Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**PKM EAP State Machine**
Date Submitted	**2004-11-4**
Source(s)	Bryan Kim, Dongkie Lee, JungPyo Han, DongIl Moon, Kang Il Koh SK Telecom Voice: +82-31-710-5329 [mailto: {kkhoon, galahad, jphan, dimoon, melomo}@sktelecom.com]
Re:	Sponsor Ballot 16e
Abstract	PKM EAP state machine and call flow are reflected based on Contribution #407.
Purpose	Discuss and Adopt as the baseline text
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>.

1

PKM EAP State Machine

Brian Kim, Dongkie Lee, JungPyo Han, DongIl Moon, KangIl Koh
SK Telecom

1. Problem Statements

Based on the premise that contribution #462 is accepted, PKM EAP state machine should be changed according to the contribution #462.

In this contribution, state machine and call flow is changed to reflect the newly defined messages such as EAP Establish-Key Request, EAP Establish-Key Reply/Reject messages whose characteristics are quite similar to Auth Request, Auth Reply/Reject.

2 Proposed Changes

[Add following Section to P802.16e-04/D5:]

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 Reply 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 and the EAP Establish-Key Request if it determines that none of the offered cryptographic suites are satisfactory.

The Authorization Reply and the EAP Establish-Key Reply 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 and the EAP Establish-Key Reply 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.

7.2.4 Authorization state machine

The Authorization state machine consists of six states and eight 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*/Auth Request or EAP Establish-Key Request " means that the state received a "timeout" event and sent an Authorization Request ("Auth Request") message or EAP Establish-Key Request 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.

