



WiMAX Forum[®] Air Interface Specification

WiMAX Forum[®] Mobile Standard Reference

WMF-T23-004-R010v03

WMF Approved

(2011-07-14)

WiMAX Forum Proprietary

Copyright © 2011 WiMAX Forum. All Rights Reserved.

1 **Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability**

2
3 Copyright 2011 WiMAX Forum. All rights reserved.

4
5 The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for
6 download from the WiMAX Forum and may be duplicated for internal use, provided that all copies contain all proprietary notices
7 and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or
8 distributed without the express written authorization of the WiMAX Forum.

9
10 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance
11 of the following terms and conditions:
12

13 **THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST**
14 **EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND**
15 **STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE,**
16 **NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX**
17 **FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND**
18 **DISCLAIMS ANY WARRANTIES TO THE CONTRARY.**

19
20 Any products or services provided using technology described in or implemented in connection with this document may be
21 subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely
22 responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all
23 required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable
24 jurisdiction.
25

26 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**
27 **APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY**
28 **OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.**

29
30 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**
31 **SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY**
32 **CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.**

33
34 The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any
35 technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any
36 technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual
37 property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology,
38 standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies,
39 technologies, standards, and specifications, including through the payment of any required license fees.
40

41 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH**
42 **RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED**
43 **INTO THIS DOCUMENT.**

44
45 **IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD**
46 **PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING,**
47 **WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL**
48 **PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY**
49 **USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS**
50 **MEMBERS RELATING TO THE USE OF THIS DOCUMENT.**

51
52 The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is
53 solely responsible for determining whether this document has been superseded by a later version or a different document.
54

55 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the
56 WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks of the WiMAX Forum. All
57 other trademarks are the property of their respective owners.

58

Table of Contents

1.	INTRODUCTION.....	2
1.1	Scope.....	2
2.	STANDARD REFERENCE.....	3

1. Introduction

WiMAX Forum® Mobile conformance and interoperability specifications for Release 1.0 air interface (PCT, RCT and MIOT aspects only) is based on the IEEE 802.16 standard. This document specifies the exact standard references that are the basis for the conformance and interoperability specifications.

1.1 Scope

The purpose of this document is to specify relevant IEEE 802.16 standard(s) documents that are the references for the WiMAX Forum Mobile conformance and interoperability specifications for Release 1.0 air interface (PCT, RCT and MIOT aspects only).

2. Standard Reference

The following is the standard reference used by WiMAX Forum® in air interface certification testing:

IEEE Std 802.16™-2004 as amended and corrected by
 IEEE Std 802.16e™-2005
 IEEE Std 802.16™-2004/Cor1-2005
 IEEE P802.16-2004/Cor2/D3

Within the context of this document, the above references are referred to as the Certification Baseline.

The following changes are applicable as exceptions to the above standard references.

Standard Reference Exception 1. Include the following specification of the MS Transmit Power Limitation Level TLV from **IEEE Std 802.16-2009** Table 571.

Table 540—UCD PHY-specific channel encodings—WirelessMAN-OFDMA (continued)

Name	Type (1 byte)	Length	Value
<u>MS Transmit Power Limitation Level</u>	<u>214</u>	<u>1</u>	<u>Unsigned 8-bit integer. Specifies the maximum allowed MS transmit power. Values indicate power levels in 1 dB steps starting from 0 dBm.</u>

Standard Reference Exception 2. Include specifications related to ND&S functionality from the following sections of **IEEE Std 802.16-2009**: **11.1.10.1-2**, 11.8.9, 11.8.11, 11.8.13, 11.8.14, 6.3.2.3.58.

IEEE Std 802.16-2009: In Section 11.4.1, only NSP Change Count TLV (at the top of page 1187).

IEEE Std 802.16-2009: (6.3.2.3.23, “SBC-REQ (SS basic capability request) message”, page 131, from “The Basic Capabilities Request ...” to “Visited NSP ID (see 11.8.11).

IEEE Std 802.16-2009: (6.3.2.3.24, “SBC-RSP (SS basic capability response) message”, page 132, from “NSP information is solicited ...” to page 133, “... Security Negotiation Parameters (see 11.8.4)”, page 133, from “If NSP information is not solicited...” to “... with a list of Verbose NSP names”, and page 133, from “If the Visited NSP ID TLV is found...” to “Visited NSP Realm (see 11.8.13)”.

