Project	IEEE 802.16 Broadband Wireless Access Working Group <***http://ieee802.org/16***>		
Title	Auth FSM		
Date Submitted	2007-02-16		
Source(s)	Avishay Shraga	Intel corporation	voice: +972-3-920-5763
	Phillip Barber	Huawei	*avishay.shraga@intel.com*
	Joseph Schumacher	Motorola	
	Tricci So	Nortel	
	Modified by		Tel: +82-31-279-5748
	Kyeong-Tae Do	Samsung	*kyeongtae.do@samsung.com*
	Wonil Roh	Samsung	*chosh@etri.re.kr*
	Seokheon Cho	ETRI	*poong2@posdata.co.kr*
	Sungho Yoo	PosData	*ksryu@lge.com*
	Kiseon Ryu	LG	
Re:	IEEE Std 802.16-2004/Cor2/D2		
Abstract	The contribution defines the Authorization FSM for PKMv2 EAP only authentication. Including States, Events and Transitions		
Purpose	Resolve ambiguity in definition of Auth FSM		
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>.

Single EAP Authorization FSM

Intel Corporation, modified by Samsung

1. Background

The standard defines the FSM for TEK exchange but does not define the FSM for Authentication.
The absence of this FSM makes it very unclear how the authentication and re-authentication are done during initial entry and reentry from HA HO and from idle.

The previous document does not include the reentry procedure that does not need 3-way handshake. The state machine has modified to handle reentry without 3-way handshake.

The previous document separates the operations for 3-way handshake failure during re-authentication. The failure of 3-way handshake indicates EAP phase was successful. It may have some meanings if the operations for EAP failure are separated by initiating entity. If the numbers of maximum resending times of SA-TEK messages are not enough, they should be modified large. If the numbers are big enough to handle the transmission errors, the Authorization FSM does not have to handle the 3-way handshake failure. Transmission failure will be handled by some internal events not by the Authorization FSM.

2. Suggested remedy

Define the Auth FSM for EAP only authentication as negotiated in SBC.
The FSM includes states events and transitions to support initial authentication, re-authentication and reentry for HO and idle.

Remove the modification regarding 3-way handshake failure during re-authentication.

3. Proposed Text Changes

[In section 7.2.2.5, perform the indicated change to page 180 of P80216-Cor2_D2]
Figure 132a – TEK state machine flow diagram for PKMv2

[In section 7.2.2.5, perform the indicated change to page 181 of P80216-Cor2_D2]
Table 134a – TEK FSM state transition matrix for PKMv2

[Please move the following sub-clauses as indicated new sub-clauses of P80216-Cor2_D2]
[page 179]
7.2.2.56 TEK state machine
[page 181]
7.2.2.56.1 States
7.2.2.56.2 Messages
7.2.2.56.3 Events
[page 182]
7.2.2.56.4 Parameters
7.2.2.56.5 Actions

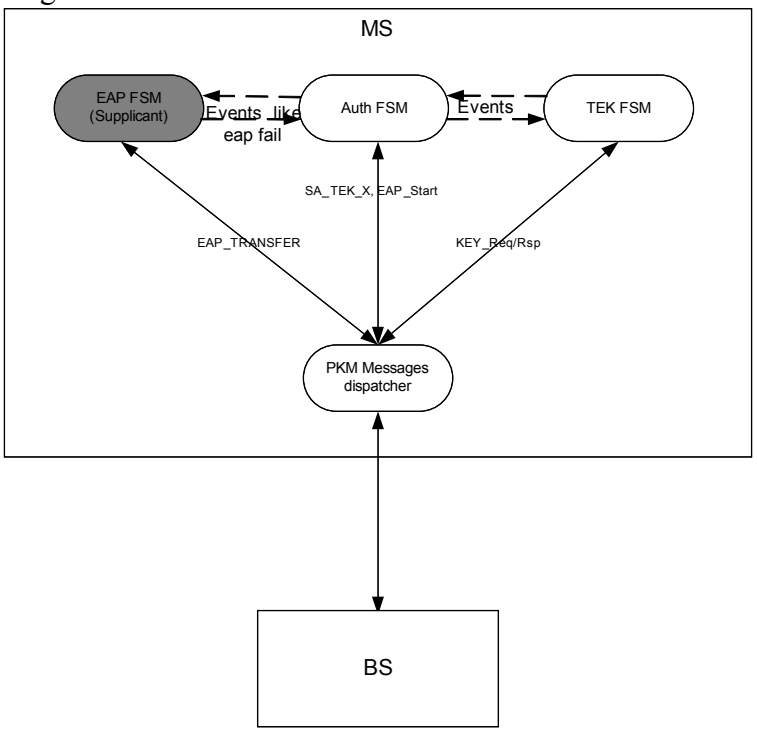
[Remove the whole section of 7.2.2.6 of P80216-Cor2_D2]

