



9

10

# WiMAX Forum Server PKI Certificate Policy Draft Specification

Version 1.0.1

April 22<sup>nd</sup>, 2008

**WiMAX Forum Proprietary**

**Copyright © 2008 WiMAX Forum. All Rights Reserved.**

11 **Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability.**

12 Copyright 2007-2008 WiMAX Forum. All rights reserved.

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

17 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance  
18 of the following terms and conditions:

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

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

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

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

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

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

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

53 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the  
54 WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum. Third-party trademarks  
55 contained in this document are the property of their respective owners.

56 **TABLE OF CONTENTS**

57 **1. INTRODUCTION ..... 1**

58 1.1 OVERVIEW ..... 1

59 1.2 DOCUMENT NAME AND IDENTIFICATION..... 1

60 1.3 PKI PARTICIPANTS ..... 1

61 1.3.1 Policy Authority ..... 1

62 1.3.2 Certification Authorities ..... 1

63 1.3.3 Registration Authority (RA) ..... 3

64 1.3.4 Certificate Subjects ..... 3

65 1.3.5 Relying Parties ..... 3

66 1.3.6 OCSP Responders ..... 4

67 1.3.7 Other Participants ..... 4

68 1.4 CERTIFICATE USAGE ..... 4

69 1.5 POLICY ADMINISTRATION ..... 4

70 1.6 DEFINITIONS AND ACRONYMS ..... 5

71 **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES ..... 7**

72 2.1 REPOSITORIES ..... 7

73 2.2 PUBLICATION OF CERTIFICATION INFORMATION ..... 7

74 2.3 TIME OR FREQUENCY OF PUBLICATION ..... 7

75 2.4 ACCESS CONTROLS ON REPOSITORIES ..... 7

76 **3. IDENTIFICATION AND AUTHENTICATION ..... 8**

77 3.1 NAMING ..... 8

78 3.1.1 Types of Names ..... 8

79 3.1.2 Meaningfulness ..... 8

80 3.1.3 Anonymity or Pseudonymity of Certificate Subjects ..... 8

81 3.1.4 Rules for Interpreting Various Name Forms ..... 9

82 3.1.5 Uniqueness of Names ..... 9

83 3.1.6 Recognition, Authentication, and Role of Trademarks ..... 9

84 3.2 INITIAL IDENTITY VALIDATION ..... 9

85 3.2.1 Method to Prove Possession of Private Key ..... 9

86 3.2.2 Authentication of Organization Identity ..... 10

87 3.2.3 Authentication of Individual Identity ..... 10

88 3.2.4 Non-verified Certificate Subject Information ..... 10

89 3.2.5 Validation of Authority ..... 10

90 3.2.6 Criteria for Interoperation ..... 10

91 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS ..... 11

92 3.3.1 Identification and Authentication of Re-Key and Renewal Requests ..... 11

93 3.3.2 Identification and Authentication of Re-Key and Renewal After Revocation ..... 11

94 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST ..... 11

95 **4. CERTIFICATE LIFE-CYCLE ..... 12**

96 4.1 CERTIFICATE APPLICATION ..... 12

97 4.1.1 Who Can Submit a Certificate Application ..... 12

98 4.1.2 Enrollment Process and Responsibilities ..... 12

99 4.2 CERTIFICATE APPLICATION PROCESSING ..... 12

100 4.2.1 Performing Identification and Authentication Functions ..... 12

101 4.2.2 Approval or Rejection of Certificate Applications ..... 12

102 4.2.3 Time to Process Certificate Applications ..... 12

103 4.3 CERTIFICATE ISSUANCE ..... 13

104 4.3.1 CA Actions During Certificate Issuance ..... 13

105 4.3.2 Notification to Certificate Subject of Certificate Issuance ..... 13

106	4.4	CERTIFICATE ACCEPTANCE.....	13
107	4.4.1	Conduct Constituting Certificate Acceptance.....	13
108	4.4.2	Publication of the Certificate by the CA.....	13
109	4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	13
110	4.5	KEY PAIR AND CERTIFICATE USAGE.....	13
111	4.5.1	Certificate Subject Private Key and Certificate Usage.....	13
112	4.5.2	Relying Party Public Key and Certificate Usage.....	13
113	4.6	CERTIFICATE RENEWAL.....	13
114	4.6.1	Circumstance for Certificate Renewal.....	13
115	4.6.2	Who May Request Renewal.....	14
116	4.6.3	Processing Certificate Renewal Requests.....	14
117	4.6.4	Notification of New Certificate Issuance to Certificate Subject.....	14
118	4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	14
119	4.6.6	Publication of the Renewal Certificate by the CA.....	14
120	4.6.7	Notification of Certificate Issuance by the CA to Other Entities.....	14
121	4.7	CERTIFICATE RE-KEY.....	14
122	4.7.1	Circumstance for Certificate Re-key.....	14
123	4.7.2	Who May Request Certification of a New Public Key.....	15
124	4.7.3	Processing Certificate Re-keying Requests.....	15
125	4.7.4	Notification of New Certificate Issuance to Certificate Subject.....	15
126	4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate.....	15
127	4.7.6	Publication of the Re-keyed Certificate by the CA.....	15
128	4.7.7	Notification of Certificate Issuance by the CA to Other Entities.....	15
129	4.8	MODIFICATION.....	15
130	4.8.1	Circumstance for Certificate Modification.....	15
131	4.8.2	Who May Request Certificate Modification.....	15
132	4.8.3	Processing Certificate Modification Requests.....	15
133	4.8.4	Notification of New Certificate Issuance to Certificate Subject.....	15
134	4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	15
135	4.8.6	Publication of the Modified Certificate by the CA.....	15
136	4.8.7	Notification of Certificate Issuance by the CA to Other Entities.....	16
137	4.9	CERTIFICATE REVOCATION AND SUSPENSION.....	16
138	4.9.1	Circumstances for Revocation.....	16
139	4.9.2	Who Can Request Revocation.....	17
140	4.9.3	Procedure for Revocation Request.....	17
141	4.9.4	Revocation Request Grace Period.....	17
142	4.9.5	Time within which CA Must Process the Revocation Request.....	17
143	4.9.6	Revocation Checking Requirements for Relying Parties.....	17
144	4.9.7	CRL Issuance Frequency.....	17
145	4.9.8	Maximum Latency for CRLs.....	17
146	4.9.9	On-line Revocation/Status Checking Availability.....	17
147	4.9.10	On-line Revocation Checking Requirements.....	17
148	4.9.11	Other Forms of Revocation Advertisements Available.....	17
149	4.9.12	Special Requirements Re Key Compromise.....	17
150	4.9.13	Circumstances for Suspension.....	18
151	4.9.14	Who can Request Suspension.....	18
152	4.9.15	Procedure for Suspension Request.....	18
153	4.9.16	Limits on Suspension Period.....	18
154	4.10	CERTIFICATE STATUS SERVICES.....	18
155	4.10.1	Operational Characteristics.....	18
156	4.10.2	Service Availability.....	18
157	4.10.3	Optional Features.....	18
158	4.11	END OF SUBSCRIPTION.....	18
159	4.12	KEY ESCROW AND RECOVERY.....	18
160	4.12.1	Key Escrow and Recovery Policy and Practices.....	18
161	4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	18

162	<b>5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS .....</b>	<b>19</b>
163	5.1 PHYSICAL CONTROLS .....	19
164	5.1.1 Site Location and Construction .....	19
165	5.1.2 Physical Access.....	19
166	5.1.3 Power and Air Conditioning.....	20
167	5.1.4 Water Exposures.....	20
168	5.1.5 Fire Prevention and Protection .....	20
169	5.1.6 Media Storage.....	20
170	5.1.7 Waste Disposal .....	20
171	5.1.8 Off-Site backup .....	20
172	5.2 PROCEDURAL CONTROLS .....	20
173	5.2.1 Trusted Roles .....	20
174	5.2.2 Number of Persons Required Per Task.....	21
175	5.2.3 Identification and Authentication for Each Role .....	21
176	5.2.4 Roles Requiring Separation of Duties.....	21
177	5.3 PERSONNEL CONTROLS .....	21
178	5.3.1 Qualifications, Experience, and Clearance Requirements .....	21
179	5.3.2 Background Check Procedures.....	21
180	5.3.3 Training Requirements .....	22
181	5.3.4 Retraining Frequency and Requirements .....	22
182	5.3.5 Job Rotation Frequency and Sequence.....	22
183	5.3.6 Sanctions for Unauthorized Actions .....	22
184	5.3.7 Independent Contractor Requirements .....	22
185	5.3.8 Documentation Supplied to Personnel.....	22
186	5.4 AUDIT LOGGING PROCEDURES .....	22
187	5.4.1 Types of Events Recorded .....	22
188	5.4.2 Frequency of Processing Log .....	23
189	5.4.3 Retention Period for Audit Log.....	23
190	5.4.4 Protection of Audit Log.....	23
191	5.4.5 Audit Log Backup Procedures .....	24
192	5.4.6 Audit Collection System (Internal vs. External).....	24
193	5.4.7 Notification to Event-Causing Subject.....	24
194	5.4.8 Vulnerability Assessments.....	24
195	5.5 RECORDS ARCHIVE .....	24
196	5.5.1 Types of Events Archived.....	24
197	5.5.2 Retention Period for Archive .....	24
198	5.5.3 Protection of Archive .....	24
199	5.5.4 Archive Backup Procedures.....	25
200	5.5.5 Requirements for Time-Stamping of Records .....	25
201	5.5.6 Archive Collection System (Internal or External).....	25
202	5.5.7 Procedures to Obtain and Verify Archive Information.....	25
203	5.6 KEY CHANGEOVER.....	25
204	5.7 COMPROMISE AND DISASTER RECOVERY .....	25
205	5.7.1 Incident and Compromise Handling Procedures.....	25
206	5.7.2 Computing Resources, Software, and/or Data Are Corrupted .....	25
207	5.7.3 CA Private Key Compromise Procedures.....	25
208	5.7.4 Business Continuity Capabilities After a Disaster.....	25
209	5.8 CA AND RA TERMINATION .....	26
210	<b>6. TECHNICAL SECURITY CONTROLS .....</b>	<b>27</b>
211	6.1 KEY PAIR GENERATION AND INSTALLATION.....	27
212	6.1.1 Key Pair Generation.....	27
213	6.1.2 Private Key Delivery to Certificate Subject.....	27
214	6.1.3 Public Key Delivery to Certificate Issuer .....	27
215	6.1.4 CA Public Key Delivery to Relying Parties .....	27

216	6.1.5	Key Sizes .....	27
217	6.1.6	Public Key Parameters Generation and Quality Checking .....	27
218	6.1.7	Key Usage Purposes (as per X.509v3 key usage field).....	27
219	6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	28
220	6.2.1	Cryptographic Module Standards and Controls.....	28
221	6.2.2	Private Key Multi-Person Control.....	28
222	6.2.3	Private Key Escrow .....	28
223	6.2.4	Private Key Backup .....	28
224	6.2.5	Private Key Archival.....	28
225	6.2.6	Private Key Transfer into or from a Cryptographic Module.....	28
226	6.2.7	Private Key Storage on Cryptographic Module.....	28
227	6.2.8	Method of Activating Private Keys .....	28
228	6.2.9	Methods of Deactivating Private Keys.....	28
229	6.2.10	Method of Destroying Private Key.....	29
230	6.2.11	Cryptographic Module Rating .....	29
231	6.3	OTHER ASPECTS OF KEY MANAGEMENT.....	29
232	6.3.1	Public Key Archival.....	29
233	6.3.2	Certificate Operational Periods/Key Usage Periods.....	29
234	6.4	ACTIVATION DATA.....	29
235	6.4.1	Activation Data Generation and Installation.....	29
236	6.4.2	Activation Data Protection .....	29
237	6.4.3	Other Aspects of Activation Data .....	29
238	6.5	COMPUTER SECURITY CONTROLS .....	30
239	6.5.1	Specific Computer Security Technical Requirements .....	30
240	6.5.2	Computer Security Rating.....	30
241	6.6	LIFE-CYCLE SECURITY CONTROLS.....	31
242	6.6.1	System Development Controls .....	31
243	6.6.2	Security Management Controls.....	31
244	6.6.3	Life Cycle Security Ratings.....	31
245	6.7	NETWORK SECURITY CONTROLS.....	31
246	6.8	TIME STAMPING .....	32
247	<b>7.</b>	<b>CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT .....</b>	<b>33</b>
248	7.1	CERTIFICATE PROFILE .....	33
249	7.2	CRL PROFILE .....	33
250	7.3	OCSP PROFILE.....	33
251	7.4	SCVP PROFILE.....	33
252	<b>8.</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>34</b>
253	8.1	FREQUENCY OF AUDIT OR ASSESSMENTS.....	34
254	8.2	IDENTITY AND QUALIFICATIONS OF ASSESSOR .....	34
255	8.3	ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY .....	34
256	8.4	TOPICS COVERED BY ASSESSMENT.....	34
257	8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	34
258	8.6	COMMUNICATION OF RESULTS.....	34
259	<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>35</b>
260	9.1	FEES .....	35
261	9.1.1	Certificate Issuance/Renewal Fees .....	35
262	9.1.2	Certificate Access Fees.....	35
263	9.1.3	Revocation or Status Information Access Fee .....	35
264	9.1.4	Fees for other Services .....	35
265	9.1.5	Refund Policy.....	35