Standard Reference Exception 3. As modified in **P802.16-2004/Cor2/D4**, in Table 283 of **P802.16-2004/Cor2/D3** change the size of “Reserved” from “1 bit” to “2 bits” (comment #1028, database **IEEE 802.16-07/029r4**).

Standard Reference Exception 4. For Bit 6 of the HO Process Optimization TLV in the RNG-RSP use the definition of **IEEE Std 802.16-2009** in Table 585 on p. 1202.

Standard Reference Exception 5. As modified in **P802.16-2004/Cor2/D4**, make the following changes in **P802.16-2004/Cor2/D3** (comment #1054, database **IEEE 802.16-07/029r4**, contribution **C802.16maint-07/037**).

[In section 6.3.22.2.8.1.6.6, perform the indicated change to page 171 of P80216-Cor2_D3]

MS context with Serving BS: Maintained with resource retain timer.

MS context with Target BS: Context is handled per bit#1 and bit#2 settings.

Bit #1=0 AND bit#2=0: Perform re-authentication and SA-TEK 3-way handshake. BS ~~should~~ **shall not** include SA-TEK-Update TLV in the SA-TEK-Response message. In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV.

Bit #1=0 AND bit#2=1: Not used. MS shall silently ignore RNG-RSP message.

[In section 6.3.22.2.8.1.6.6, perform the indicated change to page 172 of P80216-Cor2_D3]

SAID update:

When **re-authentication is not required and** SAID_update TLV is excluded from the RNG-RSP message during network re-entry, it means that SAID value(s) will be the same value(s) as the value(s) used in previous serving BS and the value of Primary SAID will be implicitly updated because MS and BS use the same value as that of Basic CID.

[In section 11.6, perform the indicated change to Table 367, page 405 of P80216-Cor2_D3]

Name	Type (1 byte)	Length	Value	PHY Scope
HO Process Optimization	21	2	... (Bit #1, Bit #2) = (0, 0): Perform re-authentication and SA-TEK 3-way handshake. BS should shall not include SA-TEK-Update TLV in the SA-TEK-Response message. In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV. ...	All

[In section 6.3.2.3.9.20, perform the indicated change to Table 37j, page 34 of P80216-Cor2_D2]

(one or more) SA-Descriptor(s)	Each compound SA-Descriptor attribute specifies an SA identifier (SAID) and additional properties of the SA. This attribute is present at the initial network entry or reentry after receipt of a RNG-RSP message with HO Process .
--------------------------------	--

3

Optimization bits (Bit#1, Bit#2)=(0, 0) only .

Standard Reference Exception 6. As modified in P802.16-2004/Cor2/D4, make the following changes in P802.16-2004/Cor2/D3 (comment #1060LL, database IEEE 802.16-07/029r4, contribution C802.16maint-07/038).

Carry out the approved change in the lay-out of SA-TEK Update TLV and apply it to TLV 142 section 11.1.10. Change unnumbered table in 11.1.10 shown below as indicated below the figure:

Name	Type	Length (byte)	Value
<u>SA-TEK-Update-Type</u>	<u>142.1</u>	1	1: TEK parameters for an SA 2: GTEK parameters for a GSA 3-255: Reserved
<u>New SAID</u>	<u>142.2</u>	2	<u>New SAID after handover to new BS</u>
<u>Old SAID</u>	<u>142.3</u>	2	<u>Old SAID before handover from old BS</u>
<u>Old TEK/GTEK-Parameters</u>	<u>142.4</u>	variable	<u>“Older” generation of key parameters relevant to (G)SAID. The compound fields contains the sub-attributes as defined in Table 372.</u>
<u>New TEK/GTEK-Parameters</u>	<u>142.5</u>	variable	<u>“Newer” generation of key parameters relevant to (G)SAID. The compound fields contains the sub-attributes as defined in Table 372.</u>
<u>GKEK-Parameters</u>	<u>142.6</u>	variable	<u>GKEK, its lifetime, and its sequence number for the corresponding GSAID.</u>

Strike out item 142.3

Old SAID	142.3	2	Old SAID before handover from old BS
---------------------	------------------	--------------	---

**Change the 3rd paragraph of 11.1.10 as indicated:
 Text in D3:**

Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK, and GKEK parameters are also included. Thus, SA_TEK_Update provides a shorthand method for renewing active SAs used by the MS in its previous serving BS. The TLVs specify SAID in the target BS that shall replace active SAID used in the previous serving BS and also “older” TEK-Parameters and “newer” TEK Parameters relevant to the active SAIDs. The update may also include multicast/broadcast Group SAIDs (GSAIDs) and associated GTEK-Parameter pairs.

