



WiMAX Forum X.509 Device Certificate Profile Approved Specification

Version 1.1.0

June 3rd, 2009

WiMAX Forum Proprietary

Copyright © 2009 WiMAX Forum. All Rights Reserved.

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

Copyright 2009 WiMAX Forum. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

1 **Table of Contents**

2 **1. INTRODUCTION AND SCOPE 6**

3 1.1 Terminology 6

4 **2. REFERENCES 7**

5 **3. ABBREVIATIONS AND DEFINITIONS..... 8**

6 **4. ASSUMPTIONS 9**

7 **5. CERTIFICATES 10**

8 5.1 WiMAX Device Root CA Certificate Profile 11

9 5.1.1 *WiMAX Device Root CA Certificate Field Requirements* 11

10 5.2 WiMAX Device Manufacturer CA and Device Sub-CA Certificate Profile 13

11 5.2.1 *WiMAX Device Manufacturer CA and Sub-CA Certificate Field Requirements* 13

12 5.3 WiMAX Device Certificate Profile 15

13 5.3.1 *Wimax Device Chain SS Device Certificate Field Requirements* 15

14 5.4 Field Requirements Common to all WiMAX Certificates 17

15 5.4.1 *Version* 17

16 5.4.2 *serialNumber* 17

17 5.4.3 *Signature* 17

18 5.4.4 *issuer* 17

19 5.4.5 *notBefore* 17

20 5.4.6 *subjectPublicKeyInfo* 17

21 5.4.7 *signatureAlgorithm* 17

22 5.4.8 *signatureValue* 17

23 5.4.9 *authorityKeyIdentifier Extension* 17

24 5.4.10 *AuthorityInfoAccessSyntax Extension* 17

25 5.4.11 *SubjectInfoAccessSyntax Extension* 17

26

27

1 **List of Figures**

2 FIGURE 5-1 – LENGTH 3 AND 4 DEVICE CERTIFICATE CHAINS FOR 2 AND 3 LEVEL CA TREES 10

3

4

1 **List of Tables**

2 TABLE 5-1 – FIELDS REQUIRED IN WIMAX DEVICE ROOT CERTIFICATES 11
3 TABLE 5-2 – EXTENSIONS REQUIRED IN WIMAX ROOT CA CERTIFICATES 11
4 TABLE 5-3 – FIELDS REQUIRED IN WIMAX DEVICE MANUFACTURER CA AND SUB-CA
5 CERTIFICATES 13
6 TABLE 5-4 – EXTENSIONS REQUIRED IN WIMAX SUBORDINATE AND LOWER SUBORDINATE CA
7 CERTIFICATE 13
8 TABLE 5-5 – FIELDS REQUIRED IN WIMAX DEVICE CERTIFICATE 15
9 TABLE 5-6 – EXTENSIONS REQUIRED IN WIMAX SS DEVICE CERTIFICATE 15
10 TABLE 5-7 – OPTIONAL EXTENSIONS PERMITTED IN WIMAX SS DEVICE CERTIFICATES 16

11

1 Revision History

October 29, 2007	Initial draft
December 5, 2007	V&V Changes Incorporated
January 27, 2008	Editorial change: allow use printable string in MAC address and manufacturer name
February 28, 2008	Editorial proofreading and cleanup.
March 6, 2008	Clarifications in Sect. 5.4.6 and 5.4.8. Removed restriction on pathLenConstraint for root CA (for consistency with server profile)
March 31, 2008	Headers fix and DN disambiguation. Refer to RFC 5216 as EAP-TLS spec. Sorted abbreviations alphabetically. Fixed copyright year to 2008.
April 8, 2008	Release 1.0. Changed headers to reflect approved release.
April 18, 2008	Changed title and headers to reflect draft spec.
June 3, 2009	Updated CRLDP text in Tables 5-4 and in section 5.2.1.3.2. Update AIA text in Tables 5-5 and 5-7 and in section 5.4.10. Added notes in 5.2.1 and 5.3.1 about other non-critical extensions. Renumbered tables 1-7. Deleted reference to 3279 and added references RFC 3986, 3647, 2119, and 4055.

1. Introduction and Scope

The purpose of this document is to specify the format of the X.509 Device and Certificate Authority (CA) certificates used by WiMAX.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below, taken from IETF RFC 2119 [9].

Note that the force of these words is modified by the requirement level of the document in which they are used.