266	9.2	FINANCIAL RESPONSIBILITY.....	35
267	9.2.1	<i>Insurance Coverage</i> .....	35
268	9.2.2	<i>Other Assets</i> .....	35
269	9.2.3	<i>Insurance/warranty Coverage for End-Entities</i> .....	35
270	9.3	CONFIDENTIALITY OF BUSINESS INFORMATION .....	36
271	9.3.1	<i>Scope of Confidential Information</i> .....	36
272	9.3.2	<i>Information Not Within the Scope of Confidential Information</i> .....	36
273	9.3.3	<i>Responsibility to Protect Confidential Information</i> .....	36
274	9.4	PRIVACY OF PERSONAL INFORMATION .....	36
275	9.4.1	<i>Privacy Plan</i> .....	36
276	9.4.2	<i>Information Treated as Private</i> .....	36
277	9.4.3	<i>Information Not Deemed Private</i> .....	36
278	9.4.4	<i>Responsibility to Protect Private Information</i> .....	36
279	9.4.5	<i>Notice and Consent to use Private Information</i> .....	36
280	9.4.6	<i>Disclosure Pursuant to Judicial/Administrative Process</i> .....	36
281	9.4.7	<i>Other Information Disclosure Circumstances</i> .....	37
282	9.5	INTELLECTUAL PROPERTY RIGHTS.....	37
283	9.6	REPRESENTATIONS AND WARRANTIES .....	37
284	9.6.1	<i>PA / WiMAX Forum</i> .....	37
285	9.6.2	<i>Generally Applicable Representations and Warranties</i> .....	38
286	9.6.3	<i>CA Representations and Warranties</i> .....	38
287	9.6.4	<i>RA Representations and Warranties</i> .....	38
288	9.6.5	<i>Certificate Subject Representations and Warranties</i> .....	39
289	9.6.6	<i>Relying Parties Representations and Warranties</i> .....	39
290	9.6.7	<i>Representations and Warranties of Other Participants</i> .....	39
291	9.7	DISCLAIMERS OF WARRANTIES .....	39
292	9.8	LIMITATIONS OF LIABILITY .....	39
293	9.8.1	<i>PA / WiMAX Forum</i> .....	39
294	9.8.2	<i>Other Participants</i> .....	39
295	9.9	INDEMNITIES .....	39
296	9.9.1	<i>PA / WiMAX Forum</i> .....	39
297	9.9.2	<i>Other Participants</i> .....	39
298	9.10	TERM AND TERMINATION.....	40
299	9.10.1	<i>Term</i> .....	40
300	9.10.2	<i>Termination</i> .....	40
301	9.10.3	<i>Effect of Termination and Survival</i> .....	40
302	9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	40
303	9.12	AMENDMENTS .....	40
304	9.12.1	<i>Procedure for Amendment</i> .....	40
305	9.12.2	<i>Notification Mechanism and Period</i> .....	41
306	9.12.3	<i>Circumstances Under Which OID Must Be Changed</i> .....	41
307	9.13	DISPUTE RESOLUTION PROVISIONS .....	41
308	9.14	GOVERNING LAW .....	41
309	9.15	COMPLIANCE WITH APPLICABLE LAW.....	41
310	9.16	MISCELLANEOUS PROVISIONS.....	41
311	9.16.1	<i>Document Incorporated into CP</i> .....	41
312	9.16.2	<i>Entire agreement</i> .....	41
313	9.16.3	<i>Assignment</i> .....	41
314	9.16.4	<i>Severability</i> .....	42
315	9.16.5	<i>Waiver</i> .....	42
316	9.16.6	<i>Attorneys' Fees</i> .....	42
317	9.16.7	<i>Force Majeure</i> .....	42
318	9.17	OTHER PROVISIONS .....	42
319			

320	<b>TABLE OF FIGURES</b>	
321	Figure 1 - Device PKI.....	2
322	Figure 2 - Server PKI.....	3
323		

## 324 **1. Introduction**

325 This chapter identifies and introduces the set of provisions, and indicates the types of entities and applications for  
326 which the WiMAX Certificate Policy (CP) is targeted.

327 The WiMAX CP is written for WiMAX Forum® products.

328 The WiMAX CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509  
329 (PKIX) Certificate Policy and Certification Practices Framework as described in RFC 3647.

### 330 **1.1 Overview**

331 The WiMAX CP is written for WiMAX Forum® products. The WiMAX CP defines the policy under which the  
332 WiMAX Public Key Infrastructure (PKI) issues Public Key Certificates (PKCs) to Manufacturer CAs, their Device  
333 Sub-CAs, and finally Devices. This CP also addresses PKCs issued to support Server CAs and Server certificates.  
334 The WiMAX PKI enables mutual authentication of devices and networks via EAP. Digital signatures as well as  
335 encryption are employed.

### 336 **1.2 Document Name and Identification**

337 This CP is known as the “WiMAX Server CP.” The Server PKI will use the OID { 1.3.6.1.4.1.24757.1.2 } to  
338 indicate the certificates issued under this CP.

### 339 **1.3 PKI Participants**

340 The following are roles relevant to the administration and operation of the WiMAX PKI.

#### 341 **1.3.1 Policy Authority**

342 The Policy Authority (PA) is the entity that approves this server certificate policy. The PA is the WiMAX Forum  
343 Board.

344 The WiMAX PA also approves all agreements (i.e., CP, Certification Practice Statement (CPS), relying party  
345 agreements, and Certificate Subject agreements) that affect the Device PKI (see sections 1.3.2, 1.3.4, and 1.3.5).

346 The WiMAX PA MAY delegate these functions to a committee or a specific individual or individuals.

#### 347 **1.3.2 Certification Authorities**

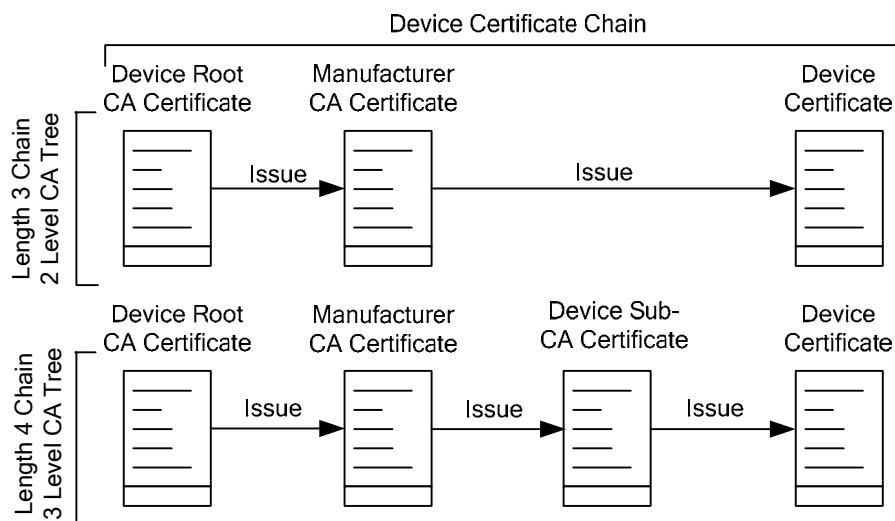
348 The CA is responsible for all aspects of the issuance and management of a PKC including:

- 349 • Registration,
- 350 • Identification and authentication,
- 351 • Issuance, and
- 352 • Ensuring that all aspects of the CA services and CA operations and infrastructure related to PKCs issued  
353 under the WiMAX CP are performed in accordance with the requirements, representations, and warranties  
354 of their WiMAX CPS.

355 CAs that support the WiMAX PKI can be divided into two categories:

- 356
- Device CAs are those that are part of the Certification Path that issues Device PKCs (see Figure 1):
    - 357 ○ Device Root CA is the entity that creates, signs, and issues PKCs to Manufacturer CAs. Device
    - 358 Root CAs are identified by the WiMAX PA, and there MAY be more than one Device Root CA.
    - 359 ○ Device Manufacturer CAs are entities that create, sign, and issue PKCs to Devices. Manufacturer
    - 360 CAs can also create, sign, and issue PKCs to Device Sub-CAs.
    - 361 ○ (optional) Device Sub-CA, when they are used, are entities that create, sign, and issue PKCs to
    - 362 Devices.
  - Server CAs are those that are part of the Certification Path that issues Server PKCs (see Figure 2):
    - 363 ○ Server Root CA is the entity that creates, signs, and issues PKCs to Server CAs. There will be at
    - 364 least one Server Root CA.
    - 365 ○ Server CAs are the entities that create, sign, and issue PKCs to Servers. Server CAs can also
    - 366 create, sign, and issue PKCs to server Sub-CAs.
    - 367 ○ (optional) Server Sub-CAs, when they are used, are entities that create, sign, and issue PKCs to
    - 368 Servers.
    - 369

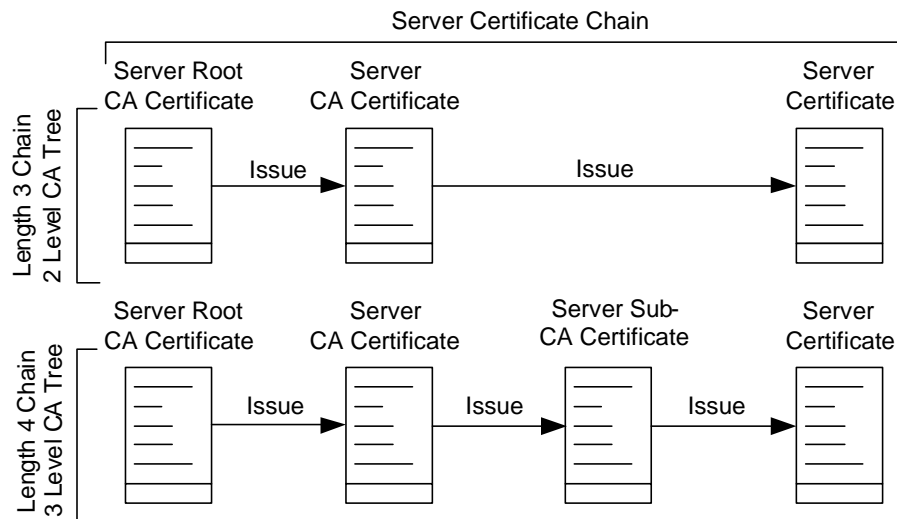
370 Server CAs SHALL NOT issue Device PKCs. Device CAs and Device Sub-CAs SHALL NOT issue Server PKCs.



371

372

**Figure 1 - Device PKI**



373

374

**Figure 2 - Server PKI**

375 In the remainder of this document, the term CA only applies to Server CAs. Distinction between Server Root CA,  
376 Server CA, and Server Sub-CAs is only made when the requirements are different for a type of CA.

377 Agreements (i.e., CP, CPS, relying party agreements, and Certificate Subject agreements) that apply to Server CAs  
378 MUST be approved by the WiMAX PA. The approved CP will be publicly available by the WiMAX Forum PA.  
379 The CPS may be kept private or made publicly available at the discretion of WiMAX Forum PA.

### 380 1.3.3 Registration Authority (RA)

381 No stipulation. If procedures and practices make use of an RA, then the CPS MUST specify the manner in which  
382 the RA is used.