Change to:

Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK, and GKEK parameters are also included. Thus, SA_TEK_Update provides a shorthand ~~method~~ **method** for renewing active SAs used by the MS in its previous serving BS. The TLVs specify SAID in the target BS that shall replace active SAID used in the previous serving BS and also “older” TEK-Parameters and “newer” TEK Parameters relevant to the active SAIDs. The update may also include multicast/broadcast Group SAIDs (GSAIDs) and associated GTEK-Parameter pairs. **The New SAID field shall refer to SAID assignments by the new BS. The mapping of these new SAIDs to the SAIDs assigned by the previous serving BS is controlled by the SAID Update TLV (11.7.18) and is further controlled by the rules for SAID updating outlined in section 6.3.22.2.8.1.6.6.**

Standard Reference Exception 7. Instead of the relevant text in the Certification Baseline, use the text beginning at the fourth paragraph of Section 8.4.10.3 on p. 1070 of IEEE Std 802.16-2009 (starting with “To maintain...”) and ending just above Table 514 on p. 1071, plus the text of the first line of p. 1072.

Standard Reference Exception 8. In addition to the Certification Baseline requirements, use the text beginning at the last paragraph of p. 1081 of **IEEE Std 802.16-2009** (starting with “ When the...” and ending after the first paragraph of p. 1082 (ending with “...STC zone.”).

Standard Reference Exception 9. In addition to the Certification Baseline requirements, use the text beginning at the last paragraph of p. 435 of **IEEE Std 802.16-2009** (starting with “ The MS shall...” and ending after the first paragraph of p. 436 (ending with “...are received.”).

Standard Reference Exception 10. In addition to the Certification Baseline requirements, use the text in **IEEE Std 802.16-2009**, Clause 10.1, Table 554, p. 1147 entry for N_ms_max_neighbors.

Standard Reference Exception 11. Add the following
IEEE P802.16-Rev2/D8, paragraph 8.4.5.3.21, page 771, line 24
IEEE P802.16-Rev2/D8, paragraph 8.4.5.4.22, page 867, line 27
IEEE P802.16-Rev2/D8, paragraph 11.8.3.5.13, page 1248, lines 1-10 excluding the specification on Persistent HARQ DL/UL MAP IE (or, “or Persistent HARQ UL MAP IE” in line 6 and “or Persistent HARQ DL MAP IE” in line 7)
IEEE P802.16-Rev2/D8, paragraph 11.13.30, from page 1323, line 58 to page 1324, line 6

Standard Reference Exception 12. Add the following
IEEE P802.16-Rev2/D8, paragraph 6.3.2.3.54, page 260, line 58-60
IEEE P802.16-Rev2/D8, paragraph 8.4.10.3, page 1085, line 7-10
IEEE P802.16-Rev2/D8, paragraph 8.4.10.3.2.1, page 1088, line 29-30
IEEE P802.16-Rev2/D8, paragraph 8.4.10.3.2.2, page 1089, line 42-44

Standard Reference Exception 13. Add **IEEE P802.16-Rev2/D8**, paragraph 6.3.6.1, page 301, lines 36-38 and lines 46-48 (that is, removing the last two sentences in **IEEE P802.16 Cor2/D3**, paragraph 6.3.6.1, page 115, lines 1-4)

Standard Reference Exception 14. Add **IEEE P802.16-Rev2/D8**, last sentence from subclause 6.3.5.2.2 (from line 63, page 299, till line 3, page 300), and whole Table 197 (Page 431, lines 8-26) (that is, specifying mandatory usage of the Unsolicited Polling Interval for any UL RT-VR service flow)

Standard Reference Exception 15. Add **IEEE P802.16-Rev2/D9**, Section 8.4.6.2.7.1, page 977, lines 55-65 and page 978 lines 1-15.

Standard Reference Exception 16. As modified in **IEEE P802.16-Rev2/D9**, make the following changes in **P802.16-2004/Cor2/D3**

Add **IEEE P802.16-Rev2/D9**, the section 11.6, Table 584, page 1216, line 10-26.
Add **IEEE P802.16-Rev2/D9**, the section 11.8.3.2, page 1236, line 42-50.

