predefined *AK Lifetime*, a BS system configuration parameter.

The AK's active lifetime a BS reports in an Authorization Reply or EAP Establish-Key Confirm message shall reflect, as accurately as an implementation permits, the remaining lifetimes of AK at the time the Authorization Reply or EAP Establish-Key Confirm message is sent.

If an SS fails to reauthorize before the expiration of its current AK, the BS shall hold no active AKs for the SS and shall consider the SS *unauthorized*. A BS shall remove from its keying tables all TEKs associated with an unauthorized SS's Primary SA.

7.4.1.2 AK transition period on BS side

For PKM RSA case, t~~T~~he BS shall always be prepared to send an AK to an SS upon request. For PKM EAP case, the BS shall always be prepared to authorize the SS to activate the AK upon request. The BS shall be able to support two simultaneously active AKs for each client SS. The BS has two active AKs during an AK transition period;the two active keys have overlapping lifetimes.

An AK transition period begins when the BS receives an Auth Request or EAP Establish-Key Reply following EAP Establish-Key Request message from an SS and the BS has a single active AK for that SS. In response to this Auth Request or EAP Establish-Key Reply, the BS activates a second AK [see point (a) and (d) in Figure 133], which shall have a key sequence number one greater (modulo 16) than that of the existing AK and for PKM EAP case it shall be sent back to the requesting SS in an Auth Reply message. The BS shall set the active lifetime of this second AK to be the remaining lifetime of the first AK (between points (a) and

(c) in Figure 133), plus the predefined *AK Lifetime*; thus, the second, "newer" key shall remain active for one *AK Lifetime* beyond the expiration of the first, "older" key. The key transition period shall end with the expiration of the older key. This is depicted on the right-hand side of Figure 133.

As long as the BS is in the midst of an SS's AK transition period, and thus is holding two active AKs for that SS, it shall respond to Auth Request or EAP Establish-Key Reply messages with the newer of the two active keys. Once the older key expires, an Auth Request or EAP Establish-Key Reply following EAP Establish-Key Request shall trigger the activation of a new AK, and the start of a new key transition period.

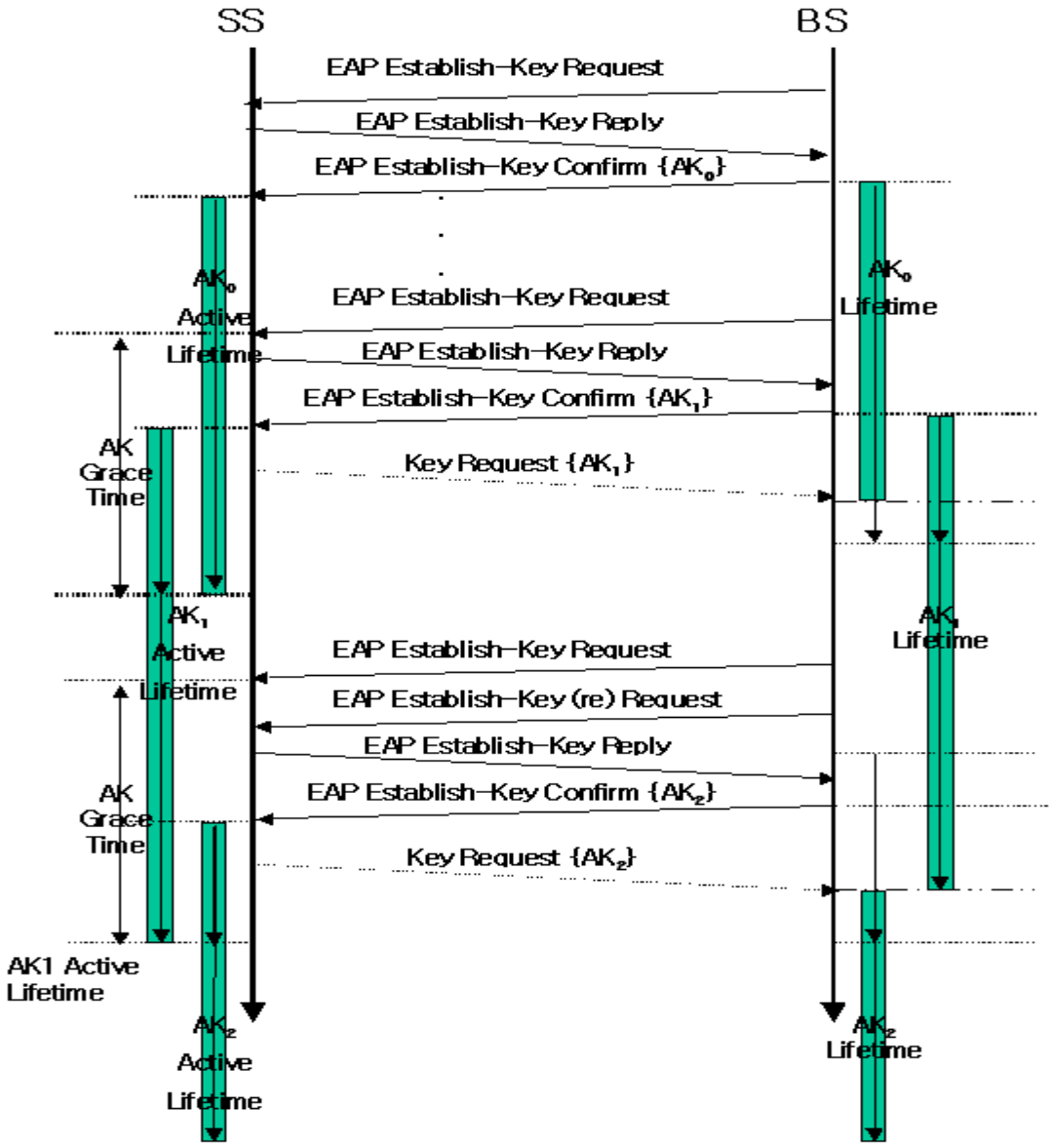

Figure 133 AK management in BS and SS

[Add the following:]

11.9.19.8 EAP Establish-Key Request Rcvd timeout

The Vale of the field specifies retransmission interval, in seconds, of EAP-Establish-Key Request messages from the EAP-Establish-Key Request Rcvd state.