- **MUST:** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT:** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- **SHOULD:** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

2. References

- 1 [1] IEEE 802.16-2004 October 2004, Air Interface for Fixed Broadband Wireless Access Systems
- 2 [2] IEEE 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and Mobile
- 3 Operation in Licensed Bands
- 4 [3] IEEE 802-2001 March 2002, IEEE Standard for Local and Metropolitan Networks: Overview and Architecture
- 5 [4] RFC 5216, The EAP TLS Authentication Protocol
- 6 [5] RFC 5480, Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile
- 7 [6] RFC 4043, Internet X.509 Public Key Infrastructure, Permanent Identifier
- 8 [7] RFC 3986, Uniform Resource Identifier (URI): Generic Syntax
- 9 [8] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- 10 [9] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels
- 11 [10] RFC 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public
- 12 Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- 13

1 **3. Abbreviations and Definitions**

2	AIA	Authority Information Access
3	CA	Cartification Authority
4	CRL	Certificate Revocation List
5	DoS	Denial-of-service
6	DN	Distinguished Name
7	FIPS	Federal Information Processing Standards
8	NIST	National Institute of Standards and Technology
9	OID	Object Identifier
10	RDN	Relative Distinguished Name
11	RFC	Request for Comments
12	SIA	Subject Information Access
13	SKU	Stock Keeping Unit
14	SS	Subscriber Station
15	URI	Uniform Resource Identifier
16	URL	Uniform Resource Locator

1 **4. Assumptions**

2 Each SS need not attain WiMAX Forum Certified™ status. Such status can be determined by accessing public
3 information for the particular model number. For the purposes of this document and Release 1.0 network
4 specification, this issue is not particularly relevant. It is assumed that determination of such status and consequent
5 actions are outside the scope of the Release 1.0 Stage 2/3 specification.

5. Certificates

This section describes the fields of certificates in the WiMAX device certificate chain.

The WiMAX certificate hierarchy assumes a two or three level tree that is rooted in the WiMAX Root CA, with subordinate CA for each of the device manufacturers and, optionally, one more lower subordinate CA for each manufacturing site that may perform local issuance of certificates at the time of manufacture.

Device Certificates and server certificates SHALL be issued by separate CAs and SHALL terminate at separate trust anchor public keys.

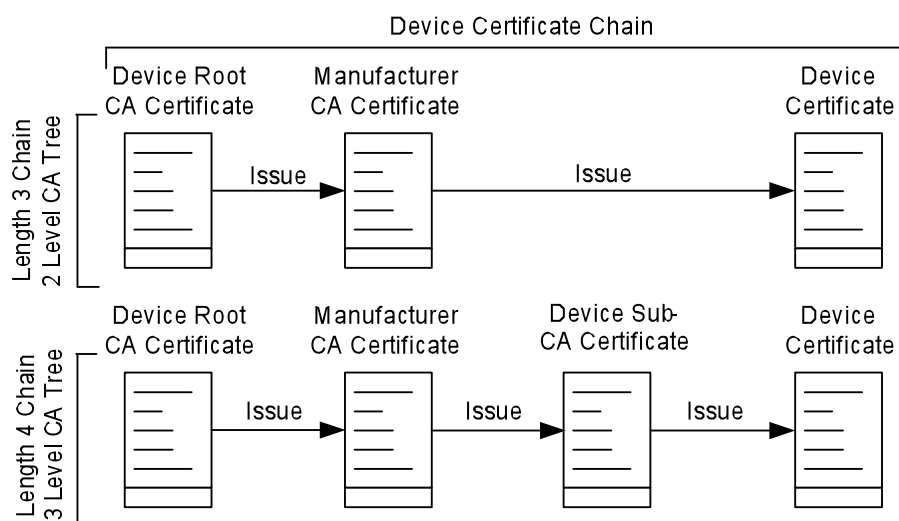


Figure 5-1 – Length 3 and 4 Device Certificate Chains for 2 and 3 level CA trees

WiMAX certificates SHALL be constructed in accordance with IETF RFC 5480 [5] and the type definitions and default values provided in [5] are implicitly incorporated here except where explicitly overridden in this clause.