Standard Reference Exception 17. Corrections to DSD and DSC state diagrams,
Replace Figure 102 in **IEEE Std 802.16-2004** with Figure 114 from **P802.16 Rev2/D9**
Replace Figure 105 in **IEEE Std 802.16-2004** with Figure 117 from **P802.16 Rev2/D9**
Replace Figure 117 in **IEEE Std 802.16-2004** with Figure 128 from **P802.16 Rev2/D9**
Replace Figure 128 in **IEEE Std 802.16-2004** with Figure 139 from **P802.16 Rev2/D9**
Substitute the entry for T10 in **IEEE Std 802.16-2004**, Table 342 (Parameters and Constants) with the corresponding entry in **P802.16 Rev2/D9**, Table 553.

Standard Reference Exception 18. Replace contents of Section “6.3.2.3.47 Neighbor Advertisement (MOB_NBR-ADV) message” Page 63 Lines 33-38 in **IEEE P802.16 Cor2/D3** by the following changes to table 144 in P802.16 section Rev/D9 6.3.2.3.42, page 198: (contribution IEEE C802.16maint-09/0015):

Syntax	Size (bit)	Notes
MOB_NBR_ADV_Message_format(){	—	—
Management Message Type = 53	—	—
Reuse factor for SBS CINR calculation for scan and handover	2	<p>00 - Physical SBS CINR for scan or handover triggers shall be calculated according to the number of subcarriers indicated in the DL Frame Prefix "Used subchannel bitmap" field. If the number of used subcarriers is lower than or equal to one third of the total number of subcarriers, then CINR shall be computed according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 3. Otherwise the CINR shall be computed according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 1</p> <p>10 – Physical SBS CINR for scan or handover triggers shall be calculated according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 1</p> <p>01 – Physical SBS CINR for scan or handover triggers shall be calculated according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 3</p> <p>11 – reserved</p>
Skip-optional-fields bitmap	6	<p>Bit [0]: if set to 1, omit Operator ID field.</p> <p>Bit [1]: if set to 1, omit NBR</p>

		<p>BS ID field.</p> <p>Bit [2]: if set to 1, omit HO process optimization field.</p> <p>Bit [3]: if set to 1, omit QoS related fields.</p> <p>Bit [4]–[5]: <i>Reserved.</i></p>
<p>Reuse factor for SBS CINR calculation for scan and handover</p>	<p>2</p>	<p>00—Physical SBS CINR for scan or handover triggers shall be calculated according to the number of subcarriers indicated in the DL Frame Prefix "Used subchannel bitmap" field. If the number of used subcarriers is lower than or equal to one third of the total number of subcarriers, then CINR shall be computed according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 3. Otherwise the CINR shall be computed according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 1</p> <p>10—Physical SBS CINR for scan or handover triggers shall be calculated according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 1</p> <p>01—Physical SBS CINR for scan or handover triggers shall be calculated according to the rule detailed in 8.4.12.3 for frequency reuse configuration = 3</p> <p>11—reserved</p>

Add page 1110 second paragraph of section 8.4.12.3 “CINR mean and standard deviation” of **IEEE P802.16-2009** to **IEEE P802.16 Cor2/D3**.

Standard Reference Exception 19. Add IEEE P802.16-Rev2/D8, section 8.4.5.4.11, Table 392, page 852, line 24-28.

Standard Reference Exception 20. Replace description of UCD TLVs 210, 211, 212 and 213 (Fast Feedback region, HARQ ACK region, Ranging Region, Sounding Region) in Table 353—UCD PHY-specific channel encodings—WirelessMAN-OFDMA of IEEE P802.16 Cor2/D3 with the description of UCD TLVs 210, 211, 212, 213(Fast Feedback region, HARQ ACK Region, Ranging Region, Sounding Region) in Table 570—UCD PHY-specific channel encodings—WirelessMAN-OFDMA of P802.16Rev2/D9.

Standard Reference Exception 21. Add IEEE P802.16-Rev2/D9, page 991, line 50-55.

Standard Reference Exception 22. As modified in P802.16 Rev2/D9, make the following changes in P802.16-2004/Cor2/D3 (session #57, contribution C80216maint-08_263r3.doc).

[In section 6.3.2.3.6, remove SA Challenge Tuple TLV encoding from RNG-RSP at page 30 of P802.16-2004/Cor2/D3]

The following TLV may be present in RNG-RSP (see 7.8.1, 11.6.1)

~~PKMv2 SA-TEK SA-Challenge Tuple~~

This carries the initial challenge of the 3-way handshake.

[In section 6.3.2.3.9.19, remove SA Challenge Tuple TLV mentioning from SA-TEK-Request at Table 37i of P802.16-2004/Cor2/D3]

Attribute	Contents
MS_Random	A 64-bit number chosen by the MS freshly for every new handshake ^a
BS_Random	The 64-bit random number used in the PKMv2 SA-TEK-Challenge message or SA-Challenge Tuple
Key Sequence Number	AK sequence number
....