### 383 1.3.4 Certificate Subjects

384 A Certificate Subject is the entity's whose name appears in the subject in a PKC and who asserts that the PKC and  
385 the keying material will be used in accordance with the WiMAX CP. Like the CAs, they are categorized in one of  
386 two ways:

- 387 • Devices are issued PKCs from the Device PKI to gain access to Servers following device authentication via  
388 EAP-TLS or EAP-TTLS methods as specified in [NWG Rel 1.0 Stage 3 Specification].
- 389 • Servers are issued PKCs from the Server PKI to grant access to Devices via EAP-TLS or EAP-TTLS  
390 methods as specified in [NWG Rel 1.0 Stage 3 Specification].

391 In this CP, none of the various types of CAs or an OCSP responder is referred to as Certificate Subjects. Only end-  
392 entity certificate holders are referred to as Certificate Subjects. In the remainder of this document, the term  
393 Certificate Subject refers to Servers.

394 Agreements (i.e., CP, CPS, relying party agreements, and Certificate Subject agreements) that apply to a Device's  
395 PKC MUST be approved by the WiMAX PA.

### 396 1.3.5 Relying Parties

397 In WiMAX Forum environment, Servers are Relying Parties of the Device PKI, and Devices are Relying Parties of  
398 the Server PKI. In the remainder of this document, the term Relying Parties only applies to Servers that validate  
399 certificates issued to Devices in conformance with this certificate policy.

400 Agreements (i.e., CP, CPS, relying party agreements, and Certificate Subject agreements) that apply to a Device's  
401 PKC MUST be approved by the WiMAX PA.

402 **1.3.6 OCSF Responders**

403 The CA operator runs the OCSF responder or arranges for a third party to do so on its behalf. OCSF responders act  
404 on behalf of CAs for a single purpose - signing OCSF response. Therefore, in the remainder of this document,  
405 OCSF responders are not addresses as separate entities from the CAs that they support unless the requirements  
406 differ.

407 **1.3.7 Other Participants**

408 No stipulation.

409 **1.4 Certificate Usage**

410 The WiMAX CP object identifier (OID) defined in this document (see Section 1.2) SHALL only be used for the  
411 following purposes:

- 412 • WiMAX Server CAs and Server Sub-CAs SHALL issue PKCs only to support WiMAX Servers, to issue  
413 revocation information, and to issue OCSF responder certificates. All other uses of WiMAX Server CA  
414 and Server Sub-CA PKCs are expressly prohibited.
- 415 • WiMAX Servers SHALL use their PKC only to establish connections with WiMAX Devices. All other  
416 uses of a WiMAX Server PKC are expressly prohibited.
- 417 • WiMAX OCSF responders SHALL use their PKC only to generate OCSF responses for WiMAX Devices  
418 and/or Servers.

419 **1.5 Policy Administration**

420 The WiMAX Forum is responsible for all aspects of this CP and approval of all Device PKI related agreements.

421 All communications regarding this CP should be directed to:

422 WiMAX Forum  
423 2495 Leghorn Street  
424 Mountain View, CA 94043

## 425 **1.6 Definitions and Acronyms**

426	ABADSG	American Bar Association Digital Signature Guidelines
427	CA	Certification Authority
428	CP	Certificate Policy
429	CPS	Certification Practice Statement
430	CRL	Certificate Revocation List
431	DN	Distinguished Name
432	EAP	Extensible Authentication Protocol
433	EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
434	HSM	Hardware Security Module
435	I&A	Identification and Authentication
436	IEEE/RAC	Institute of Electrical and Electronics Engineers Registration Authority Committee
437	IETF	Internet Engineering Task Force
438	MCC	Mobile Country Code
439	MNC	Mobile Network Code
440	NSP-ID	Network Service Provider ID
441	OCSP	Online Certificate Status Protocol
442	OID	Object Identifier
443	PA	Policy Authority
444	PKC	Public Key Certificate
445	PKI	Public Key Infrastructure
446	RP	Relying Party
447	RA	Registration Authority
448	SCVP	Server-based Certificate Verification Protocol
449	SP	Service Party
450	TLS	Transport Layer Security
451		
	Archive	Long-term, physically separate storage.
	Administrator	A trusted role that installs, configures, and maintains the CA.
	Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
	Auditor	A trusted role that performs the Audit.
	Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
	Backup	Copy of files and programs made to facilitate recovery if necessary.
	Certification Authority (CA)	The CA is responsible for all aspects of the issuance and management of a PKC including: registration, identification and authentication, issuance, and ensuring that all aspects of the CA services and CA operations and infrastructure related to PKCs issued under the WiMAX CP are performed in accordance with the requirements, representations, and warranties of their WiMAX CPS.
	Certificate (or Public Key Certificate)	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Certificate Subject, (3) contains the Certificate Subject's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it [ABADSG].

Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module [FIPS140].
Device	An entity that uses EAP with a Server for authentication prior to gaining network access.
Extensible Authentication Protocol - Transport Layer Security	The Extensible Authentication Protocol (EAP) provides a standard mechanism for support of multiple authentication methods. The use of EAP allows support for a number of authentication schemes. The WiMAX Forum plans to use EAP-TLS, EAP-TTLS and IEEE 802.16, as specified in [NWG Rel 1.0 Stage 3 Specification].
PKC holder	An entity that is control of the private key associated with a PKC.
National Archive and Records Administration (NARA)	US Federal Agency responsible for identifying federal records management and retention policies.
Network Service Provider ID (NSP-ID)	A 24-bit identifier which is used to represent a Network Service Provider. Defined in NWG Release 1.0 Stage 3 Specification. This document only relates to globally-unique NSPIDs, which are either assigned by IEEE RAC or computed from a globally-unique MCC/MNC <a href="https://standards.ieee.org/regauth/BOPID/IEEERegistrationAuthority_BOPID.html">[https://standards.ieee.org/regauth/BOPID/IEEERegistrationAuthority_BOPID.html]</a> and <a href="https://standards.ieee.org/regauth/BOPID/Broadband_OperatorID_Tutorial.html">[https://standards.ieee.org/regauth/BOPID/Broadband_OperatorID_Tutorial.html]</a> .
Server	An entity that uses EAP to grant a Device network access.

## 452 **2. Publication and Repository Responsibilities**

453 This chapter specifies requirements for publication of PKCs and CRLs in a repository.

### 454 **2.1 Repositories**

455 Server, Server CA and Server Sub-CA revocation information **MUST** be published in a Device accessible  
456 repository. This repository **MUST** be accessible to OCSP responders.

457 No stipulation for the repository on Server CA, Server Sub-CA, and Server PKCs.

### 458 **2.2 Publication of certification information**

459 No stipulation for the repository on Server CA, Server Sub-CA, and Server PKCs.

460 Revocation information **SHALL** be published in a Certificate Revocation List (CRL) and **SHALL** also be available  
461 via the Online-Certificate Status Protocol (OCSP).<sup>1</sup> It **MAY** also be available via the Server-based Certificate  
462 Verification Protocol (SCVP).<sup>2</sup>

### 463 **2.3 Time or Frequency of Publication**

464 No stipulation for the repository on Server CA, Server Sub-CA, and Server PKCs.

465 CAs **SHALL** promptly publish CRLs after they are generated. In the absence of a revocation event, updated CRLs  
466 **SHALL** be published at least quarterly by Server Root CAs and at least monthly by Server CAs and Server Sub-  
467 CAs.

### 468 **2.4 Access Controls on Repositories**

469 No stipulation.

---

<sup>1</sup> Profiles for WiMAX Forum CRLs and OCSP requests and responses are in section 7.

<sup>2</sup> Profiles for WiMAX Forum SCVP requests and responses are in section 7.

---

## 470 3. Identification and Authentication

471 This chapter specifies the requirements for Identification and Authentication (I&A) of the Certificate Subject and  
472 CA.

### 473 3.1 Naming

#### 474 3.1.1 Types of Names

475 Within the Server PKI, the Certificate Subject Name MUST be an X.501 Distinguished Name (DN) carried in the  
476 PKC. The following SHALL be the name forms:

- 477 • Server Root CA: C=US, O=WiMAX Forum(R), CN=WiMAX Forum(R) Server Root-CA<n>
- 478 • Server CA: C=<country>, O=<Service Provider>, OU=WiMAX Forum(R) Server, CN=<defined by  
479 Service Provider>-<n>
- 480 • Server Sub-CA: C=<country>, O=<Service Provider>, OU=WiMAX Forum(R) Server, OU=<defined by  
481 Service Provider>, CN=<defined by Service Provider>  
482 or  
483 Server Sub-CA: C=<country>, O=<Service Provider>, OU=WiMAX Forum(R) Server, L=<defined by  
484 Service Provider>, CN=<defined by Service Provider>
- 485 • Server: C=<country>, O=<Service Provider>, OU=WiMAX Forum(R) Server, OU=<NSPID>,<sup>3</sup>  
486 CN=<Domain Name of the Service Provider>
- 487 • OCSP Responder:
  - 488 ○ For Root CAs: For Root CAs: C=US, O=WiMAX Forum(R), CN=Server OCSP Responder-<x>
  - 489 ○ For Server CAs: C=<country>, O=<Service Provider>, OU=WiMAX Forum(R) Server,  
490 CN=OCSP Responder-<y>

491 When the naming element is DirectoryString (i.e., O= and OU=) either PrintableString or UTF8String MUST be  
492 used. The following determines which choice is used:

- 493 • PrintableString only if it is limited to the following subset of US ASCII characters (as required by ASN.1):  
494 A, B, ..., Z  
495 a, b, ..., z  
496 0, 1, ...9,  
497 (space) ' ( ) + , - . / : = ?
- 498 • UTF8String for all other cases, e.g., subject name attributes with any other characters or for international  
499 character sets.

#### 500 3.1.2 Meaningfulness

501 Names SHALL be meaningful and unambiguously identify all entities with PKCs.

#### 502 3.1.3 Anonymity or Pseudonymity of Certificate Subjects

503 Names SHALL NOT be anonymous or be a pseudonym.

---

<sup>3</sup> Globally-unique NSPID (see clause 1.6).

504 **3.1.4 Rules for Interpreting Various Name Forms**

505 See Section 3.1.1.

506 **3.1.5 Uniqueness of Names**

507 CA names SHALL be unique across the whole WiMAX Server PKI. No stipulation regarding uniqueness of Server  
508 Names.

509 No stipulation for Server names.

510 **3.1.6 Recognition, Authentication, and Role of Trademarks**

511 CAs SHALL NOT knowingly issue a PKC with a name that a court of competent jurisdiction has determined  
512 infringes on the trademark of another.

513 Server Root CAs, Server CAs, Server Sub-CAs, and Server PKCs all include the string “WiMAX Forum(R)” in  
514 their name. A written agreement with the WiMAX Forum is needed to obtain authorization to use this trademark-  
515 protected string.

516 Server Root CAs issue PKCs to Server CAs that includes trademark-protected names, namely, the Service  
517 Provider’s name. The Server Root CAs MUST verify that applicant is authorized to request on behalf of the service  
518 provider.

519 Server CAs MAY issue PKCs to Server Sub-CAs that include trademark-protected names; however, Server CAs  
520 SHALL only issue PKCs with subject names that use the same organization as the service provider’s CA name. If  
521 the Server CAs includes a second organizational unit name that is trademarked, then the trademark MUST be owned  
522 by the service provider.

523 **3.2 Initial Identity Validation**

524 **3.2.1 Method to Prove Possession of Private Key**

525 CAs SHALL generate their own keys. They MUST prove to the issuing CA that they possess the private keys that  
526 corresponds to the public keys in PKC requests.

527 Servers MAY or MAY NOT generate their own keys:

- 528 • If a Server generates its own key, then they MUST prove to the issuing CA that they possess the private  
529 key that corresponds to the public key in PKC requests.
- 530 • If a Server does not generate its own private key, then the key generation and distribution process MUST  
531 be explained in the CPS. These processes MUST ensure that the private key is provided to the proper  
532 Service Provider in a manner that protects the key from unauthorized disclosure and modification. The  
533 Service Provider MUST ensure that the proper key and certificate is installed in the corresponding Server  
534 in a manner that protects the key from unauthorized disclosure and modification. The Service Provider  
535 process MUST be documented.