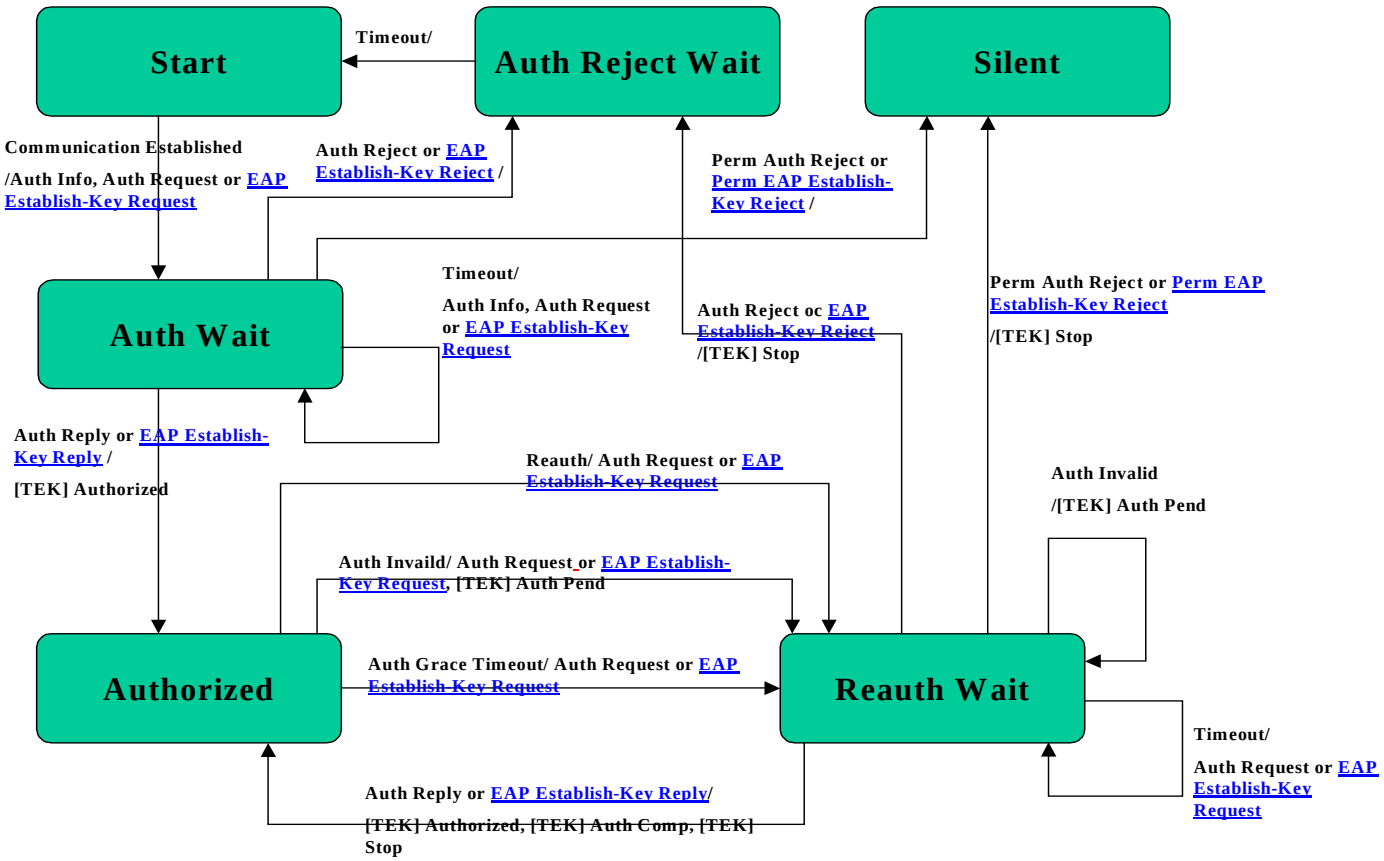

Figure 1Authorization state machine flow diagram

Table 131 Authorization FSM state transition matrix

State Event or Rcvd Message	(A) Start	(B) Auth Wait	(C) Authorized	(D) Reauth Wait	(E) Auth Reject Wait	(F) Silent
(1) Communication Established	Auth Wait					
(2) Auth Reject or EAP Establish-Key Reject		Auth Reject Wait		Auth Reject Wait		

State Event or Rcvd Message	(A) Start	(B) Auth Wait	(C) Authorized	(D) Reauth Wait	(E) Auth Reject Wait	(F) Silent
(3) Perm Auth Reject or Perm EAP Establish-Key Reject		Silent		Silent		
(4) Auth Reply or EAP Establish-Key Reply		Authorized		Authorized		
(5) Timeout		Auth Wait		Reauth Wait	Start	
(6) Auth Grace Timeout			Reauth Wait			
(7) Auth Invalid			Reauth Wait	Reauth Wait		
(8) Reauth			Reauth Wait			

The Authorization state transition matrix presented in Table 131 lists the six Authorization machine states in the topmost row and the eight 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-B represents the receipt of an Authorization Reply (Auth Reply) or EAP Establish-Key Reply message when in the Authorize Wait (Auth Wait) state. Within cell 4-B 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 Reply 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-B, 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 Auth Reply or EAP Establish-Key Reply message arrives when in the Authorized state, that message should be ignored (cell 4-C). 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) *Authorize Wait (Auth Wait):* The SS has received the "Communication Established" event indicating that it has completed basic capabilities negotiation with the BS. For PKM RSA case ~~i~~In response to receiving the event, the SS has sent both an Authentication Information and an Auth Request message to the BS and is waiting for the reply. For PKM EAP case in response to receiving the event, the BS has sent EAP Establish-Key Request and the SS has responded with EAP Establish-Key Reply to the BS and is waiting for the reply.

c) *Authorized:* The SS has received an Auth Reply or EAP Establish-Key Reply 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.

d) *Reauthorize Wait (Reauth Wait):* The SS has an outstanding reauthorization request or outstanding EAP Establish-Key Request. The SS was either about to expire (see Authorization Grace Time in Table 341) its current authorization or received an indication (an Authorization Invalid message from the BS) that its authorization is no longer valid. The SS sent an Auth Request or EAP Establish-Key Request message to the BS and is waiting for a response.

e) *Authorize Reject Wait (Auth Reject Wait):* The SS received an Authorization Reject (Auth Reject) or EAP Establish-Key Reject

message in response to its last Auth Request or EAP Establish-Key Request. The Auth Reject and 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.

f) *Silent:* The SS received an Auth Reject or EAP Establish-Key Reject message in response to its last Auth Request or EAP Establish-Key Request. The Auth Reject and 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 Auth Reject or 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.

Authorization Request (Auth Request): Request an AK and list of authorized SAIDs. Sent from SS to BS.

Authorization Reply (Auth Reply): Receive an AK and list of authorized, static SAIDs. Sent from BS to SS. The AK is encrypted with the SS's public key.

Authorization Reject (Auth Reject): Attempt to authorize was rejected. Sent from the BS to the SS.

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

EAP Establish-Key Reply: 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 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.

Authentication Information (Auth Info): The Auth Info message contains the SS manufacturer's X.509 Certificate, issued by an external authority. The Auth Info message is strictly an informative message the SS sends to the BS; with it, a BS may dynamically learn the manufacturer certificate of client SS. Alternatively, a BS may require out-of-band configuration of its list of manufacturer certificates.

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 resent.

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 Auth Reply and EAP Establish-Key Reply 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.

Permanent Authorization Reject (Perm Auth Reject), Perm EAP Establish-Key Reject: The SS receives an Auth Reject or EAP Establish-Key Reject in response to an Auth Request or EAP Establish-Key Request. The error code in the Auth Reject and 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. Auth Request processing errors that can be interpreted as permanent error conditions include:

a) unknown manufacturer (do not have CA certificate of the issuer of the SS Certificate)
b) invalid signature on SS certificate
c) ASN.1 parsing failure
d) inconsistencies between data in the certificate and data in accompanying PKM data attributes
e) incompatible security capabilities

When an SS receives an Auth Reject or 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 Auth Reject or Perm EAP Establish-Key Reject. The SS shall also issue an SNMP Trap upon entering the Silent state.