^aReceipt of a new BS random value in SA-TEK-Challenge ~~or SA-Challenge tuple~~ indicates the beginning of a new handshake.

[In section 6.3.2.3.9.20, remove SA Challenge Tuple TLV mentioning from SA-TEK-Response description at Table 37j of P802.16-2004/Cor2/D3]

Attribute	Contents
MS_Random	The number received from the MS.
BS_Random	The 64-bit random number used in the PKMv2 SA-TEK-Challenge message or SA-Challenge Tuple
...	...

[In section 6.3.22.2.8.1.6.6, remove Option 2 and modify the description from page 171 to 172 of P802.16-2004/Cor2/D3 as follows]

6.3.22.2.8.1.6.6 Security settings

MS context with Serving BS: Maintained with resource retain timer.

MS context with Target BS: Context is handled per bit#1 and bit#2 settings.

Bit #1=0 AND bit#2=0:Perform re-authentication and SA-TEK 3-way handshake

In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV.

Bit #1=0 AND bit#2=1:Not used. MS shall silently ignore RNG-RSP message.

Bit #1=1 AND bit#2=0: ~~One of two options is allowed:~~

~~Option 1: SA-TEK-Update TLV is included in the RNG-RSP message and updates the TEKS for all the SAs. In this way SA TEK 3-way handshake shall not occur. SA Challenge Tuple TLV shall not be included in the RNG-RSP message.~~

~~Option 2: SA TEK Update TLV is included in a SA TEK Response message. In this case, SATEK 3-way handshake is performed with SA Challenge Tuple TLV included in the RNG-RSP message.~~

Bit #1=1 AND bit#2=1:Re-authentication ~~and SA TEK 3-way handshake~~ is not performed. The RNG-RSP message does not include SA-TEK-Update TLV ~~nor SA Challenge Tuple TLV.~~

[In section 6.3.24.9, delete the paragraph regarding SA Challenge Tuple TLV from line#13~#18, page 184 of P802.16-2004/Cor2/D3]

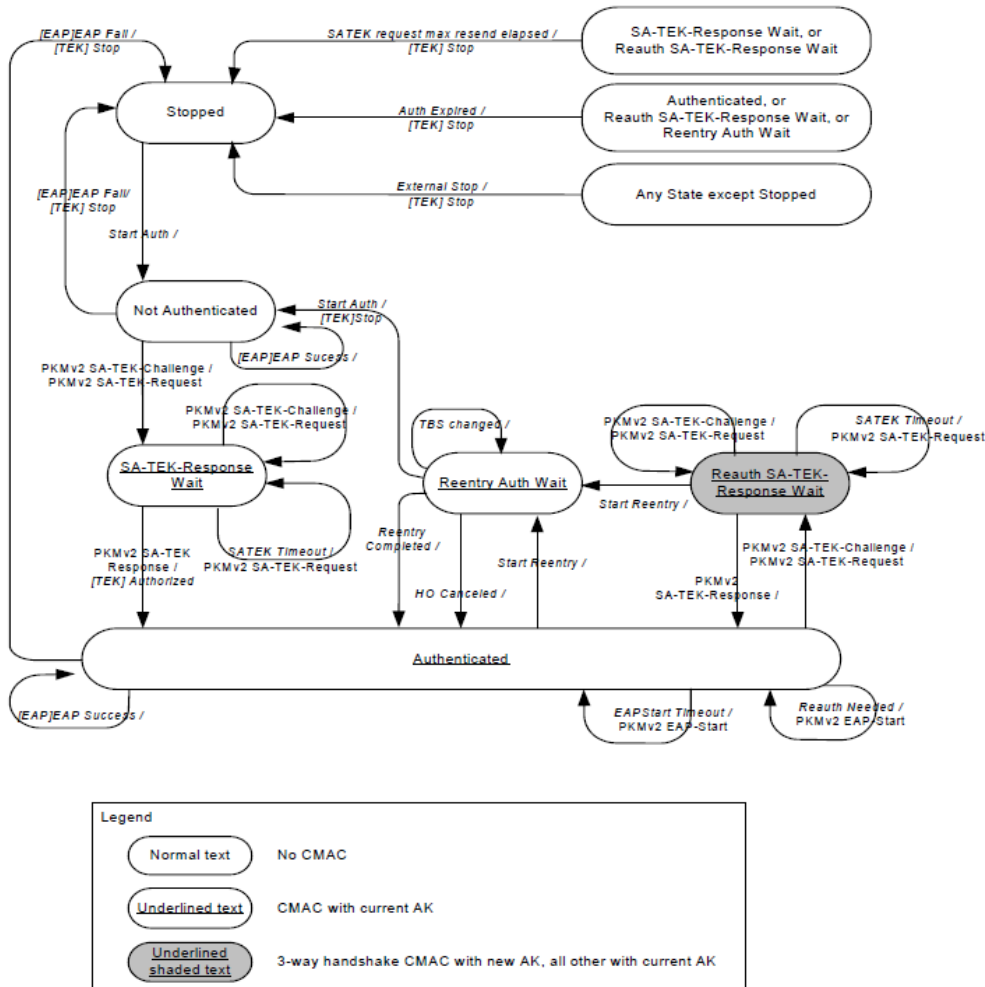
~~For a security keying process that has not been determined to be omitted in the HO Process Optimization TLV settings, if MS RNG-REQ includes Ranging Purpose Indication TLV with Bit #0 set to 1 and Paging Controller ID TLVs, and target BS has keying material for the MS, the MS and target BS shall may use the RNG-RSP including the SA Challenge Tuple information TLV to initiate the 3-way handshake reauthorization process as defined in 7.8.1.~~