All of the following certificates have the following common attributes:

- All certificates SHALL be version 3 X.509 certificates.
- The Certificate signature algorithm SHALL be SHA-256 with RSA encryption as defined in RFC 4055 [10] (PKCS#1 v1.5).
- All certified RSA public keys (including those of Root CAs, Manufacturer CAs, Sub CAs and devices) SHALL have RSA public key exponent $e = 65537$.
 - This allows for significant computational savings both on the MS and HAAA. Additionally, this mitigates variants of DoS attack targeting CPU capacity of HAAA. The use of $e = 65537$ is recommended by NIST draft FIPS PUB 186-3 (March 2006).
- To reduce over the air transmission costs and fragmentation, AIA (Authority Information Access) section 4.2.2.1 of RFC 5480 [5] and SIA (Subject Information Access) 4.2.2.2 MAY be employed in non root certificates. AIA and SIA both SHALL use the id-ad-caIssuers access method as specified in RFC 5480 [5]. The implication is that WiMAX forum will have to make the WiMAX CA certificate available at a well known URI. Root Certificates SHALL NOT use AIA or SIA.

5.1 WiMAX Device Root CA Certificate Profile

The WiMAX Device Root CA Certificate format is defined in RFC 5480 [5], with additional requirements described in 5.1.1 and 5.4.

5.1.1 WiMAX Device Root CA Certificate Field Requirements

A WiMAX root CA certificate SHALL include the fields in Table 1.

Table 1 – Fields Required in WiMAX Device Root Certificates

Field Name	RFC5480 type	Value	Reference
<i>TBSCertificate</i> {	SEQUENCE	Certificate contents	N/A
<i>version</i>	INTEGER	v3	5.4.1
<i>serialNumber</i>	INTEGER	Unique positive integer	5.4.2
<i>signature</i>	AlgorithmIdentifier	See 5.4.3	5.4.3
<i>issuer</i>	Name	Name of issuing CA	5.1.1.2
<i>validity</i> {	SEQUENCE	<i>notBefore</i> and <i>notAfter</i>	
<i>notBefore</i>	Time	Date on which the certificate validity period begins	5.4.5
<i>notAfter</i>	Time	Date on which the certificate validity period ends.	5.1.1.1
}			
<i>subject</i>	Name	Name of Issuing CA	5.1.1.2
<i>subjectPublicKeyInfo</i>	SubjectPublicKeyInfo	The 1024 or 2048 bit credential public key and algorithm identifier	5.4.6
<i>extensions</i>	Extensions	See 5.1.1.3	5.1.1.3
}			
<i>signatureAlgorithm</i>	AlgorithmIdentifier	See 5.4.7	5.4.7
<i>signatureValue</i>	BIT STRING	Certificate Signature	5.4.8

Except where otherwise noted in Table 2, the Extensions field SHALL contain the extensions shown in Table 2.

Table 2 – Extensions Required in WiMAX Root CA Certificates

Extension Name	Critical	Contents	Reference
<i>authorityKeyIdentifier</i>	N	KeyIdentifier Equal to the issuer's subjectKeyIdentifier field This extension MAY be omitted in self signed root certificates, as per 4.2.1.1 of RFC 5480.	5.4.9
<i>keyUsage</i>	Y	060x (bits 5 & 6 - keyCertSign & cRLSign)	5.1.1.3.1
<i>subjectKeyIdentifier</i>	N	<i>subjectKeyIdentifier</i> SHALL be generated using RFC 5480 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the issuer's public key.	5.1.1.3.2
<i>basicConstraints</i>	Y	cA=true	5.1.1.3.3

A WiMAX device certificate SHALL NOT include any additional critical extensions.

1 **5.1.1.1 notAfter**

2 The difference between the *notBefore* and *notAfter* fields determines the lifetime of the certificate.

3 **5.1.1.2 issuer and subject Names**

4 *subject* contains a valid DN, conformant with RFC 5480 [5], identifying the device root CA. The subject DN and
5 issuer DN are identical for a self-signed root certificate.

6 **5.1.1.3 extensions**

7 The *extensions* field in WiMAX certificates contains a number of required and optional extension fields described
8 below.

9 **5.1.1.3.1 keyUsage**

10 The *keyUsage* extension field SHALL be present.

11 The *keyUsage* extension field SHALL have bits set for 5 and 6 set for *keyCertSign* and *cRLSign*.

12 The *keyUsage* extension field SHALL be critical.

13 **5.1.1.3.2 subjectKeyIdentifier**

14 *subjectKeyIdentifier* SHALL be present.

15 *subjectKeyIdentifier* SHALL be generated using RFC 5480 [5] 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the
16 issuer's public key.

17 **5.1.1.3.3 basicConstraints**

18 The *basicConstraints* extension field SHALL be present.

19 The *basicConstraints* extension SHALL be marked critical.

20 The *cA* bit SHALL be true.

21

22

1

2 **5.2 WiMAX Device Manufacturer CA and Device Sub-CA Certificate Profile**

3 The WiMAX Subordinate CA Certificate format is defined in RFC 5480 [5], with additional requirements described
4 in 5.2.1 and 5.4. It covers both Device Manufacturer CA certificates and Device Manufacturer Sub-CA certificates.