[Add the following text to page 179 below Table 133d of P80216-Cor2_D2]

7.2.2.5 Authorization state machine

The Authentication state machine for single EAP authentication consists of six states and sixteen events (including receipt of messages and events from other FSMs) that may trigger state transitions. The Authentication state machine is presented in both a state flow diagram (Figure XXX) and a state transition matrix (Table XXX).The state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

The Authentication process has 2 phases: EAP phase and 3-way handshake phase (also known as SA_TEK exchange).
The EAP phase is controlled by the EAP_FSM as defined in RFC3748 and RFC4173 and it is out of scope in this standard.
The Authorization FSM is responsible for all PKM phase but the actual EAP exchange and communicates with other FSMs in the system using events.
The relationships between the security-related FSMs in the system are as described in the diagram:



Through operation of an Authentication state machine, the MS attempts to get authenticated with the NW, maintain this authentication and support Authentication context switching for HO and Idle situations.
The state machine takes care of getting authenticated with the NW, ensuring re-

authentication will occur before authentication expires and support key derivations according to support optimized reentry for HO and idle.
The optimized reentry support is done in a special state in which the NW connection is suspended and therefore re-authentication can't occur, the triggers for re-authentication continue to work in this state but the initiation is done only after returning to an authenticated state.

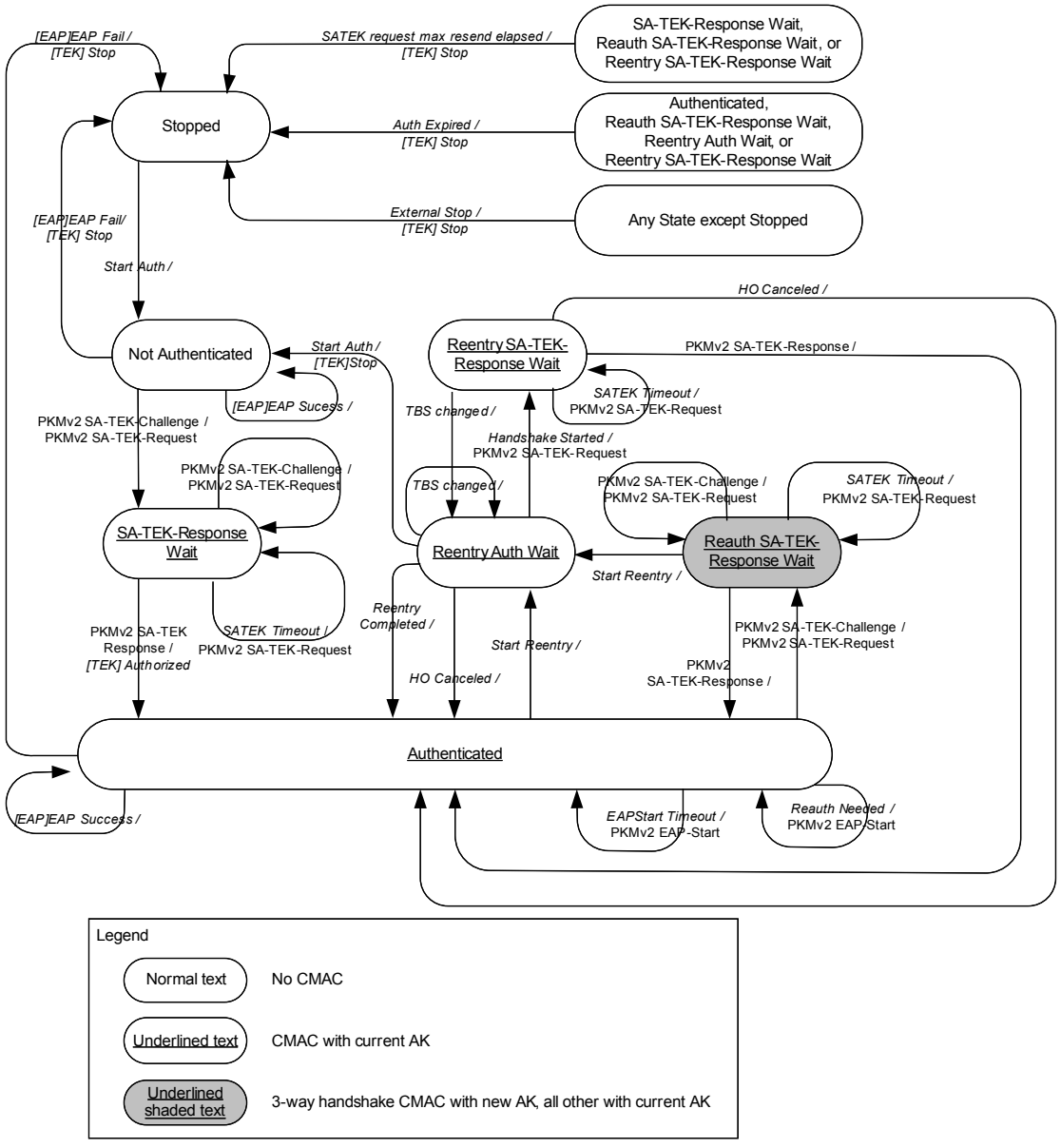


Figure 131a – Authentication State Machine for PKMv2 single EAP

Table 133a – Authorization FSM state transition matrix for PKMv2

State Event or receive message	(A) *Stopped*	(B) *Not Authenticated*	(C) *SA-TEK-Rsp Wait*	(D) *Authenticated*	(E) *Reauth SA-TEK-Rsp Wait*	(F) *Reentry Auth Wait*	(G) *Reentry SA-TEK-Rsp Wait*