Authorization Reject (Auth Reject), Perm EAP Establish-Key Reject: The SS receives an Auth Reject or *EAP Establish-Key Reject* in response to an Auth Request. The error code in the Auth Reject and 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 Auth Reply message.

Authorize Wait Timeout (Auth Wait Timeout): Timeout period between sending Authorization Request or EAP Establish-Key Request 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 SS 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).

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 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 Reply 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 Reply message shall reflect, as accurately as an implementation permits, the remaining lifetimes of AK at the time the Authorization Reply or EAP Establish-Key Reply 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 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 Request, 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 RSA 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 Request messages with the newer of the two active keys. Once the older key expires, an Auth Request or EAP Establish-Key Request shall trigger the activation of a new AK, and the start of a new key transition period.

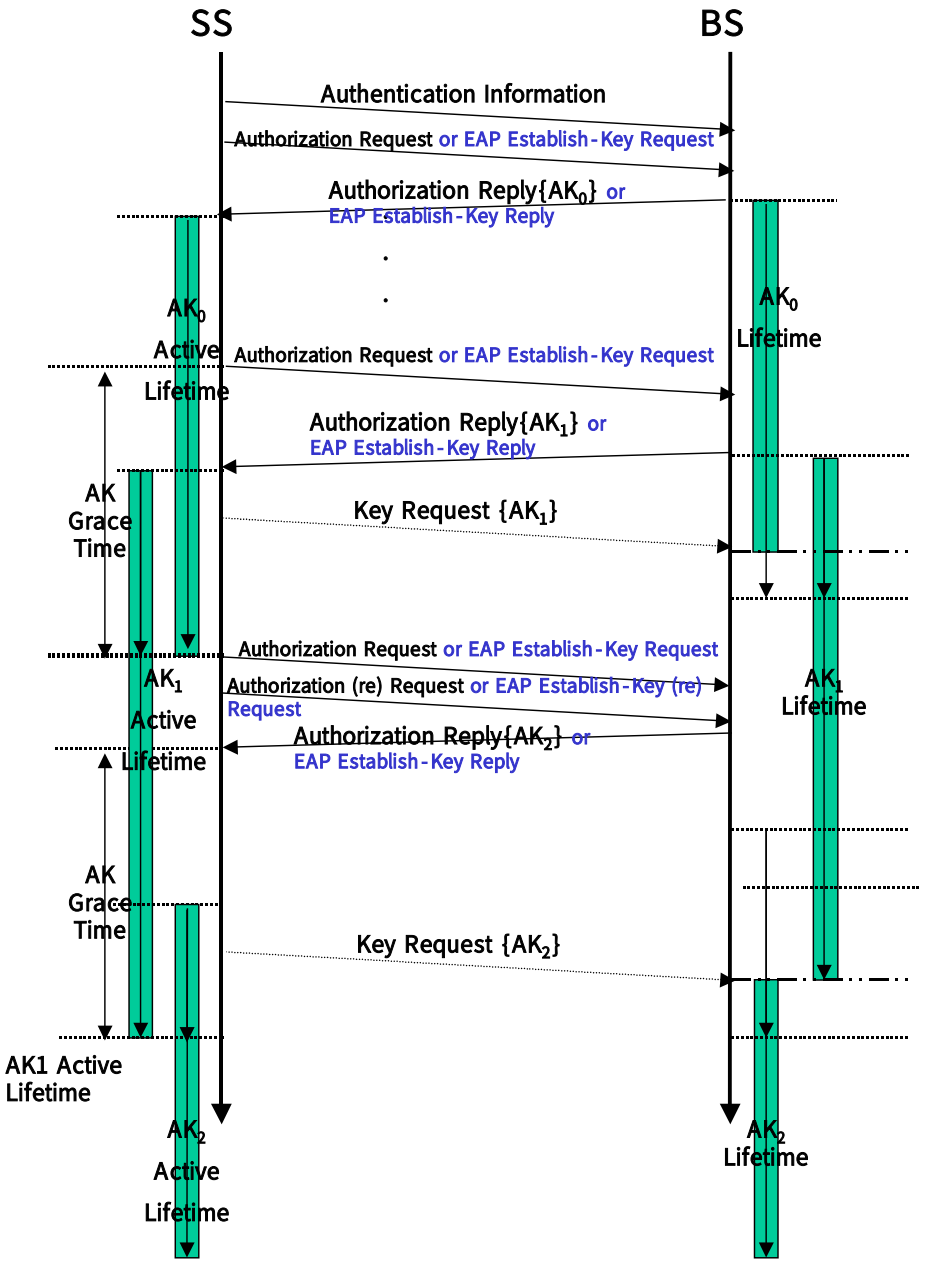

Figure 133 AK management in BS and SS