5 **5.2.1 WiMAX Device Manufacturer CA and Sub-CA Certificate Field Requirements**

6 A WiMAX subordinate CA certificate SHALL include the fields in Table 3.

7 **Table 3 – Fields Required in WiMAX Device Manufacturer CA and Sub-CA Certificates**

Field Name	RFC 5480 type	Value	Referenc e
<i>TBSCertificate</i> {	SEQUENCE	Certificate contents	N/A
<i>version</i>	INTEGER	v3	5.4.1
<i>serialNumber</i>	INTEGER	Unique positive integer	5.4.2
<i>signature</i>	AlgorithmIdentifier	See 5.4.3	5.4.3
<i>issuer</i>	Name	Name of issuing CA	5.4.4
<i>validity</i> {	SEQUENCE	notBefore and notAfter	
<i>notBefore</i>	Time	Date on which the certificate validity period begins	5.4.5
<i>notAfter</i>	Time	Date on which the certificate validity period ends.	5.2.1.1
}			
<i>subject</i>	Name	Name of the Subject CA	5.2.1.2
<i>subjectPublicKeyInfo</i>	SubjectPublicKeyInfo	The 1024 or 2048 bit credential public key and algorithm identifier	5.4.6
<i>extensions</i>	Extensions	See 5.2.1.3	5.2.1.3
}			
<i>signatureAlgorithm</i>	AlgorithmIdentifier	See 5.4.7	5.4.7
<i>signatureValue</i>	BIT STRING	Certificate Signature	5.4.8

8

9 Except where otherwise noted in Table 4, the Extensions field SHALL contain the extensions shown in Table 4.

10 **Table 4 – Extensions Required in WiMAX Device Manufacturer CA and Sub-CA Certificates**

Extension Name	Critical	Contents	Reference
<i>authorityKeyIdentifier</i>	N	KeyIdentifier Equal to the issuer's subjectKeyIdentifier field	5.4.9
<i>keyUsage</i>	Y	060x (bits 5 & 6 - keyCertSign & cRLSign)	5.2.1.3.1
<i>cRLDistributionPoints</i>	N	Only distributionPoint with fullName choice. Contains HTTP pointer to location of CRL: Manufacturer CA: <URL to Root's CRL> Device Sub-CA: <URL to Manufacturer CA's CRL>	5.2.1.3.2
<i>subjectKeyIdentifier</i>	N	<i>subjectKeyIdentifier</i> SHALL be generated by using RFC 5480 [5] 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the subject's public key.	5.2.1.3.3
<i>basicConstraints</i>	Y	cA=true, pathLenConstraint = 0 or 1.	5.2.1.3.4
<i>certificatePolicies</i>	N	CertPolicyId	5.2.1.3.5

11

**Table 5 – Optional Extensions Permitted in
WiMAX Device Manufacturer CA and Sub-CA Certificates**

Extension Name	Critical	Contents	Reference
<i>authorityInfoAccessSyntax</i>	N	<accessMethod=id-ad-ocsp, accessLocation=URL to OCSF Responder>	5.4.10

A WiMAX device manufacturer CA and sub-CA certificate certificate SHALL NOT include any additional critical extensions.¹

5.2.1.1 notAfter

The difference between the *notBefore* and *notAfter* fields determines the lifetime of the certificate. The *notBefore* and *notAfter* fields SHALL comply with the bounds required by RFC 5480 [5].

5.2.1.2 subjectName

subjectName SHALL contain a valid DN, conformant with RFC 5480 [5], identifying the CA.

5.2.1.3 extensions

The *extensions* field in WiMAX certificates contains a number of required and optional extension fields described below.

5.2.1.3.1 keyUsage

The *keyUsage* extension SHALL be present and it SHALL be marked as critical. The *keyUsage* extension field SHALL have bits set for only *keyCertSign* and *cRLSign*.

5.2.1.3.2 cRLDistributionPoints

The *crlDistributionPoint* extension SHALL be present. It MUST include only the *distributionPoint* using the *fullName* CHOICE populated with an HTTP pointer to the location of the CRL published by PKCs issuer. In a Manufacturer CA's PKC, the CRLDP points to a Root CA generated CRL. In a Sub-CA's PKC, the CRLDP points to the Manufacturer CA generated CRL. The format for the pointer is as follows:

- Manufacturer CA: <http://deviceCA#-crl.wimaxforum.org/latest.crl>
- Sub-CA: <http://deviceCA#-crl.wimaxforum.org/<Manufacturer Name>/latest.crl>

See RFC 3986 [7] to convert the PKCs <Manufacturer Name> to the CRLDP URI.