(1) *Start Auth*	*Not Authenticated*					*Not Authenticated*	
(2) PKMv2 SA-TEK-Challenge		*SA-TEK-Rsp Wait*	*SA-TEK-Rsp Wait*	*Reauth SA-TEK-Rsp Wait*	*Reauth SA-TEK-Rsp Wait*		
(3) PKMv2 SA-TEK-Response			*Authenticated*		*Authenticated*		*Authenticated*
(4) *EAP Success*		*Not Authenticated*		*Authenticated*			
(5) *SATEK Timeout*			*SA-TEK-Rsp Wait*		*Reauth SA-TEK-Rsp Wait*		*Reentry SA-TEK-Rsp Wait*
(6) *SATEK req max resend elapsed*			*Stopped*		*Stopped*		*Stopped*
(7) *Reauth Needed*				*Authenticated*			
(8) *Start Reentry*				*Reentry Auth Wait*	*Reentry Auth Wait*		
(9) *EAPStart Timeout*				*Authenticated*			
(10) *Handshake Started*						*Reentry SA-TEK-Rsp Wait*	
(11) *HO Canceled*						*Authenticated*	*Authenticated*
(12) *TBS Changed*						*Reentry Auth Wait*	*Reentry Auth Wait*
(13)						*Authentic*	

Reentry Completed						*ated*	
(14) *Auth Expired*				*Stopped*	*Stopped*	*Stopped*	*Stopped*
(15) *EAP Fail*		*Stopped*		*Stopped*			
(16) *External Stop*		*Stopped*	*Stopped*	*Stopped*	*Stopped*	*Stopped*	*Stopped*

7.2.2.5.1 States

Stopped: This is the initial state of the FSM. Nothing is done in this state.

Not Authenticated: The Authorization FSM is not authenticated and waiting for an MSK from the EAP FSM to perform 3-way handshake. The FSM also waits for a PKMv2 SA-TEK-Challenge message in this state. Upon receiving a PKMv2 SA-TEK-Challenge message, the MS validates H/CMAC Digest using H/CMAC_KEY_D. Any PKMv2 SA-TEK-Challenge messages with invalid H/CMAC Digest or without H/CMAC Digest are discarded.

SA-TEK-Response Wait: The Authorization FSM has sent a PKMv2 SA-TEK-Request and waits for a PKMv2 SA-TEK-Response message in this state. If it does not receive a PKMv2 SA-TEK-Response message within SATEK Timer, the MS may resend the message up to SATEKRequestMaxResends times. Upon receiving a PKMv2 SA-TEK-Challenge message, the MS resends a PKMv2 SA-TEK-Request message. Any PKMv2 SA-TEK-Challenge or SA-TEK- Response messages with invalid H/CMAC Digest or without H/CMAC Digest are discarded.