536 **3.2.2 Authentication of Organization Identity**

537 Confirm that the organization has authorized the application and that the person submitting the application is  
538 authorized to do so. At a minimum, a letter from the Service Provider’s Chief Legal Officer (or other authorized  
539 representative recognized by WiMAX Forum's PA) required for authorization. At a minimum, the following MUST  
540 occur:

- 541 • Use a third party to confirm the organization exists; and
- 542 • Confirm that the organization has authorized the application and that the person submitting the application  
543 is authorized to do so. At a minimum, a letter from the Service Provider’s Chief Legal Officer (or other  
544 authorized legal representative recognized by the WiMAX Forum) is required for authorization.

545 Server CAs that issue PKCs to Server Sub-CAs and Servers are exempt from these rules only when they issue PKCs  
546 to Server Sub-CAs they control and Servers they own.

547 **3.2.3 Authentication of Individual Identity**

548 Issuing CA SHALL validate at least the identity in the “Service Provider” field of server certificate issued. CA  
549 names SHALL be validated by the issuing CA.

550 **3.2.4 Non-verified Certificate Subject Information**

551 All information SHALL be verified. Non-verified information SHALL NOT be included in PKCs.

552 **3.2.5 Validation of Authority**

553 Server Root CAs SHALL verify that the Server CA is a WiMAX Forum's PA's recognized Service Provider, and the  
554 letter from the Service Provider’s Chief Legal Officer (or other authorized representative recognized by WiMAX  
555 Forum's PA) is valid. The Root CA SHALL have access to a list of approved Service Providers maintained by the  
556 WiMAX Forum. This list SHALL be consulted prior to issuing a Server CA’s PKC.

557 Server CAs and Server Sub-CAs MUST perform the following checks for servers:

- 558 • Ensure requested Network Service Provider ID (NSP-ID) has been allocated by Institute of Electrical and  
559 Electronics Engineers Registration Authority Committee (IEEE-RAC) to the requesting party or computed  
560 from the Mobile Country Codes (MCC) and Mobile Network Codes (MNC) allocated to the requesting  
561 party.<sup>4</sup>
- 562 • Ensure requested Domain Name has been assigned to the requesting party.
- 563 • Obtain and verify a signed letter from server’s authorized representative indicating that they are allowed to  
564 assert the NSP-ID their certificate(s).<sup>5</sup>

565 **3.2.6 Criteria for Interoperation**

566 WiMAX Server CAs and Server Sub-CAs SHALL issue PKCs only to support WiMAX Servers, to issue revocation  
567 information, and to issue OCSP responder certificates. All other uses of WiMAX Server CA PKCs are expressly  
568 prohibited.

569 WiMAX Servers SHALL use their PKC only to establish a connection with WiMAX Devices. All other uses of a  
570 WiMAX Server PKC are expressly prohibited.

---

<sup>4</sup> See clause 1.6 for NSPID, MNC, and MCC definitions.

<sup>5</sup> • Certificates with “private” or “test” NSPIDs which are not globally-unique may be required for testing purposes. It is recommended to allow flexibility in the solution to serve this need. It should be specified in the CPS how this certificate is used only for testing.

### 571 **3.3 Identification and Authentication for Re-key Requests**

572 Prior to the expiration of an existing PKC, it is necessary to re-key or renew the PKC to maintain continuity of PKC  
573 usage. An overlap period is recommended to ensure continuity. This continuity is supported for Server CAs and  
574 Server Sub-CAs with both re-key (see Section 4.7) and renewal (see Section 4.6). Server continuity is supported  
575 with re-key (see Section 4.7).

#### 576 **3.3.1 Identification and Authentication of Re-Key and Renewal Requests**

577 The superior CA SHALL be responsible for authentication of a request for re-key or renewal. Re-key and renewal  
578 procedures ensure the entity requesting the re-key or renewal is in fact the entity that is named in the PKC.

579 The procedures for a re-key and renewal procedures are the same those for the original certificate.

#### 580 **3.3.2 Identification and Authentication of Re-Key and Renewal After Revocation**

581 Re-key and renewal after revocation is not permitted if the revocation occurred for any of the following reasons:

- 582 • The PKC was issued to an entity other than the one named as the Subject of the PKC.
- 583 • The PKC was issued without the authorization of the entity named as the Subject of the PKC.
- 584 • The entity approving the PKC application has reason to believe that a material fact in the PKC application  
585 is false.
- 586 • The PKC was deemed by the WiMAX PA to be harmful to the WiMAX Forum.

587 Subject to the above bullets, re-key or renewal following revocation of the PKC is permissible as long as re-key or  
588 renewal procedures ensures that the entity seeking re-key or renewal is in fact the entity named in the PKC.

### 589 **3.4 Identification and Authentication for Revocation Request**

590 WiMAX Forum PA, or recognized representative, or an authorized process from the service provider can request  
591 revocation and SHALL use their credentials to authenticate the request. The form of credential accepted by the  
592 revoking CA is based on CA CPS. A revocation request authentication MUST be properly verified before an  
593 approval decision is made.

594 The revocation of any CA requires authorization from the WiMAX PA. See 4.9 for more information revocation.

## 595 **4. Certificate Life-Cycle**

596 This chapter specifies the requirements for PKC life-cycle management by all entities in the PKI.

### 597 **4.1 Certificate Application**

#### 598 **4.1.1 Who Can Submit a Certificate Application**

599 A recognized Service Provider representative can submit CA PKC applications. An authorized Server  
600 representative, an authorized Server process, or a Server can submit Server PKC applications.

601 Applications for Server certificates associated with public networks will only be honored from WiMAX Forum  
602 Members. There are no membership requirements for certificates associated with private networks.

#### 603 **4.1.2 Enrollment Process and Responsibilities**

604 A recognized Server CAs representatives SHALL provide their credentials to Server Root CAs to demonstrate their  
605 identity, to demonstrate their authority, and to provide contact information. Service providers receive and approve  
606 requests from a recognized Server Sub-CAs representative and from an authorized Server representative, an  
607 authorized Server process, or a Server.

608 A recognized Server Sub-CAs representative SHALL provide their credentials to Server CAs to demonstrate their  
609 identity, to demonstrate their authority, and to provide contact information. Server Sub-CAs receive and approve  
610 enrollments from an authorized Server representative, an authorized Server process, or a Server.

611 An authorized Server representative, an authorized Server process, and a Server SHALL provide their credentials to  
612 Server CAs or Server Sub-CAs to demonstrate their identity, to demonstrate their authority, and to provide contact  
613 information.

### 614 **4.2 Certificate Application Processing**

#### 615 **4.2.1 Performing Identification and Authentication Functions**

616 CAs SHALL verify and authenticate the identity of each applicant, as described in Section 3.2.

#### 617 **4.2.2 Approval or Rejection of Certificate Applications**

618 The CA MAY approve or reject a certification request. Approval is granted if the applicant's identity has been  
619 authenticated as described in Section 3.2, and payment, if required, has been received. Rejection is based inability  
620 to successfully authenticate the applicant, not receiving required information from the applicant, not paying for PKC  
621 (if required).

622 The WiMAX PA MUST approve all Server Sub-CAs.

#### 623 **4.2.3 Time to Process Certificate Applications**

624 PKC requests SHALL be processed in a timely manner.

## 625 **4.3 Certificate Issuance**

### 626 **4.3.1 CA Actions During Certificate Issuance**

627 The CA SHALL verify and authenticate the source of each PKC request, ensure that the public key is bound to the  
628 correct applicant, obtain a proof of possession of the private key, generate a properly formed PKC, and provide the  
629 PKC to the applicant.

### 630 **4.3.2 Notification to Certificate Subject of Certificate Issuance**

631 The CA SHALL notify the applicant of PKC issuance by returning the PKC (and the corresponding private key, if  
632 the key was generated by the CA) to the applicant.

## 633 **4.4 Certificate Acceptance**

### 634 **4.4.1 Conduct Constituting Certificate Acceptance**

635 Failure to object to the PKC or its contents prior to use constitutes acceptance of the PKC.

### 636 **4.4.2 Publication of the Certificate by the CA**

637 No stipulation.

### 638 **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

639 No stipulation.

## 640 **4.5 Key Pair and Certificate Usage**

### 641 **4.5.1 Certificate Subject Private Key and Certificate Usage**

642 Certificate Subjects SHALL be responsible for and SHALL protect their private keys from access by other parties.

643 Certificate Subjects SHALL only use private keys for purposes identified in Section 1.4.

### 644 **4.5.2 Relying Party Public Key and Certificate Usage**

645 Relying parties SHALL ensure that the public key in a PKC is used only for appropriate purposes as identified in  
646 critical certificate extensions (See Section 7).

## 647 **4.6 Certificate Renewal**

648 PKC renewal is the issuance of a new PKC to the Server CA, Server Sub-CA, or Server without changing the public  
649 key or any other information other than the validity dates and the serial number in the PKC. Certificate renewal is  
650 supported for Server CAs, Server Sub-CAs, and Servers.

### 651 **4.6.1 Circumstance for Certificate Renewal**

652 When a Server CA PKC renewal is desired, it is necessary for the renewal to take place prior to the expiration of an  
653 existing Server CA's PKC to maintain continuity of PKC usage. An overlap period is recommended to ensure  
654 continuity.

655 When a Server Sub-CA PKC renewal is desired, it is necessary for the renewal to take place prior to the expiration  
656 of an existing Server Sub-CA's PKC to maintain continuity of PKC usage. An overlap period is recommended to  
657 ensure continuity.

658 When a Server PKC renewal is desired, it is necessary for the renewal to take place prior to the expiration of an  
659 existing Server's PKC to maintain continuity of PKC usage. An overlap period is recommended to ensure  
660 continuity.

661 Server CA, Server Sub-CA, and Server PKCs MAY also be renewed after expiration.

#### 662 **4.6.2 Who May Request Renewal**

663 All requests for PKC renewals MUST come from WiMAX Forum Members.

664 A recognized representative can submit Server CA and Sub-CA PKC renewal requests.

665 An authorized Server representative, an authorized Server process, or a Server can submit Server PKC renewal  
666 request.

#### 667 **4.6.3 Processing Certificate Renewal Requests**

668 In accordance with Section 4.2.

#### 669 **4.6.4 Notification of New Certificate Issuance to Certificate Subject**

670 In accordance with Section 4.3.2.

#### 671 **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**

672 In accordance with Section 4.4.1.

#### 673 **4.6.6 Publication of the Renewal Certificate by the CA**

674 In accordance with Section 4.4.2.

#### 675 **4.6.7 Notification of Certificate Issuance by the CA to Other Entities**

676 No stipulation.

### 677 **4.7 Certificate Re-Key**

678 PKC re-key is the application for the issuance of a new PKC that certifies a new public key. PKC re-key is  
679 supported for Server CAs, Sub-CAs, and Servers.

#### 680 **4.7.1 Circumstance for Certificate Re-key**

681 When a Server CA PKC re-key is desired, it is necessary for the re-key to take place prior to the expiration of an  
682 existing Server CA's PKC to maintain continuity of PKC usage. An overlap period is recommended to ensure  
683 continuity.

684 When a Server Sub-CA PKC re-key is desired, it is necessary for the re-key to take place prior to the expiration of  
685 an existing Server Sub-CA's PKC to maintain continuity of PKC usage. An overlap period is recommended to  
686 ensure continuity.

687 When a Server PKC re-rekey is desired, it is necessary for the re-key to take place prior to the expiration of an  
688 existing Server's PKC to maintain continuity of PKC usage. An overlap period is recommended to ensure  
689 continuity.

690 Server CA, Server Sub-CA, and Server PKCs MAY also be renewed after expiration.

691 **4.7.2 Who May Request Certification of a New Public Key**

692 All requests for PKC re-keys MUST come from WiMAX Forum Members.

693 A recognized representative can submit Server CA and Sub-CA PKC re-key requests. Server CAs can request re-  
694 keys for their PKCs and Server Sub-CAs can request rekeys for their PKCs. This is a multiparty procedure as  
695 specified in Section 5.2.2 and requires a "Key Ceremony" as specified in Section 6.1.1.

696 An authorized Server representative, an authorized Server process, or a Server can submit Server PKC renewal  
697 request.