[In section 11.6, remove Option B from HO Process Optimization TLV encoding of RNG-RSP at table 367 of P802.16-2004/Cor2/D3]

Name	Type (1 byte)	Length	Value (variable-length)	PHY scope
...
HO Process Optimization	21	2	<p>...</p> <p><u>(Bit #1, Bit #2) = (0,0): Perform re-authentication and SA-TEK 3-way handshake.</u></p> <p><u>In addition, the RNG-RSP message does not include SA-TEK-Update TLV or SA Challenge Tuple TLV.</u></p> <p><u>(Bit #1, Bit #2) = (0,1): Reserved.</u></p> <p><u>(Bit #1, Bit #2) = (1,0): In this case, option A is recommended.</u></p> <p><u>Option A) SA-TEK-Update TLV is included in the RNG-RSP message. In this case, SA-TEK 3-way handshake is avoided and SA Challenge Tuple TLV shall not be included in the RNG-RSP message.</u></p> <p><u>Option B) SA TEK Update TLV is included in a SATEK-Response message. In this case, SA-TEK 3-way handshake is performed with SA Challenge Tuple TLV included in the RNG-RSP message.</u></p> <p><u>(Bit #1, Bit #2) = (1, 1): Re-authentication and SA-TEK 3-way handshake is not performed. The RNG-RSP message does not include SA-TEK-Update TLV nor SA Challenge Tuple TLV.</u></p> <p><u>All the TEKS received from the serving BS are reused</u></p> <p>...</p>	All
...

[For the section 7.2.2.5 Authorization State Machine, from page 195 to 204 of **P802.16-2004/Cor2/D3** refer to the section 7.2.2.5 Authentication State Machine of **P802.16 Rev2/D9**.]

[Replace the Figure 130s of **P802.16-2004/Cor2/D3** with the following Figure 164 of **P802.16 Rev2/D9**.]



[Adopt the changes in the Table 133e of **P802.16-2004/Cor2/D3** as follows.]

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	
(10) HO Canceled						Authenticated	Authenticated
(11) TBS Changed						Reentry Auth Wait	Reentry Auth Wait
(12) Reentry Completed						Authenticated	
(13) Auth Expired				Stopped	Stopped	Stopped	Stopped
(14) EAP Fail		Stopped		Stopped			
(15) External Stop		Stopped	Stopped	Stopped	Stopped	Stopped	Stopped

[In section 7.2.2.5.1, delete sentences regarding SA Challenge Tuple TLV from line#55~#65, page 199 of P802.16-2004/Cor2/D3.]

~~In the case HO Process Optimization Bit #1 and Bit #2 set to one and zero respectively and the SAChallenge Tuple TLV is included in the RNG-RSP, the next state is Reentry SATEKResponseWait.~~

~~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.~~

[In section 7.2.2.5.3, delete sentence regarding SA Challenge Tuple TLV from line#61~#65, page 200 of P802.16-2004/Cor2/D3.]

~~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 re-entry.~~

[Adopt the changes in the section 7.2.2.5.5 of P802.16-2004/Cor2/D3 as follows.]