Authenticated: The MS has successfully completed EAP-based authentication and has valid PMK context and AK context derived from the MSK from the EAP FSM.. Transition from SA-TEK-Response Wait into this state triggers the creation of TEK FSMs.
If the MS has a valid AK context, all the management messages with Basic CID or Primary Management CID should be sent with H/CMAC Digest/Tuple. It should be discarded if the message does not have a valid H/CMAC Digest/Tuple.
In this state the MS may hold two AK contexts: the old AK context and the new AK context which is created during re-authentication. The old AK context is deleted in the frame number specified in the PKMv2 SA-TEK-Response message.
In addition, the Authorization FSM also waits for a PKMv2 SA-TEK-Challenge message in this state before the AK expires.

Reauth SA-TEK-Response Wait: The Authorization FSM has sent a PKMv2 SA-TEK-Request message for re-authentication and waits for a PKMv2 SA-TEK-Response message. If it does not receive a PKMv2 SA-TEK-Response message within SATEK Timer, the MS may resend the message up to SATEKRequestMaxResends times.

In this state there are two AK contexts: the old AK context for the management messages which need H/CMAC-Tuple and new AK context for 3-way handshake messages during re-authentication. The new AK context is created as soon as EAP phase is completed. After the completion of the 3-way handshake, the new AK context should be used.

Reentry Authentication Wait: In this state the Authorization FSM has the AK context of the target BS. The MS should have the AK context of the target BS in this state before it sends a RNG-REQ message with H/CMAC Tuple during HO or reentry. During HO or reentry, the Authorization FSM is in this state when the MS sends a RNG-REQ message. The state of Authorization FSM changes when the MS receives a RNG-RSP message. The next state depends on the value of HO Process Optimization TLV included in the received RNG-RSP message. If HO Process Optimization Bit #1 set to zero, meaning the PKM Authentication phase is not omitted, the Authorization FSM receives Start Authentication event which triggers to stop all the TEK FSMs, re-initialize the Authorization FSM and change the state to Not Authenticated. The TLVs included in the RNG-RSP message also affects the next state. If HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SA-TEK-Update TLV is included in the RNG-RSP, the FSM receives Reentry Completed event. The state of the Authorization FSM changes to Authenticated when the Reentry Completed event is issued. In the case HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SA-Challenge Tuple TLV is included in the RNG-RSP, the next state is Reentry SA-TEK-Response Wait.

Reentry SA-TEK-Response Wait: The Authorization FSM has received Handshake Started event which is issued when the MS has received a RNG-RSP message with HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SA-Challenge Tuple TLV during reentry. If it does not receive a PKMv2 SA-TEK-Response message within SATEK Timer, the MS may resend the message up to SATEKRequestMaxResends times.

7.2.2.5.2 Messages

PKMv2 SA-TEK-Challenge: The first message of 3-way handshake. It is sent from the BS to the MS after EAP-based authentication has finished and it is protected by H/CMAC-Digest using H/CMAC_KEY_D of the last EAP-based authentication.

PKMv2 SA-TEK-Request: The second message of 3-way handshake. It is sent from the MS to the BS as a response to a PKMv2 SA-TEK-Challenge message, protected by CMAC-Digest using H/CMAC_KEY_U of the last EAP-based authentication.

PKMv2 SA-TEK-Response: The last message of 3-way handshake. It is sent from the BS to the MS as a response to a PKMv2 SA-TEK-Request message and it is protected by CMAC-Digest using H/CMAC_KEY_D of the last EAP-based authentication.

PKMv2 EAP Start: The message used by the MS to initiate EAP-based re-authentication. If the BS does not respond with PKMv2 EAP Transfer messages, the MS resends it to start re-authentication.

PKMv2 EAP Transfer: This message is bidirectional and used for transmission of EAP packet. This message is sent unprotected in “Not Authenticated” state. In Authenticated state, H/CMAC Digest and Key Sequence Number attributes shall be included in the message.

7.2.2.5.3 Events

Start Authentication: After completion of basic capabilities negotiation, this event is generated to start the Authentication state machine. It is also issued when the HO Process Optimization Bit #1 of the RNG-RSP message is set to zero during HO or network reentry.