698 **4.7.3 Processing Certificate Re-keying Requests**

699 In accordance with Section 4.2.

700 **4.7.4 Notification of New Certificate Issuance to Certificate Subject**

701 In accordance with Section 4.3.2.

702 **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

703 In accordance with Section 4.4.1.

704 **4.7.6 Publication of the Re-keyed Certificate by the CA**

705 In accordance with Section 4.4.2.

706 **4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

707 No stipulation.

708 **4.8 Modification**

709 **4.8.1 Circumstance for Certificate Modification**

710 PKC Modification is prohibited.

711 **4.8.2 Who May Request Certificate Modification**

712 No stipulation.

713 **4.8.3 Processing Certificate Modification Requests**

714 No stipulation.

715 **4.8.4 Notification of New Certificate Issuance to Certificate Subject**

716 No stipulation.

717 **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

718 No stipulation.

719 **4.8.6 Publication of the Modified Certificate by the CA**

720 No stipulation.

721 **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

722 No stipulation.

723 **4.9 Certificate Revocation and Suspension**

724 In an event when certificate's further use is deemed detrimental (e.g. when private key is lost or compromised), the  
725 certificate can be declared invalid, or revoked. This section begins with a brief informative overview of revocation,  
726 and then formally describes corresponding operational procedures.

727 PKC revocation information must be authenticated by the issuing CA to prevent DoS attacks, since inappropriate  
728 PKC revocation prevents the PKC owner from connecting to the network. The choice of the method of  
729 dissemination of revocation information to relying parties is only the matter of efficiency. The WiMAX Forum uses  
730 two of the most popular methods -- CRL and OCSP protocols. CRL is a CA-signed dated list of revoked certificates  
731 which is published regularly. OCSP is a protocol that relies on an online OCSP server, which provides signed dated  
732 statements indicating whether a particular PKC is revoked. CRL and OCSP response are signed objects. Relying  
733 parties can verify the signature on the CRL and OCSP response to determine whether it is valid.

734 Because of connectivity and hardware specifics, device revocation information is more efficiently distributed by  
735 CRL. Indeed, servers have large storage and a fast persistent Internet connection. At the same time, server talks to  
736 many devices, and much of the information included in the CRL is actually used. On the other hand, any particular  
737 device might usually connect to only a few servers. Moreover, the device's network connectivity is achieved via the  
738 server, and is slow. Downloading a potentially large CRL is often less efficient than a short OCSP message, with  
739 which the device is convinced that the server is not revoked. In the WiMAX Forum environment, both OCSP and  
740 CRLs are needed. When OCSP is used, the OCSP message may be periodically obtained by the server, and  
741 forwarded to the device as part of EAP. In this case, the Device need not ever interact with the OCSP server.  
742 However, direct interaction with the OCSP responder is also allowed. When OCSP is not used, the Device obtains  
743 the CRL via an unspecified method.

744 There are many ways to implement OCSP. One example of a typical sequence of events following a decision to  
745 revoke a server's PKC would be as follows. CA includes the PKC in the next CRL update, and updates its OCSP  
746 server within the timeframe specified in the CA's CPS. From that point on, the revoked server would not be able to  
747 obtain a new OCSP response that indicates the certificate is valid. The server would still be able to use the old one  
748 until it expires (expiry periods will be specified in the CA's CPS). After the OCSP response expiry, devices will not  
749 accept the old OCSP response, and will reject EAP-(T)TLS sessions.

750 Another example of a typical sequence of events following a decision to revoke a Server's PKC would be as  
751 follows. CA includes the PKC in the next CRL update, posted at its CRL URL. From that point on, the Device will  
752 be aware that the PKC is revoked, and will reject EAP-(T)TLS session attempts.

753 The following specifies formal operational requirements of PKC revocation procedures.

754 **4.9.1 Circumstances for Revocation**

755 A PKC SHALL be revoked when the binding between the subject and the subject's public key within the PKC is no  
756 longer considered valid (e.g., loss or comprise of the private key). PKCs will be revoked when the PA requests that  
757 a PKC be revoked, when the PKC holder submits an authenticated revocation request, and when the CA determines  
758 a situation has occurred that MAY affect the integrity of the PKCs.

759 **4.9.2 Who Can Request Revocation**

760 Any PKC can be revoked upon the direction of the PA. Additionally:

- 761 • Server CA operators MAY request revocation of their Server CA PKCs, Server Sub-CAs PKCs they issued,  
762 and Server PKCs they issued.
- 763 • Server Sub-CA operators MAY request revocation of their Server Sub-CA PKCs and the Device PKCs  
764 they issued.
- 765 • Server PKCs MAY be revoked at the request of the PA, issuing CA, or Server operator.

766 **4.9.3 Procedure for Revocation Request**

767 PKCs SHALL be revoked upon receipt of sufficient evidence of compromise or loss of the corresponding private  
768 key. A request to revoke a PKC SHALL identify the PKC to be revoked, explain the reason for revocation, and  
769 allow the request to be authenticated (e.g., manually signed).

770 Prior to revocation of Server CA or Server Sub-CA the WiMAX PA MUST authorize the revocation.

771 **4.9.4 Revocation Request Grace Period**

772 The revocation request grace period is the time available to the PKC holder within which the PKC holder MUST  
773 make a revocation request after reasons for revocation have been identified.

774 **4.9.5 Time within which CA Must Process the Revocation Request**

775 CAs MUST process revocation requests in a timely manner.

776 **4.9.6 Revocation Checking Requirements for Relying Parties**

777 If the device is checking revocation of server certificate, it SHOULD use OCSP. If the server is checking revocation  
778 of device certificate, it MAY use OCSP.

779 **4.9.7 CRL Issuance Frequency**

780 CRLs to be issued as described in Section 2.3.

781 **4.9.8 Maximum Latency for CRLs**

782 No stipulation.

783 **4.9.9 On-line Revocation/Status Checking Availability**

784 An OCSP responder MUST be available 24x7 with minimal scheduled interruptions.

785 **4.9.10 On-line Revocation Checking Requirements**

786 No stipulation.

787 **4.9.11 Other Forms of Revocation Advertisements Available**

788 No stipulation.

789 **4.9.12 Special Requirements Re Key Compromise**

790 No stipulation.

791 **4.9.13 Circumstances for Suspension**

792 PKC suspension is prohibited.

793 **4.9.14 Who can Request Suspension**

794 No stipulation.

795 **4.9.15 Procedure for Suspension Request**

796 No stipulation.

797 **4.9.16 Limits on Suspension Period**

798 No stipulation.

799 **4.10 Certificate Status Services**

800 **4.10.1 Operational Characteristics**

801 The status of PKCs is available via CRL through a Device available online repository. Device available OCSP  
802 responders MUST also be provided.

803 **4.10.2 Service Availability**

804 An OCSP responder MUST be available 24x7 with minimal scheduled interruptions.

805 **4.10.3 Optional Features**

806 SCVP MAY be provided.

807 **4.11 End of Subscription**

808 Subscriptions SHALL end when a PKC is revoked or the PKC expiry time passes.

809 **4.12 Key Escrow and Recovery**

810 **4.12.1 Key Escrow and Recovery Policy and Practices**

811 No stipulation.

812 **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

813 No stipulation.

---

## 814 **5. Management, Operational, and Physical Controls**

815 This chapter specifies the requirements for non-technical security controls used by the CA to securely perform the  
816 functions of key generation, subject authentication, PKC issuance, and PKC revocation.

### 817 **5.1 Physical Controls**

#### 818 **5.1.1 Site Location and Construction**

819 The location and construction of the facility that will house CA equipment and operations SHALL be in accordance  
820 with that afforded the most sensitive business and financial information. CA operations SHALL be conducted within  
821 a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of  
822 sensitive information and systems.

#### 823 **5.1.2 Physical Access**

824 The physical security requirements pertaining to CAs are:

- 825 • Ensure no unauthorized access to the hardware is permitted;
- 826 • Ensure manual or electronic monitoring for unauthorized intrusion at all times;
- 827 • Ensure an access log is maintained and inspected periodically; and,
- 828 • Require two person physical access control to both the cryptographic module and computer system.

829 When not in use:

- 830 • Paper containing sensitive plain-text information SHALL be stored in secure containers;
- 831 • Media storing Server Root CA private key material SHALL be deactivated. The media and the activation  
832 information (see Section 6.4) for the Server Root CA private keys SHALL be stored in a secure container.  
833 Activation data SHALL either be memorized, or recorded and stored in a manner commensurate with the  
834 security afforded the cryptographic module, and SHALL NOT be stored with the cryptographic module.
- 835 • Media storing CA private key material SHALL be deactivated. The media SHALL be encrypted. The  
836 activation information (see Section 6.4) for the CA private key SHALL be stored in a secure container.  
837 Activation data SHALL either be memorized, or recorded and stored in a manner commensurate with the  
838 security afforded the cryptographic module, and SHALL NOT be stored with the cryptographic module.

839 If the facility is not continuously attended, the last person to depart SHALL initial a sign-out sheet that indicates the  
840 date and time, and asserts that all necessary physical protection mechanisms are in place and activated. A security  
841 check of the facility housing the CA equipment SHALL occur if the facility is to be left unattended. At a minimum,  
842 the check SHALL verify the following:

- 843 • The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules  
844 are in place when “open”, and secured when “closed”; and for the CA, that all equipment other than the  
845 repository is shut down);
- 846 • Any security containers are properly secured;
- 847 • Physical security systems (e.g., door locks, vent covers) are functioning properly; and,
- 848 • The area is secured against unauthorized access.

849 If at any time the Hardware Security Module (HSM) contain a CA's private is physically moved permanently from  
850 one location to another (i.e., not during normal activation), then:

- 851 • The HSM MUST be protected from destruction, unauthorized disclosure, and unauthorized modification.
- 852 • PA MUST approve the movement.
- 853 • PA or authorized representative MUST be present.
- 854 • The process MUST be videotaped.
- 855 • Record when old location gives new location HSM.

### 856 **5.1.3 Power and Air Conditioning**

857 The facility that houses the CA equipment SHALL be supplied with power and air conditioning sufficient to create a  
858 reliable operating environment.

### 859 **5.1.4 Water Exposures**

860 Facilities that house CAs SHALL be installed such that it is not in danger of exposure to water (e.g., on tables or  
861 elevated floors). Moisture detectors SHALL be installed in areas susceptible to flooding. CA operators who have  
862 sprinklers for fire control SHALL have a contingency plan for recovery should the sprinklers malfunction, or cause  
863 water damage outside of the fire area.

### 864 **5.1.5 Fire Prevention and Protection**

865 Facilities that house CAs SHALL be constructed and equipped, and procedures SHALL be implemented, to prevent  
866 and extinguish fires or other damaging exposure to flame or smoke. These measures SHALL meet all local  
867 applicable safety regulations. A description of the CMA's approach for recovery from a fire disaster SHALL be  
868 included in the Disaster Recovery Plan as specified in Section 5.7.4.

### 869 **5.1.6 Media Storage**

870 When not in operation, the cryptographic modules storing the Server Root CA private key SHALL be stored in a  
871 secure container. When not in operation, the cryptographic modules storing the CA private key SHALL be stored in  
872 a secure room in encrypted form. Media that contains security audit and backup information SHALL be stored in a  
873 separate location from the CA equipment.

### 874 **5.1.7 Waste Disposal**

875 CAs SHALL implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the  
876 unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

### 877 **5.1.8 Off-Site backup**

878 System backups, sufficient to recover from system failure, SHALL be made on a periodic schedule. Backups  
879 SHALL be performed and stored off-site not less than quarterly or when the CA is operational, whichever is less  
880 frequent. At least one backup copy SHALL be stored at an offsite location (separate from the CA equipment). Only  
881 the latest backup need be retained. The backup SHALL be stored at a site with physical and procedural controls  
882 commensurate to that of the operational CA system.

## 883 **5.2 Procedural Controls**

### 884 **5.2.1 Trusted Roles**

885 A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out  
886 properly, whether accidentally or maliciously. The people selected to fill these roles MUST be extraordinarily

887 responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for  
888 all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried  
889 out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the  
890 functions among more than one person, so that any malicious activity would require collusion.

891 The following are the trusted Roles within the PKI:

- 892 • CA Administrator: installs, configures, and maintains the CA; configures PKC profiles and parameters;  
893 generates and performs backup of CA keys;
- 894 • CA Officer: approves/rejects certification requests and PKC revocations;
- 895 • Auditor: maintains and reviews audit logs; and,
- 896 • Backup Operator: performs routine system backup and recovery.