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-Response 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~~

~~10-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~~

~~11-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

123-F: Reentry Authentication Wait (Reentry Completed) -> Authenticated

a) Update the AK context for the target BS

134-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

145-B: Not Authenticated (EAP Failure) -> Stopped

a) Stop the Authorization FSM

145-D: Authenticated (EAP Failure) -> Stopped

a) Stop TEK FSMs

b) Stop the Authorization FSM

156-B,C: Not Authenticated and SA-TEK-Response Wait (External Stop) -> Stopped

a) Stop the Authorization FSM

156-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 7.8.1, delete sentences regarding SA Challenge Tuple TLV from line62, page 215 to line8, page 216 of **P802.16-2004/Cor2/D3** as follows]

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 begins updates TEKs either by beginning the 3-way handshake, by appending 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-way handshake, If if the BS does not receive PKMv2 SA-TEK-Request from the MS within SaChallengeTimer (suggested to be several times greater than the length of 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-TEK-Request is expected, it shall send a new RNG-RSP with another SaChallenge SA-Challenge-Tuple TLV.~~

[In section 11.6.1, delete the section 11.6.1 regarding SA Challenge Tuple TLV from page 683 to 684 of **IEEE Std 802.16e™-2005**]

11.6.1 SA Challenge Tuple

~~This compound TLV enables the BS to abbreviate the 3-way handshake during handover by appending the initial challenge to the RNG-RSP message.~~

Name	Type	Length	Value	Scope
SA-Challenge	31	Variable	Compound	RNG-RSP

The following TLV values shall appear in each SA-Challenge-TLV:

Name	Type	Length	Value
BS-Random	31.1	8bytes	-
AKId	31.2	8bytes	-

Standard Reference Exception 23. As modified in IEEE 802.16-2009, in page 855, subclause 8.4.5.4.22, use the fourth paragraph starting with “When Allocation Start Indication is 1, ...”.

Note: This change supersedes the amended language found in IEEE 802.16e-2005.

Standard Reference Exception 24. Instead of the text of Subsection 8.4.10.3.2.1 of the Certification Baseline, use the text of Subsection 8.4.10.3.2.1 of IEEE Std 802.16-2009.

Standard Reference Exception 25. As modified in ‘Annex A.2’ of L80216-09_0070.doc, make the following changes in IEEE Std 802.16-2009.

Modifying the section 6.3.5.2.2.1, page 294, in IEEE Std 802.16-2009 as follows

6.3.5.2.2.1 Extended rtPS

Extended rtPS is a scheduling mechanism which builds on the efficiency of both UGS and rtPS. The BS shall provide unicast grants in an unsolicited manner like in UGS, thus saving the latency of a BR. However, whereas UGS allocations are fixed in size, ertPS allocations are dynamic.

The BS may provide periodic UL allocations that may be used for requesting the bandwidth as well as for data transfer. By default, size of allocations corresponds to current value of Maximum Sustained Traffic Rate at the connection. The MS may request the BS to change ~~changing~~ the size of the UL allocation by indicating the desired UL allocation size ~~either by~~ using an Extended Piggyback Request field of the GMSH or the BR field of the MAC signaling headers as described in Table 7 or by sending a codeword (defined in 8.4.11.13) over CQICH. ~~The BS shall not change the size of UL allocations until receiving another bandwidth change request from the MS.~~ When the BR size is set to zero, the BS may provide allocations for only BR header or no allocations at all. In case that no unicast BR opportunities are available, the MS may use contention request opportunities for that connection, or send the CQICH codeword to inform the BS of its having the data to send. If the BS receives the CQICH codeword, the BS shall start allocating the UL grant corresponding to the current Maximum Sustained Traffic Rate value.

The mandatory QoS parameters are the Maximum Sustained Traffic Rate, the Minimum Reserved Traffic Rate, the Maximum Latency, the Request/Transmission Policy and Unsolicited Grant Interval (11.13.19).

The Extended rtPS is designed to support real-time service flows that generate variable-size data packets on a periodic basis, such as Voice over IP services with silence suppression.

Standard Reference Exception 26.

- Instead of Table 96—Action codes and actions use the Table 96—Action codes and actions in IEEE L802.16-09/0058 Annex B.2.
- Change Table 109—DREG-REQ message format and its related text as shown in IEEE L802.16-09/0058 Annex B.2.
- Modify chapter 6.3.23.1 MS idle mode initiation as shown in IEEE L802.16-09/0058 Annex B.2.