EAP Success: EAP FSM generates this event to notify the Authorization FSM that EAP protocol has been completed successfully.

SATEK Timeout: This event is generated when the MS does not receive PKMv2 SA-TEK-Response message from the BS within SATEK Timer after transmitting a PKMv2 SA-TEK-Request message. The MS may resend the PKMv2 SA-TEK-Request up to SATEKRequestMaxResends times.

SATEK request max resends elapsed: The Authorization state machine generates this event when the MS has transmitted the PKMv2 SA-TEK-Request message up to SATEKRequestMaxResends times and SATEK Timer expires.

Re-authentication Needed: An internal event to trigger re-authentication. This event can be derived from several sources such as Authorization Grace Timeout or other reason that makes authentication close to expiration.

Start Reentry: An event to inform the Authorization FSM that MS is in reentry phase. The FSM should derive the new AK context for the target BS.

EAPStart Timeout: A timer event that causes the MS to resend a PKMv2 EAP-Start message in order to ask the BS to start EAP-based re-authentication. This event is used in the case Authorization FSM does receive neither EAP Failure event nor EAP Success event after transmitting the PKMv2 EAP Start message. This timer is active only after Re-authentication Needed event occurred.

Handshake Started: An event to notify the Authorization FSM that the MS has received SA-Challenge Tuple TLV to start SA-TEK 3-way handshake. This event is issued when the MS receives a RNG-RSP message including HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and SA-Challenge Tuple TLV during HO or network reentry.

Reentry Completed: An event to notify the Authorization FSM that reentry has finished successfully. This event is issued when the MS receives a RNG-RSP message including HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and SA-TEK-Update TLV during HO or network reentry from Idle mode. This event is also issued when the MS receives a RNG-RSP message including HO Process Optimization Bit #1 and Bit #2 both set to one during HO.

HO Canceled: An event to notify the Authorization FSM that HO was canceled. The cached AK context for the serving BS should be retrieved.

TBS (Target BS) changed: An Event to notify the Authorization FSM that it needs to generate the AK context for the new target BS.

Authentication Expired: This event indicates the AK context became obsolete due to the expiration of AK lifetime.

EAP Failure: This event indicates EAP-based authentication has failed.

External Stop: The event to stop the Authorization FSM and terminate connection with BS.

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. This event shall be sent to the TEK FSM in the Operational Wait (Op Wait) or Rekey Wait states when Authorization FSM starts re-authentication.

[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. This event shall be sent to the TEK FSM in the Operational Reauthorize Wait or Rekey Reauthorize Wait states when Authorization FSM ends re-authentication.

7.2.2.5.4 Parameters

SATEK Timer: The timer which expires if the MS does not receive a PKMv2 SA-TEK-Response message after sending a PKMv2 SA-TEK-Request message.

EAPStart Timeout: Timeout period between sending PKMv2 EAP Start messages from Authenticated state.

Authorization Grace Time: Amount of time before the AK is scheduled to expire in order that the MS may start re-authentication before the authentication expiry.

7.2.2.5.5 Actions

1-A: Stopped (Start Auth)→ Not Authenticated
a) Enable PKMv2 EAP-Transfer messages to be transferred.

1-F: Reentry Authentication Wait (Start Auth)→ Not Authenticated
a) Stop TEK FSMs
b) Re-initialize the Authorization FSM
c) Enable PKMv2 EAP-Transfer messages to be transferred.

2-B: Not Authenticated (PKMv2 SA-TEK-Challenge)→SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message.
b) Start SATEK Timer.

2-C: SA-TEK-Response Wait (PKMv2 SA-TEK-Challenge)→SA-TEK-R*esponse* Wait
a) Send a PKMv2 SA-TEK-Request message.
b) Start SATEK Timer.

2-D: Authenticated (PKMv2 SA-TEK-Challenge)→Reauth SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message.
b) Start SATEK Timer.

2-E: Reauth SA-TEK-Response Wait (PKMv2 SA-TEK-Challenge)→Reauth SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message.
b) Start SATEK Timer.

3-C: SA-TEK-Response Wait (PKMv2 SA-TEK-Response)→Authenticated
a) Stop SATEK Timer
b) Start TEK FSMs
c) Start Authorization Grace Timer

3-E: Reauth SA-TEK-Response Wait (PKMv2 SA-TEK-Response)→Authenticated
a) Stop SATEK Timer
b) Start Authorization Grace Timer
c) Set the frame number for old AK context to be invalid.