897 Multi-Person control requirements are specified in Section 6.2.2.

## 898 **5.2.2 Number of Persons Required Per Task**

899 CA private key actions require at least “two-party” control:

- 900 • Generation of CA keys;
- 901 • Access to CA keys;
- 902 • Transport of HSM containing CA keys;
- 903 • Backup of CA keys; and,
- 904 • Access to backup CA keys.

905 Where multiparty control is required, at least one of the participants SHALL be an Administrator. All participants  
906 MUST serve in a trusted role as defined in Section 5.2.1. Multiparty control SHALL NOT be achieved using  
907 personnel that serve in the Auditor Trusted Role.

## 908 **5.2.3 Identification and Authentication for Each Role**

909 A person occupying a trusted role SHALL have their identity and authorization verified, before being permitted to  
910 perform any action for that role or identity.

## 911 **5.2.4 Roles Requiring Separation of Duties**

912 Individuals MAY only assume one of the Officer, Administrator, and Auditor roles, but any individual MAY  
913 assume the Operator role. The CA software and hardware SHALL identify and authenticate its users and SHALL  
914 ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator  
915 and Auditor roles, and assume both the Auditor and Officer roles. No individual SHALL have more than one  
916 identity.

## 917 **5.3 Personnel Controls**

### 918 **5.3.1 Qualifications, Experience, and Clearance Requirements**

919 Personnel engaged in the PKI SHALL be suitable qualified and experienced.

### 920 **5.3.2 Background Check Procedures**

921 Vetting process used for trusted personnel engaged in the PKI SHALL be described in the CPS.

922 **5.3.3 Training Requirements**

923 Prior to operation of the CA, the CA operator SHALL be appropriately trained. Topics SHALL include the  
924 operation of the CMA software and hardware, operational and security procedures, and the stipulations of this policy  
925 and local guidance.

926 **5.3.4 Retraining Frequency and Requirements**

927 Refresher training will be provided to the extent and frequency required to ensure the required level of proficiency  
928 to perform job responsibilities competently.

929 **5.3.5 Job Rotation Frequency and Sequence**

930 No stipulation.

931 **5.3.6 Sanctions for Unauthorized Actions**

932 If an unauthorized action takes place than an appropriate action SHALL be taken to ensure disciplinary or other  
933 appropriate action is taken. In cases where an unauthorized action brings into question the security of the system,  
934 then recovery procedures will be followed (see Section 5.7).

935 **5.3.7 Independent Contractor Requirements**

936 Contractor personnel employed to perform functions pertaining to the CA SHALL meet the personnel requirements  
937 set forth in this CP.

938 **5.3.8 Documentation Supplied to Personnel**

939 Documentation sufficient to define duties and procedures for each role SHALL be provided to their personnel filling  
940 that role.

941 **5.4 Audit Logging Procedures**

942 **5.4.1 Types of Events Recorded**

943 Any security auditing capabilities of the underlying CA equipment operating system SHALL be enabled during  
944 installation and operation.

945 At a minimum, the following events SHALL be recorded:

- 946 • CA equipment access;
- 947 • Operating system logon/logoff;
- 948 • CA application access;
- 949 • CA private key generation;
- 950 • CA private key use;
- 951 • Certification request;
- 952 • PKC issuance;
- 953 • PKC revocation request;
- 954 • PKC revocation;
- 955 • Software and/or configuration updates to CA and account management;
- 956 • Clock Adjustments;
- 957 • Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages;
- 958 and,
- 959 • Any known or suspected violations of physical security, suspected or known attempts to attack the CA
- 960 equipment via network attacks, equipment failures, power outages, network failures, or violations of this
- 961 certificate policy.

962 At a minimum, for each auditable event the record SHALL include:

- 963 • The type of event;
- 964 • The time the event occurred;
- 965 • A success or failure indication for signing;
- 966 • The identity of the equipment operator who initiated the action; and,

967 Audit logs SHALL be generated automatically and periodically backed up.

#### 968 **5.4.2 Frequency of Processing Log**

969 Offline CA audit logs SHALL be reviewed at least annually or any time the CA is brought online. Online CA audit  
970 logs SHALL be reviewed quarterly.

971 The review is to include searches for anomalous patterns. Action taken as a result of this review SHALL be  
972 documented.

973 Audit log reviews SHALL also be conducted when requested by the PA.

#### 974 **5.4.3 Retention Period for Audit Log**

975 The information generated on the CA equipment SHALL be kept on the CA equipment until the information is  
976 moved to an appropriate archive facility. Audit logs SHALL be available for three months, at a minimum, then  
977 offsite as archive records (See Section 5.5).

#### 978 **5.4.4 Protection of Audit Log**

979 Only personnel assigned to a trusted role have read access to the logs. Only authorized personnel MAY archive  
980 audit logs. Audit logs MUST be protected against unauthorized viewing, modification, and deletion. Audit logs  
981 SHALL only be deleted from a system after it has been archived.

982 **5.4.5 Audit Log Backup Procedures**

983 Audit logs SHALL be backed up. A copy of the audit log SHALL be stored at a separate facility from the active  
984 audit log as required.

985 **5.4.6 Audit Collection System (Internal vs. External)**

986 Automated audit processes SHALL be invoked at system (or application) startup, and cease only at system (or  
987 application) shutdown.

988 **5.4.7 Notification to Event-Causing Subject**

989 No stipulation.

990 **5.4.8 Vulnerability Assessments**

991 Trusted Roles SHALL routinely assess the CA system and its components for malicious activity.

992 **5.5 Records Archive**

993 **5.5.1 Types of Events Archived**

994 CA archive records SHALL be detailed enough to establish the validity of a signature and of the operation of the  
995 PKI. The following MUST be recorded at a minimum:

- 996 • CA accreditation;
- 997 • CPS;
- 998 • System equipment configuration;
- 999 • Modification and updates to system or configuration;
- 1000 • Contractual obligations;
- 1001 • Key Signing Ceremony video footage;
- 1002 • Certificate Subject identity authentication data from 3.1.9;
- 1003 • Documentation of receipt and acceptance of certificates;
- 1004 • Audit logs from Section 5.4.1;
- 1005 • All PKCs issued;
- 1006 • Other data or applications to verify archive contents; and,
- 1007 • Documentation required by compliance auditors.

1008 **5.5.2 Retention Period for Archive**

1009 Archive data SHALL be maintained for a minimum of the period of validity of all Certificates issued by CA plus  
1010 seven (7) years or such longer period as MAY be required by National Archive and Records Administration  
1011 (NARA).

1012 **5.5.3 Protection of Archive**

1013 Archive data SHALL be protected to ensure there is no unauthorized disclosure or modification. Archive media  
1014 SHALL be stored in a safe, secure storage facility separate from the CA itself.

1015 **5.5.4 Archive Backup Procedures**

1016 Archive facility SHALL support backups.

1017 **5.5.5 Requirements for Time-Stamping of Records**

1018 Archive data SHALL indicate the date on which the archive was created.

1019 **5.5.6 Archive Collection System (Internal or External)**

1020 No stipulation.

1021 **5.5.7 Procedures to Obtain and Verify Archive Information**

1022 WiMAX PA or designated representative MUST be granted timely access to archive information when requested.

1023 **5.6 Key Changeover**

1024 Server CAs MAY be renewed (Section 4.6) or re-keyed (Section 4.7) if the superior CA reconfirms the identity of  
1025 the CA, which the superior CA either accepts or rejects.

1026 Server Sub-CAs MAY be renewed (Section 4.6) or re-keyed (Section 4.7) if the superior CA reconfirms the identity  
1027 of the CA, which the superior CA either accepts or rejects.

1028 Re-keying is a multiparty procedure as specified in Section 5.2.2 and requires a "Key Ceremony" as specified in  
1029 Section 6.1.1.

1030 **5.7 Compromise and Disaster Recovery**

1031 **5.7.1 Incident and Compromise Handling Procedures**

1032 In the event of suspected compromise of a CA, it SHALL be investigated in order to determine the nature and the  
1033 degree of damage. If the CA PKC is compromised and the CA PKC is revoked, a new CA PKC MUST be issued  
1034 and the old CA PKC in RP trust stores MUST be replaced with a newly issued CA PKC. Server Root CA PKCs  
1035 will be distributed via secure out-of-band mechanism.

1036 **5.7.2 Computing Resources, Software, and/or Data Are Corrupted**

1037 Backup or Archived data MUST be used when computing resources, software, and data are corrupted.

1038 **5.7.3 CA Private Key Compromise Procedures**

1039 Compromised CA private keys MUST be revoked. Compromised CA private keys MUST NOT be used to sign new  
1040 PKCs. CA with compromised private keys MUST generate new private keys. Follow procedures in Section 5.3.6 if  
1041 the CA operator is suspected of compromising the CA's public key.

1042 **5.7.4 Business Continuity Capabilities After a Disaster**

1043 In the case of a disaster in which the CA equipment is damaged and inoperative:

- 1044 • The Server Root CA operations SHALL be established as quickly as possible, giving priority to the ability  
1045 to issue CA PKCs.
- 1046 • The CA operations SHALL be reestablished as quickly as possible, giving priority to the ability to issue  
1047 Certificate Subject PKCs.

1048 **5.8 CA and RA Termination**

1049 In the event a Root CA terminates, or ceases operation, the Root CA ships its HSM, which contains the Root CA's  
1050 private key, and any backup copies and archival copies to the WiMAX PA.

1051 In the event a Server or Server Sub CA terminates, or ceases operation, the CA ships its HSM, which contains the  
1052 CA's private key, and any backup copies and archival copies to the parent CA and the parent CA MUST only use  
1053 this key to issue CRLs.

1054 There is no stipulation for RAs.

## 1055 **6. Technical Security Controls**

1056 This chapter specifies the requirements for technical security controls to securely perform the functions of key  
1057 generation, subject authentication, PKC issuance, and PKC revocation.

### 1058 **6.1 Key Pair Generation and Installation**

1059 A Server certificate SHOULD be inserted into only one active production Server. Use of identical copies (same  
1060 name, serial number, key) of certificates in multiple active Servers in commercial networks is not  
1061 RECOMMENDED. This is not meant to preclude hot standby for redundancy, or copies for test systems.

1062 Multiple active production Servers serving the same NSPID/Domain Name SHOULD get multiple certificates.

1063 A Server MAY have multiple server certificates, e.g. if there are multiple DN handled by the server.

#### 1064 **6.1.1 Key Pair Generation**

1065 CA keys are generated in FIPS 140-2 validated cryptographic module. Modules SHALL meet security level 2 or  
1066 above and keys are generated as part of a multiparty operation. If the keys are generated outside the module, then  
1067 they SHALL be loaded into the module during a key ceremony. Any unencrypted copies of the keys SHALL be  
1068 destroyed after the key ceremony, while encrypted backups MAY exist at secured locations.

1069 Root Server CAs MUST be generated on removable a HSM device.

1070 Certificate Subject keys are generated in a FIPS 140-2 validated cryptographic module. Software cryptographic  
1071 modules SHALL meet Security Level 1 and hardware cryptographic modules SHALL meet Security Level 2.

#### 1072 **6.1.2 Private Key Delivery to Certificate Subject**

1073 If the Server does not generate its private key, then the private key MUST be delivered to the Server in a manner  
1074 that protects the private key from unauthorized disclosure and modification. See Section 3.2.1.

#### 1075 **6.1.3 Public Key Delivery to Certificate Issuer**

1076 A Certificate Subject's public key and identity SHALL be delivered securely to the CA in certification request.

#### 1077 **6.1.4 CA Public Key Delivery to Relying Parties**

1078 CA public keys SHALL be delivered to the RP as part of the certification response.

1079 The self-signed Server CA PKC SHALL be conveyed to relying parties in a secure fashion to preclude substitution  
1080 attacks.

#### 1081 **6.1.5 Key Sizes**

1082 Keys MUST be 1024 bits or longer. Keys which will be used past 2010 MUST be 2048 bits or longer. Shorter keys  
1083 MUST NOT be used to certify PKCs that contain longer keys.

#### 1084 **6.1.6 Public Key Parameters Generation and Quality Checking**

1085 See PKCS #1 for key generation requirements.

#### 1086 **6.1.7 Key Usage Purposes (as per X.509v3 key usage field)**

1087 See Section 7.

1088 **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

1089 **6.2.1 Cryptographic Module Standards and Controls**

1090 The relevant standard for cryptographic modules is FIPS PUB 140-2, Security Requirements for Cryptographic  
1091 Modules.