5.2.1.3.3 subjectKeyIdentifier

The *subjectKeyIdentifier* extension SHALL be present. It SHALL be generated by using RFC 5480 [5] 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the subject's public key.

5.2.1.3.4 basicConstraints

The *basicConstraints* extension SHALL be present.

The *basicConstraints* extension SHALL be marked critical.

The *cA* bit SHALL be true

Where there are no lower level subordinate CAs and this certificate is used to directly sign device certificates, the *pathLenConstraint* SHALL be 0.

Where this certificate is used to sign Device sub-CA certificates, the *pathLenConstraint* SHALL be 1.

¹ Other non-critical extensions MAY also be included.

1 **5.2.1.3.5 certificatePolicies**

2 The *certificatePolicies* extension SHALL be present and SHALL be defined in accordance with the framework in
3 RFC 3647 [8].

4 The *certificatePolicies* extension SHALL NOT be critical.

5 **5.3 WiMAX Device Certificate Profile**

6 The WiMAX SS Device Certificate format is defined in RFC 5480 [5] and RFC 4043 [6], with additional
7 requirements described in 5.3.1 and 5.4.

8 **5.3.1 Wimax Device Chain SS Device Certificate Field Requirements**

9 A WiMAX SS device certificate SHALL include the fields in Table 6.

10 **Table 6 – Fields Required in WiMAX Device Certificate**

Field Name	RFC 5480 type	Value	Reference
<i>TBSCertificate</i> {	SEQUENCE	Certificate contents	N/A
<i>version</i>	INTEGER	v3	5.4.1
<i>serialNumber</i>	INTEGER	positive integer	5.4.2
<i>signature</i>	AlgorithmIdentifier	See 5.4.3	5.4.3
<i>issuer</i>	Name	Name of issuing CA	5.4.4
<i>Validity</i> {	SEQUENCE	<i>notBefore</i> and <i>notAfter</i>	N/A
<i>notBefore</i>	Time	Date on which the certificate validity period begins	5.4.5
<i>notAfter</i>	Time	Date on which the certificate validity period ends.	5.3.1.1
}			
<i>subject</i>	Name	Name of the device	5.3.1.2
<i>subjectPublicKeyInfo</i>	SubjectPublicKeyInfo	The 1024 or 2048 bit credential public key and algorithm identifier	5.4.6
<i>extensions</i>	Extensions	See 5.3.1.3	5.3.1.3
}			
<i>signatureAlgorithm</i>	AlgorithmIdentifier	See 5.4.7	5.4.7
<i>signatureValue</i>	BIT STRING	Certificate Signature	5.4.8

11
12 The Extensions field SHALL contain the extensions shown in Table 7.

13 **Table 7 – Extensions Required in WiMAX SS Device Certificate**

Extension Name	Critical	Contents	Reference
<i>keyUsage</i>	N	0x005 (bits 0&2 set – digitalSignature & keyEncipherment)	5.3.1.3.1
<i>authorityKeyIdentifier</i>	N	KeyIdentifier Equal to the issuer’s subjectKeyIdentifier field	5.4.9
<i>certificatePolicies</i>	N	CertPolicyId	5.3.1.3.2

1 The Extensions field MAY contain the extensions shown in Table 8.²

2 **Table 8 – Optional extensions Permitted in WiMAX SS Device Certificates**

Extension Name	Critical	Contents	Reference
<i>authorityInfoAccessSyntax</i>	N	<accessMethod=id-ad-ocsp, accessLocation=URL to OCSF Responder>	5.4.10

3

4 **5.3.1.1 notAfter**

5 The difference between the *notBefore* and *notAfter* fields determines the lifetime of the certificate. The *notBefore*
6 and *notAfter* fields SHALL comply with the bounds required by RFC 5480 [5].

7 **5.3.1.2 subject**

8 *subject* contains a valid DN as required by [5]. Standard RDN fields are permitted as per RFC 5480 [5]. Additional
9 requirements are given in 5.3.1.2.1 through 5.3.1.2.2.