3-G: Reentry SA-TEK-Response Wait (PKMv2 SA-TEK-Response)→Authenticated
a) Stop SATEK Timer
b) Start Authorization Grace Timer
d) Update the AK context for the target BS

4-B: Not Authenticated (EAP Success)→Not Authenticated
a) Obtain the MSK
b) Derive the keys derived from the PMK

4-D: Authenticated (EAP Success)→Authenticated

a) Obtain the new MSK
b) Derive the keys derived from the PMK

5-C: SA-TEK-Response Wait (SATEK Timeout)→ SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message
b) Start SATEK Timer

5-E: Reauth SA-TEK-Response Wait (SATEK Timeout)→ Reauth SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message
b) Start SATEK Timer

5-G: Reentry SA-TEK-Response Wait (SATEK Timeout)→ Reentry SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message
b) Start SATEK Timer

6-C: SA-TEK-Response Wait (SATEK request max resend elapsed)→ Stopped
a) Stop the Authorization FSM

6-E: Reauth SA-TEK-Response Wait (SATEK request max resend elapsed)→ Stopped
a) Stop TEK FSMs
b) Stop the Authorization FSM

6-G: Reentry SA-TEK-Response Wait (SATEK request max resend elapsed)→ Stopped
a) Stop TEK FSMs
b) Stop the Authorization FSM

7-D: Authenticated (Re-authentication Needed)→Authenticated
a) Send a PKMv2 EAP-Start message
b) Start EAPStart Timer

8-D: Authenticated (Start Reentry)→Reentry Authentication Wait
a) Generate the AK context for the target BS

8-E: Reauth SA-TEK-Response Wait (Start Reentry)→ Reentry Authentication Wait
a) Remove the new AK context for the serving BS generated during performing EAP-based re-authentication procedure
b) Generate the AK contexts for the target BS generated from old PMK context and new PMK context

9-D: Authenticated (EAPStart Timeout)→Authenticated
a) Send a PKMv2 EAP-Start message
b) Start EAPStart Timer

10-F: Reentry Authentication Wait (Handshake Started)→ Reentry SA-TEK-Response Wait
a) Send a PKMv2 SA-TEK-Request message

b) Start SATEK Timer

11-F: Reentry Authentication Wait (HO Canceled)→ Authenticated
a) Remove the AK context for the target BS
b) Retrieve the cached AK context for the serving BS

11-G: Reentry SA-TEK-Response Wait (HO Canceled)→ Authenticated
a) Remove the AK context for the target BS
b) Retrieve the cached AK context for the serving BS

12-F: Reentry Authentication Wait (TBS changed)→ Reentry Authentication Wait
a) Generate the AK context of new target BS

12-G: Reentry SA-TEK-Response Wait (TBS changed)→ Reentry Authentication Wait
a) Generate the AK context of new target BS

13-F: Reentry Authentication Wait (Reentry Completed)→ Authenticated
a) Update the AK context for the target BS

14-D,E,F,G: Any state except Stopped, SA-TEK-Response Wait and Not Authenticated (Authentication Expired)→Stopped
a) Stop TEK FSMs
b) Stop the Authorization FSM

15-B: Not Authenticated (EAP Faiure)→Stopped
a) Stop the Authorization FSM

15-D: Authenticated (EAP Faiure)→Stopped
a) Stop TEK FSMs
b) Stop the Authorization FSM

16-B,C: Not Authenticated and SA-TEK-Response Wait (External Stop)→Stopped
a) Stop the Authorization FSM

16-D,E,F,G: Any state except Stopped, Not Authenticated, and SA-TEK-Response Wait (External Stop)→Stopped
a) Stop TEK FSMs
b) Stop Authorization Grace Timer
c) Stop the Authorization FSM

[In section 6.3.22.2.7, perform the indicated change to page 151 of P80216-Cor2_D1]

When, during capabilities negotiation, MS specifies that it supports IEEE 802.16 security, if the normal PKM initial network entry process as defined in 7.2 is to be abridged or omitted, then the MS shall include the HMAC/CMAC Tuple as the last message item in the RNG-REQ management message using the Authorization Key and Key Sequence Number derived for use on the target BS. If the required HMAC/CMAC Tuple is invalid or omitted in the RNG-REQ management message, then the full PKM REQ/RSP sequence must be completed and cannot be omitted. The target BS shall include a valid HMAC/CMAC Tuple as the last message item in the RNG-RSP if it instructs the MS, through the HO Process Optimization TLV, that the PKM-REQ/RSP sequence may be omitted. If the HO Process Optimization TLV Bit #1 included in the RNG-RSP is set to 0, HMAC/CMAC Tuple is not attached to the RNG-RSP message.