1092 **6.2.2 Private Key Multi-Person Control**

1093 Use of CA private keys requires action by multiple persons as set forth in Section 5.2.2 of this CP.

1094 There is no stipulation for Certificate Subject private keys.

1095 **6.2.3 Private Key Escrow**

1096 No stipulation.

1097 **6.2.4 Private Key Backup**

1098 CA private keys SHALL be backed up under multi-person control, as required in Section 5.2.2. No more than a  
1099 single copy of the signature key SHALL be stored at the CA's location (i.e., only the operational and backup key  
1100 MAY be stored at the CA's location). Additional copies MAY exist off-site provided that accountability for them is  
1101 maintained. This does not preclude the ability of the operator of a CA to explain in the CPS and get explicit  
1102 approval for a secure high-availability high-throughput system which parallelizes the operation among several  
1103 machines.

1104 Certificate Subject private keys SHALL be securely backed up.

1105 **6.2.5 Private Key Archival**

1106 No stipulation.

1107 **6.2.6 Private Key Transfer into or from a Cryptographic Module**

1108 CA private keys never leave the cryptographic module.

1109 Certificate Subject private keys that are not generated by the Certificate Subject MUST be transferred to Certificate  
1110 Subject in a manner that protects the key from unauthorized disclosure and modification. See Section 3.2.1.

1111 **6.2.7 Private Key Storage on Cryptographic Module**

1112 CA private keys SHALL be encrypted on removable memory storage devices.

1113 There is no stipulation for Certificate Subject private keys.

1114 **6.2.8 Method of Activating Private Keys**

1115 Activation of the CA signing key requires multiparty control, as specified in Section 5.2.2. The CA private key  
1116 media SHALL NOT be left unattended when active.

1117 There is no stipulation for activation of Certificate Subject private keys.

1118 **6.2.9 Methods of Deactivating Private Keys**

1119 Root CA private keys SHALL be deactivated and the media holding the Root CA private key SHALL be stored in a  
1120 secure container (see Section 5.1.6). CA private keys SHALL be deactivated and stored in encrypted form in a  
1121 secure room when not in use (see Section 5.1.6). These actions requires multiparty control, as specified in Section 5  
1122 2.2. The Root CA and CA private key media SHALL NOT be left unattended when not in use.

1123 There is no stipulation for deactivation of Certificate Subject private keys.

1124 **6.2.10 Method of Destroying Private Key**

1125 Private keys SHALL be destroyed when they are no longer needed or when the PKC to which they corresponds  
1126 expires or is revoked.

1127 **6.2.11 Cryptographic Module Rating**

1128 See Section 6.2.1.

1129 **6.3 Other Aspects of Key Management**

1130 **6.3.1 Public Key Archival**

1131 Public keys SHALL be archived as part of the PKC archival.

1132 **6.3.2 Certificate Operational Periods/Key Usage Periods**

1133 Server Root CA certificate lifetimes SHALL be limited to 45 years or less. Server CA and Server Sub-CAs  
1134 certificates SHALL be limited to 30 years or less. Server certificates SHALL be limited to 1 years or less.

1135 **6.4 Activation Data**

1136 **6.4.1 Activation Data Generation and Installation**

1137 Activation data generation and installation for CA private keys SHALL use methods that protect the activation data  
1138 to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such  
1139 private keys.

1140 There is no stipulation for Certificate Subject private keys.

1141 **6.4.2 Activation Data Protection**

1142 Activation data to invoke private keys SHALL be protected from disclosure by a combination of cryptographic and  
1143 physical access control mechanisms. The protection mechanism SHALL include a facility to temporarily lock the  
1144 account, or terminate the application, after 3 failed login attempts.

1145 **6.4.3 Other Aspects of Activation Data**

1146 Before the Root CA private key activation data MAY be enter, the media storing the Root CA's private key MUST  
1147 be retrieved from the locked container.

1148 No stipulation for Server CAs, Server Sub-CAs, or Certificate Subjects.

1149 **6.5 Computer Security Controls**

1150 **6.5.1 Specific Computer Security Technical Requirements**

1151 For the CA, the computer security functions listed below are required. These functions MAY be provided by the  
1152 operating system, or through a combination of operating system, software, and physical safeguards. The CA and its  
1153 ancillary parts SHALL include the following functionality:

- 1154 • Require authenticated logins;
- 1155 • Provide Discretionary Access Control;
- 1156 • Provide a security audit capability;
- 1157 • Restrict access control to Trusted Roles;
- 1158 • Enforce separation of Trusted Roles;
- 1159 • Require identification and authentication;
- 1160 • Restrict CA application to be the only application running on computer;
- 1161 • Require use of cryptography for session communications and database security;
- 1162 • Archive CA history and audit data; and,
- 1163 • Require a recovery mechanism for keys, CA system, and CA application.

1164 **6.5.2 Computer Security Rating**

1165 No Stipulation.

## 1166 **6.6 Life-Cycle Security Controls**

### 1167 **6.6.1 System Development Controls**

1168 The System Development Controls for the CA are as follows:

- 1169 • For commercial off-the-shelf software, the software SHALL be designed and developed under a formal,  
1170 documented development methodology.
- 1171 • For hardware and software developed specifically for a particular CA, the applicant SHALL demonstrate  
1172 that security requirements were achieved through a combination of software verification & validation,  
1173 structure.
- 1174 • Where open source software has been utilized, the applicant SHALL demonstrate that security  
1175 requirements were achieved through software verification & validation and structured development/life-  
1176 cycle management.
- 1177 • Hardware and software procured to operate the CA SHALL be purchased and shipped in a fashion to  
1178 reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment  
1179 was randomly selected at time of purchase).
- 1180 • The CA software SHALL be dedicated to performing one task: the CA. There SHALL be no other  
1181 applications; hardware devices, network connections, or component software installed which are not part of  
1182 the CA operation.
- 1183 • Proper care SHALL be taken to prevent malicious software from being loaded onto the CA equipment.  
1184 Hardware and software SHALL be scanned for malicious code on first use and periodically thereafter.
- 1185 • Hardware and software updates SHALL be purchased or developed in the same manner as original  
1186 equipment, and be installed by trusted and trained personnel in a defined manner.
- 1187 • Any code return to open source community does not disclose security relevant information.

### 1188 **6.6.2 Security Management Controls**

1189 The configuration of the CA system as well as any modifications and upgrades SHALL be documented and  
1190 controlled. There SHALL be a mechanism for detecting unauthorized modification to the CA software or  
1191 configuration. A formal configuration management methodology SHALL be used for installation and ongoing  
1192 maintenance of the CA system.

### 1193 **6.6.3 Life Cycle Security Ratings**

1194 No stipulation.

## 1195 **6.7 Network Security Controls**

1196 CAs SHALL be protected prevent unauthorized access, tampering, and denial-of-service. Communications of  
1197 sensitive information SHALL be protected using point-to-point encryption for confidentiality and digital signatures  
1198 for non-repudiation and authentication.

1199 Server Root CAs SHOULD be offline. Permanently online Server Root CAs will need to explain why they are  
1200 always online in their CPS.

1201 **6.8 Time Stamping**

1202 Times asserted in PKCs SHALL be accurate to within three minutes. Electronic or manual procedures MAY be  
1203 used to maintain system time. Clock adjustments are auditable events (See Section 5.4.1).

1204 There is no trusted time source.

## 1205 **7. Certificate, CARL/CRL, And OCSP profiles Format**

1206 This Chapter specifies the requirements for the PKC, CRL, and OCSP format.

### 1207 **7.1 Certificate Profile**

1208 See WiMAX Forum PKC Profile Release 1.0.

### 1209 **7.2 CRL Profile**

1210 See WiMAX Forum CRL Profile Release 1.0.

### 1211 **7.3 OCSP Profile**

1212 See WiMAX Forum OCSP Profile Release 1.0.

### 1213 **7.4 SCVP Profile**

1214 A WiMAX Forum SCVP profile will be developed when the need arises.

## 1215 **8. Compliance Audit and Other Assessments**

1216 This chapter specifies the requirements for audits.

### 1217 **8.1 Frequency of Audit or Assessments**

1218 CAs are subject to a compliance audit at least once per year.

### 1219 **8.2 Identity and Qualifications of Assessor**

1220 The auditor **MUST** demonstrate competence in the field of compliance audits. The PA **SHALL** identify the  
1221 compliance auditor for the CA.

### 1222 **8.3 Assessor's Relationship to Assessed Entity**

1223 The compliance auditor either **SHALL** be a private firm, that is independent from the entity being audited, or it  
1224 **SHALL** be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

1225 The PA **SHALL** determine whether a compliance auditor meets this requirement.

### 1226 **8.4 Topics Covered By Assessment**

1227 The compliance audit of the CA **SHALL** verify that the CA is implementing all provisions of a CP approved by the  
1228 PA.

### 1229 **8.5 Actions Taken As A Result of Deficiency**

1230 Any discrepancies between how the CA is designed to or is being operated or maintained and the requirements of  
1231 this CP will result in the compliance auditor documenting the discrepancy.

### 1232 **8.6 Communication of Results**

1233 Upon completion, the audit compliance report will be returned to the PA. The report **SHALL** be treated as company  
1234 confidential. The report **SHALL** identify the versions of the CP used in the assessment.

## 1235 **9. Other Business and Legal Matters**

1236 This chapter specifies requirements on general business and legal matters.

### 1237 **9.1 Fees**

1238 Any fees **MUST** be approved by the WiMAX PA.

#### 1239 **9.1.1 Certificate Issuance/Renewal Fees**

1240 Any fees **MUST** be approved by the WiMAX PA.

#### 1241 **9.1.2 Certificate Access Fees**

1242 Any fees **MUST** be approved by the WiMAX PA.

#### 1243 **9.1.3 Revocation or Status Information Access Fee**

1244 Any fees **MUST** be approved by the WiMAX PA.

#### 1245 **9.1.4 Fees for other Services**

1246 Any fees **MUST** be approved by the WiMAX PA.

#### 1247 **9.1.5 Refund Policy**

1248 Any refund policy **MUST** be approved by the WiMAX PA.

### 1249 **9.2 Financial Responsibility**

1250 CA **MUST** have assets and resources that ensure an ability to provide meet all operational requirements as a CA on  
1251 an uninterrupted basis and to pay damages that could reasonably occur as a result of CA operations. Levels **MUST**  
1252 be reasonably acceptable to WiMAX PA.

#### 1253 **9.2.1 Insurance Coverage**

1254 Server Root CA must obtain insurance coverage obtained from a reputable financially sound insurer with  
1255 appropriate policy limits that is equal to or exceeds industry norms. The WiMAX Forum will be named as an  
1256 additional insured. Insurance carrier and coverage **MUST** be acceptable to WiMAX PA.

1257 No stipulation regarding insurance requirements for Server CA and Server Sub-CA.

#### 1258 **9.2.2 Other Assets**

1259 No stipulation.

#### 1260 **9.2.3 Insurance/warranty Coverage for End-Entities**

1261 No stipulation.

1262 **9.3 Confidentiality of Business Information**

1263 Sensitive and confidential information will be exchanged and provided under this CP. Written confidential  
1264 information SHALL be adequately marked in writing as confidential. Oral confidential information SHALL be  
1265 identified as confidential.

1266 **9.3.1 Scope of Confidential Information**

1267 Confidential Information means all information in written or oral form that the disclosing party identifies as  
1268 confidential, and any trade secret or other proprietary information that the recipient knows or reasonably ought to  
1269 know SHOULD be treated as confidential.

1270 **9.3.2 Information Not Within the Scope of Confidential Information**

1271 Information that is not Confidential Information includes information that is generally known to the public or  
1272 properly known by the receiving party at the time of disclosure and other typical exceptions.

1273 **9.3.3 Responsibility to Protect Confidential Information**

1274 The PA and CAs MUST protect confidential information from unauthorized disclosure.

1275 **9.4 Privacy of Personal Information**

1276 It is the responsibility of all parties to ensure privacy of personal information under their control. No personal  
1277 information is registered or certified. Information about subordinate CA operators is retained by the CA as part of  
1278 certification request, which is subsequently logged and later archived. Manufacturer point of contact information is  
1279 also retained by the Root CAs. If a party collects, transmits or stores personal information, its practices will comply  
1280 with all applicable laws.