10 **5.3.1.2.1 MAC Address and Model**

11 The MAC address and model SHALL be specified with the X520CommonName RDN and it SHALL use either the
12 printableString or utf8 string choice. The first 13 bytes of the value SHALL contain the MAC address as a sequence
13 of 12 printable ascii characters followed by a space. The remaining characters of the value will represent the
14 WiMAX Modem Model. The MAC address characters SHALL appear in the order they would appear in the IEEE
15 802-2001 compliant dashed form of the written MAC address³.

16 E.G. “006021A50A23 ABCD” will be interpreted as a WiMAX modem with the model name “ABCD” with a MAC
17 address that would be written 00-60-21-A5-0A-23.

18 **5.3.1.2.2 Manufacturer**

19 The manufacturer SHALL be specified with the X520OrganizationName RDN and it SHALL use either the
20 printableString or utf8 string choice. The value SHALL contain the name of the manufacturer of the WiMAX
21 modem model.

22 **5.3.1.3 extensions**

23 The *extensions* field in WiMAX certificates contains a number of required and optional extension fields described
24 below.

25 A WiMAX device certificate SHALL NOT include any additional critical extensions.

26 **5.3.1.3.1 keyUsage**

27 The *keyUsage* extension SHALL be present. The *keyUsage* extension field SHALL have bits 0 and 2 set for
28 digitalSignature and keyEncipherment.

29 The *keyUsage* extension SHALL NOT be critical.

30 **5.3.1.3.2 certificatePolicies**

31 The *certificatePolicies* extension SHALL be present and SHALL defined in accordance with the framework in RFC
32 3647 [8].

33 The *certificatePolicies* extension SHALL NOT be critical.

² Other non-critical extensions MAY also be included.

³ The MAC address octet separator often is a colon. This is an error. IEEE 802-2001 specifies that the colon separator indicates a reverse order representation. The dashes matter.

1 **5.4 Field Requirements Common to all WiMAX Certificates**

2 This section describes the fields common to all the WiMAX certificate formats.

3 **5.4.1 Version**

4 WiMAX Certificates SHALL be version 3.

5 **5.4.2 serialNumber**

6 The certificate serial number SHALL be a string of up to 20 octets representing a non-negative integer.

7 RFC 5480 [5] requirements mean that serialNumber SHALL be unique in the scope of WiMAX certificates signed
8 by the CA.

9 **5.4.3 Signature**

10 RFC 5480 [5] states that the signature field contains the algorithm identifier for the algorithm used by the CA to sign
11 the certificate.

12 The WiMAX certificate SHALL be signed by the CA using the SHA-256 algorithm with RSA indicated with the
13 OID sha256WithRSAEncryption as defined in RFC 4055 [10] (PKCS#1 v1.5).

14 **5.4.4 issuer**

15 The *issuer* field SHALL be the name of the issuer CA as required by and formatted as defined by RFC 5480 [5].

16 **5.4.5 notBefore**

17 *notBefore* is defined as per RFC 5480 [5].

18 **5.4.6 subjectPublicKeyInfo**

19 The *subjectPublicKey* subfield type SHALL be RSAPublicKey and the value SHALL be the 2048 bit RSA public
20 key.

21 **5.4.7 signatureAlgorithm**

22 The signature algorithm field SHALL be identical to the signature field described in 5.4.3.

23 **5.4.8 signatureValue**

24 This field (of device and each of CAs in its chain) SHALL be at least 2048 bits.

25 **5.4.9 authorityKeyIdentifier Extension**

26 *authorityKeyIdentifier* extension field is identical to the subjectKeyIdentifier value from the issuers's CA certificate.

27 **5.4.10 AuthorityInfoAccessSyntax Extension**

28 The *AuthorityInfoAccessSyntax* extension field MAY be present in Device PKCs.

29 In Manufacturer CA and Device Sub-CA PKCs, the *AuthorityInformationAccessSyntax* extension MAY be present.
30 If OCSP support for certificates issued by Manufacturer CA and Device Sub-CA PKCs is required, then it MUST be
31 present.

32

33 If present, the extension MUST indicate the id-ad-ocsp access method with a URI access location of the OCSP
34 Responder. The OCSP Responder is either delegated from the Root or from the Manufacturer CA. The format for
35 the pointer is as follows:

- 36 • Manufacturer CA: <http://deviceCA#-ocsp.wimaxforum.org/>
- 37 • Sub-CA: <http://deviceCA#-ocsp.wimaxforum.org/>

- 1 **5.4.11 SubjectInfoAccessSyntax Extension**
- 2 The *subjectInfoAccessSyntax* extension field MAY be present.
- 3
- 4