- Add a new line to Table 554—Parameters and constants as shown in IEEE L802.16-09/0058 Annex B.2.
- Change section 11.7.8.11 – Extended Capability, as shown in IEEE L802.16-09/0058 Annex B.2.

Standard Reference Exception 27. Modify 11.8.3.5.18 OFDMA parameters sets as shown in IEEE L802.16-09/0070 Annex D.2.

Standard Reference Exception 28. Add sections 7.2.2.2.9.1, 7.2.2.2.9.1.1, 7.2.2.2.9.1.1.1, 7.2.2.2.9.1.2, and the following paragraph of 6.3.2.3.5 page 90 of IEEE P802.16-2009:

The following TLV shall be included whenever the CMAC tuple is included in the RNG-REQ message during re-entry, secure Location Update or handover.

CMAC_KEY_COUNT

This field contains the MSs current value of the CMAC_KEY_COUNT, which is used to generate the CMAC_KEY_U used to generate the CMAC Tuple included in this message. See 7.2.2.2.9.

Standard Reference Exception 29. Add the following IEEE Std 802.16-2009, 11.4.1, page 1187, Table 575:

BS classes are defined as specified in the “Value (variable length)” column.

Table 575—DCD channel encodings (continued)

Name	Type (1 byte)	Length	Value (variable length)	PHY scope
Cell Type TLV	57	1	Cell type TLV may be used by the MS in the network for cell selection and reselection. Cell Type is encoded as follows: Bits 0–3: Indicates class of BS a) if bits 0–3= 0000, Macro BS with GPS it is a class-0 BS b) if bits 0–3= 0001, CSG-open Femto [5] with GPS it is a class-1 BS c) if bits 0–3= 0010, CSG-closed Femto [5] with GPS it is a class-2 BS d) if bits 0–3= 0011, Open Femto [5] with GPS it is a class-3 BS e) if bits 0–3= 0100, CSG-open Femto with Network synchronization it is a class-4 BS f) if bits 0–3= 0101, CSG-closed Femto with Network synchronization it is a class-5 BS g) if bits 0–3= 0110, Open Femto/Indoor BS with Network synchronization it is a class-6 BS h) if bits 0–3= 0111, it is a class-7 BS i) if bits 0–3= 1000, it is a class-8 BS j) if bits 0–3= 1001, it is a class-9 BS k) if bits 0–3= 1010, it is a class-10 BS l) if bits 0–3= 1011, it is a class-11BS m) if bits 0–3= 1100, it is a class-12 BS n) if bits 0–3= 1101, it is a class-13BS o) if bits 0–3= 1110, it is a class-14 BS p) if bits 0–3= 1111, it is a class-15 BS Bits 4–7 of the cell Type are reserved.	All

Standard Reference Exception 30.

- Instead of reference to P802.16-2004/Cor2/D3, p398, table 358b, “Action” row, use reference to IEEE Std 802.16-2009 Table 577, “Action” row” (page 1191).

Standard Reference Exception 31.

As modified in IEEE 802.16-2009, subclause 11.6, Table 585—RNG-RSP message encodings, page 1203, add row item:

Table 585—RNG-RSP message encodings (continued)

Name	Type (1 byte)	Length	Value (variable length)	PHY scope
Preamble Index Override	39	Length is defined as: (Num of Preamble Index) × 1	Cell Preamble Indices of new target BS(s) where the MS should redo ranging. If this TLV is used, the Ranging Status value shall be set to 2. This TLV shall be used for licensed bands only.	All
Ranging Abort Timer	40	1	0–255: In units of seconds.	All

Standard Reference Exception 32. As modified in IEEE 802.16-2009, subclause 6.3.2.3.6, page 92, line #3~#10:

Preamble Index Override

Preamble Indices of new target BS(s) where the MS should redo ranging. If the TLV includes two or more Preamble Indices, the first one in the list is the most preferable and the second is the next preferable. When the TLV is used with Downlink frequency override TLV, the MS should redo ranging on the new DL channel identified by the Preamble Indices.

Ranging Abort Timer

Timer defined by a BS to prohibit the MS from attempting network entry at this BS, for a specific time duration.

Standard Reference Exception 33.

- Include specifications from the third and fourth paragraphs of Subsection 11.13.30 “HARQ Service Flows field” of IEEE P802.16-2009 (two last paragraphs at bottom of Page 1307) to Subsection 11.13.32 “HARQ Service Flows” of IEEE P802.16 Cor2/D3.

Standard Reference Exception 34.

- Add IEEE P802.16m-D10, page 23, line 34 - 47.