1281 **9.4.1 Privacy Plan**

1282 A privacy plan SHALL manage relevant information. Sponsor contact information SHALL be stored in a secure  
1283 container.

1284 **9.4.2 Information Treated as Private**

1285 CA operator's name, organizational affiliation, and phone number and other information within that definition.

1286 **9.4.3 Information Not Deemed Private**

1287 CP, CPS, PKCs, and revocation information are not considered private information.

1288 **9.4.4 Responsibility to Protect Private Information**

1289 All parties will protect private information when it is within their control.

1290 **9.4.5 Notice and Consent to use Private Information**

1291 Notice and consent practices regarding private information MUST comply with any applicable law.

1292 **9.4.6 Disclosure Pursuant to Judicial/Administrative Process**

1293 Disclosure in response to a valid judicial or administrative order MUST be permitted.

1294 **9.4.7 Other Information Disclosure Circumstances**

1295 Except as required for operation of the PKI system, as expressly permitted or required under the CP, or as required  
1296 by applicable law, no private information will be disclosed without the express written consent of the party to which  
1297 that private information pertains.

1298 **9.5 Intellectual Property Rights**

1299 The CP, CPS, each root certificate and all certificates issued under the root certificate are the property of the  
1300 WiMAX Forum.

1301 No party will use any property of the WiMAX Forum, including, without limitation, any trademark, copyright, trade  
1302 secret or other proprietary right of the WiMAX Forum, unless the WiMAX Forum has licensed that use.

1303 No party will infringe the intellectual property rights of any third party or the WiMAX Forum. Without limitation,  
1304 except as the WiMAX Forum MAY expressly authorize in writing, it is prohibited to:

- 1305 • Reverse engineer, translate, disassemble, decompile the whole or any part of any software or system or any  
1306 part therefore or otherwise attempt to access any software source code embedded in or operating using any  
1307 system;
- 1308 • Assign, transfer, sell, license, sub-license, lease, rent, charge or otherwise deal in or encumber any software  
1309 or system or any part thereof or use same on behalf of or for the benefit of any third party, or make  
1310 available the same in any way whatsoever to any third party without the WiMAX Forum's prior written  
1311 consent;
- 1312 • Remove or alter any trademark or any copyright or other proprietary notice on any software, system or any  
1313 other materials;
- 1314 • Distribute, create derivative works of or modify any materials, software or system or any part thereof in any  
1315 way, or use, copy, duplicate or display same on a commercial or development basis.
- 1316 • Provide any service using a certificate provided under this CP except as authorized and provided in this CP  
1317 and an approved CPS.

1318 These restrictions SHALL NOT be construed in a manner that would violate any applicable law.

1319 **9.6 Representations and Warranties**

1320 The obligations described below pertain to the WiMAX PKI Participants. The obligations applying to CAs pertain  
1321 to their activities as issuers of PKCs.

1322 **9.6.1 PA / WiMAX Forum**

1323 The WiMAX Forum and the PA make no representations and disclaim all warranties, however characterized, to the  
1324 maximum extent permitted by law. The CP notice and disclaimer terms on page [i] above.

1325 **9.6.2 Generally Applicable Representations and Warranties**

1326 Agreements involving CA's, RA's, Subscribers, and Relying Parties will include standard representations and  
1327 warranties:

- 1328 • It has full right, power and authority to enter into the agreement and there is nothing that would prevent it  
1329 from performing its obligations under the terms and conditions imposed on it by the agreement.
- 1330 • The agreement has been duly authorized by all necessary corporate action and constitutes a valid and  
1331 binding obligation on it, enforceable in accordance with the terms hereof (except to the extent of any relief  
1332 that MAY be afforded under the laws of bankruptcy or under general principles of equity).
- 1333 • If it is an entity: It is a [corporation] duly organized and validly existing and in good standing under the  
1334 laws of its jurisdiction of incorporation and is duly qualified and authorized to do business wherever the  
1335 nature of its activities or properties requires such qualification or authorization.
- 1336 • No registration with or approval of any government agency or commission of any jurisdiction is necessary  
1337 for the execution, delivery or performance by it of any of the terms of the agreement, or for the validity and  
1338 enforceability hereof or with respect to its obligations under the agreement.
- 1339 • There is no provision in its company or corporate charter, articles of incorporation, Bylaws or equivalent  
1340 governing documents, and no provision in any existing mortgage, indenture, contract or agreement binding  
1341 on it, which would be contravened by the execution, delivery or performance by it of the agreement.
- 1342 • No consent of any third party or holder of any of its indebtedness is or SHALL be required as a condition to  
1343 the validity of the agreement.
- 1344 • Neither its execution nor its delivery of the agreement nor its fulfillment of or compliance with the terms  
1345 and provisions hereof SHALL contravene any provision of the laws of any jurisdiction including, without  
1346 limitation, any statute, rule, regulation, judgment, decree, order, franchise or permit applicable to it.

1347 **9.6.3 CA Representations and Warranties**

1348 CAs warrant that:

- 1349 • There are no material misrepresentations of fact in the PKC known to or originating from the entities  
1350 approving the Certificate Application or issuing the Certificate,
- 1351 • There are no errors in the information in the PKC that were introduced by the entities approving the  
1352 Certificate Application or issuing the PKC as a result of a failure to exercise reasonable care in managing  
1353 the Certificate Application or creating the PKC,
- 1354 • Their PKCs meet all material requirements of this CP and the applicable CPS, and
- 1355 • Revocation services and use of a repository conform to all material requirements of this CP and the  
1356 applicable CPS in all material aspects.
- 1357 • It will perform all services in a professional and workmanlike manner and in conformity with standards that  
1358 equal or exceed industry norms for the services that it is providing.

1359 **9.6.4 RA Representations and Warranties**

1360 In addition to the generally applicable representations and warranties in Section 9.6.2, RA's MUST make the same  
1361 warranties as CA's with respect to any service that is delegated from the CA.

1362 **9.6.5 Certificate Subject Representations and Warranties**

1363 Certificate Subjects SHALL:

- 1364 • Use their private key and PKC for uses, in accordance with this CP (see Section 1.4).
- 1365 • Protect the confidentiality of their private keys at all times, in accordance with this CP.

1366 **9.6.6 Relying Parties Representations and Warranties**

1367 Relying Parties SHALL:

- 1368 • Use the PKC for uses, in accordance with this CP (see Section 1.4).

1369 **9.6.7 Representations and Warranties of Other Participants**

1370 No stipulation.

1371 **9.7 Disclaimers of Warranties**

1372 Disclaimers of implied warranties MAY be included. No disclaimer MAY contradict a required express warranty.

1373 **9.8 Limitations of Liability**

1374 **9.8.1 PA / WiMAX Forum**

1375 In no event is the PA or WiMAX Forum liable for any losses, liabilities, or damages, whether direct or indirect and  
1376 however characterized.

1377 **9.8.2 Other Participants.**

1378 Mutual limitations of liability that exclude liability for special, indirect, incidental and consequential damages MAY  
1379 be included. An agreement MAY NOT impose a specific liability limit such as, for example, limiting a party's  
1380 liability to the value of the fees paid or some multiple thereof.

1381 **9.9 Indemnities**

1382 **9.9.1 PA / WiMAX Forum**

1383 The WiMAX will not indemnify any party. The WiMAX Forum will be indemnified against third-party claims  
1384 arising from or relating to use of the PKI system and any related services, systems, software or materials.

1385 **9.9.2 Other Participants.**

1386 The agreements MUST have standard commercial indemnities covering the breach of the CP or an applicable CPS,  
1387 infringement of third-party proprietary rights, breaches of nondisclosure obligations, and damages resulting from a  
1388 party's breach of a representation, warranty, or material obligation under the agreement

1389 **9.10 Term and Termination**

1390 **9.10.1 Term**

1391 **9.10.1.1 CP Term**

1392 The CP becomes effective when the PA approves it and SHALL continue until the PA terminates it.

1393 **9.10.1.2 Other Agreements**

1394 No stipulation provided that the term is reasonable for the services to be provided. The WiMAX PA will resolve  
1395 any disagreement.

1396 **9.10.2 Termination**

1397 **9.10.2.1 CP Termination**

1398 Termination of the CP is at the discretion of the PA. The CP remains in force until such time as WiMAX PA  
1399 terminates it.

1400 **9.10.2.2 Other Agreements**

1401 Termination for material breach, bankruptcy or insolvency, and upon expiration of a fixed term is permitted. A  
1402 service provider MAY NOT terminate for convenience.

1403 Termination of this CP is at the discretion of the PA. The CP remains in force until such time as it is replaced by a  
1404 new version or it is terminated by the WiMAX PA.

1405 **9.10.3 Effect of Termination and Survival**

1406 **9.10.3.1 CP**

1407 Upon termination of this CP, WiMAX PKI participants are nevertheless bound by the terms of the CP for all PKCs  
1408 issued for the remainder of the validity periods of such PKCs.

1409 **9.10.3.2 Other Agreements**

1410 No stipulation except that provisions relating to the following CP provisions MUST survive: 5.5 (to the extent  
1411 required pursuant to Sections 5.5.2 and 9.10.3.1), 9.3, 9.4, 9.5, 9.7, 9.8, 9.9, and 9.10.3.1.

1412 **9.11 Individual Notices and Communications With participants**

1413 No stipulation.

1414 **9.12 Amendments**

1415 **9.12.1 Procedure for Amendment**

1416 **9.12.1.1 CP**

1417 The WiMAX PA MAY amend the CP in its sole discretion. The WiMAX PA MAY issue amendments,  
1418 clarifications, or an update.

1419 **9.12.1.2 CPS and Participant Agreements.**

1420 Other participants will amend the CPS, which is provided by the CA operator, and other agreements to conform  
1421 them to amendments to the CP.

1422 **9.12.2 Notification Mechanism and Period**

1423 The CP and any subsequent changes SHALL be made available the WiMAX PKI participants via the publically  
1424 available repository.

1425 **9.12.3 Circumstances Under Which OID Must Be Changed**

1426 The object identifier representing the CP will be changed if significant changes are made to the CP portions of this  
1427 document.

1428 **9.13 Dispute Resolution Provisions**

1429 Any dispute arising with respect to this policy or PKCs issued under this policy is addressed by the PA. All  
1430 determinations of the PA are final.

1431 **9.14 Governing Law**

1432 All parties SHALL comply with all laws, rules, regulations and orders that are applicable to them.

1433 **9.15 Compliance with Applicable Law**

1434 This CP SHALL comply with the laws of the State of California Law and the United States of America.

1435 **9.16 Miscellaneous Provisions**

1436 **9.16.1 Document Incorporated into CP**

1437 The following documents also apply:

- 1438 • NWG Rel 1.0 Stage 3 Specification: [http://www.wimaxforum.org/technology/documents/WiMAX\\_End-to-](http://www.wimaxforum.org/technology/documents/WiMAX_End-to-End_Network_Systems_Architecture_Stage_2-3_Release_1.1.0.zip)  
1439 [End\\_Network\\_Systems\\_Architecture\\_Stage\\_2-3\\_Release\\_1.1.0.zip](http://www.wimaxforum.org/technology/documents/WiMAX_End-to-End_Network_Systems_Architecture_Stage_2-3_Release_1.1.0.zip)
- 1440 • RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices  
1441 Framework <http://www.ietf.org/rfc/rfc3647.txt>
- 1442 • FIPS 140-2 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES  
1443 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- 1444 • IEEE 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and  
1445 Mobile Operation in Licensed Bands
- 1446 • WiMAX Forum Server Certificate Profile Version 1.0.0
- 1447 • WiMAX Forum CRL Profile Version 1.0.0
- 1448 • WiMAX Forum OCSP Profile Version 1.0.0

1449 **9.16.2 Entire agreement**

1450 No stipulation.

1451 **9.16.3 Assignment**

1452 No stipulation.

1453 **9.16.4 Severability**

1454 No stipulation.

1455 **9.16.5 Waiver**

1456 No stipulation.

1457 **9.16.6 Attorneys' Fees**

1458 Participants SHALL reimburse the WiMAX Forum for all fees, expenses, and costs that it incurs in enforcing the  
1459 terms of the CP.

1460 **9.16.7 Force Majeure**

1461 Optional. If included, force majeure period SHOULD NOT exceed 60 days.

1462 **9.17 Other Provisions**

1463 No stipulation