[In section 7.8.1, perform the indicated change to page 196 of P80216-Cor2_D2]

The PKMv2 SA-TEK 3-way handshake sequence proceeds as follows:
1) During initial network entry or reauthorization, the BS shall send PKMv2 SA-TEK-Challenge (including a random number BS_Random) to the SS after protecting it with the HMAC/CMAC Tuple. If the BS does not receive PKMv2 SA-TEK-Request from the SS within SAChallenge-Timer, it shall resend the previous PKMv2 SA-TEK-Challenge up to SAChallengeMaxResends times. If th~~Bit #~~e BS reaches its maximum number of resends, it shall~~:~~ initiate another full authentication or drop the SS. If SS had been in the midst of an EAP exchange and had been awaiting notification of completion of the exchange through PKMv2 EAP Transfer with EAP-Success, or PKMv2 Authenticated EAP Transfer with EAP-Success, and the SS instead receives SA-TEK-Challenge signed with a CMAC derived from the new key material then the SS shall first treat the SA-TEK-Challenge as receipt of PKMv2 EAP Transfer with EAP-Success, or PKMv2 Authenticated EAP Transfer with EAP-Success, and then the SS shall process the SA-TEK-Challenge as if it had received the message after normally receiving the preceding PKMv2 EAP Transfer with EAP-Success, or PKMv2 Authenticated EAP Transfer with EAP-Success.
~~in case of initial entry - initiate another full authentication or drop the SS;~~
~~in case of BS initiated re-authentication - initiate another full re-authentication;~~
~~in case of MS initiated re-authentication - ignore and continue using current authentication.~~
2) If HO Process Optimization Bit #1 is set to 1 indicating that PKM Authentication phase is omitted and HO Process Optimization Bit #2 is set to 0 during network re-entry or handover, the BS updates TEKs either by beginning the 3-way-handshake, by including the SA Challenge Tuple TLV to the RNG-RSP or by appending the SA-TEK-Update TLV to RNG-RSP message. In case the BS begins 3-wayhandsake, if the BS does not receive PKMv2 SA-TEK-Request from the MS within SaChallengeTimer, it may initiate full re-authentication or drop the MS. If the BS receives an initial RNG-REQ during the period that PKMv2 SA-TEKRequest is expected, it shall send a new RNG-RSP with another SA-Challenge Tuple TLV.

3) The SS shall send PKMv2 SA-TEK-Request to the BS after protecting it with the HMAC/CMAC. If the SS does not receive PKMv2 SA-TEK-Response from the BS within SATEKTimer, it shall resend the request. The SS may resend the PKMv2 SA-TEK-Request up to SATEKRequestMaxResends times. If the SS reaches its maximum number of resends, it shall~~:~~
~~in case of initial entry -~~ initiate another full authentication or attempt to connect to another BS.~~;~~
~~in case of BS initiated re-authentication - ignore and continue using current authentication;~~
~~in case of MS initiated re-authentication ñ initiate another full re-authentication.~~
The SS shall include, through the Security Negotiation Parameters attribute, the security capabilities that it included in the SBC-REQ message during the basic capabilities negotiation phase.

[In section10.2, remove the row from Table343, the page 355 of P80216-Cor2_D2]

System	*Name*	*Description*	*Min*	*Default*	*max*
~~MS~~	~~PN grace value~~	~~The value of CMAC PN counter that triggers re-authentication~~	~~0x7FFFFFFF~~	~~0xFF000000~~	~~0xFF000000~~

[In section10.2 perform the indicated change to the page 354, Table343 of P80216-Cor2_D2]

System	*Name*	*Description*	*Min*	*Default*	*max*
BS	SaChallenge-MaxResends	Maximum number of transmissions of SA-TEK-Challenge.	1	3	~~3~~
MS	SATEKRequest-MaxResends	Maximum number of transmissions of SA-TEK-Request.	1	3	~~3~~