



WiMAX Forum X.509 Server 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.

Table of Contents

1. INTRODUCTION AND SCOPE	5
1.1 TERMINOLOGY	5
2. REFERENCES	6
3. ABBREVIATIONS AND DEFINITIONS.....	7
4. CERTIFICATES	8
4.1 WIMAX SERVER ROOT CA CERTIFICATE PROFILE	9
4.1.1 <i>WiMAX Server Root CA Certificate Field Requirements</i>	9
4.2 WIMAX SERVER CA AND SERVER SUB-CA CERTIFICATE PROFILE.....	11
4.2.1 <i>WiMAX Server CA and Server Sub-CA Certificate Field Requirements</i>	11
4.3 WIMAX SERVER CERTIFICATE PROFILE	13
4.3.1 <i>Wimax Server Certificate Field Requirements</i>	13
4.4 FIELD REQUIREMENTS COMMON TO ALL WIMAX CERTIFICATES	15
4.4.1 <i>Version</i>	15
4.4.2 <i>serialNumber</i>	15
4.4.3 <i>Signature</i>	15
4.4.4 <i>issuer</i>	16
4.4.5 <i>notBefore</i>	16
4.4.6 <i>subjectPublicKeyInfo</i>	16
4.4.7 <i>signatureAlgorithm</i>	16
4.4.8 <i>signatureValue</i>	16
4.4.9 <i>authorityKeyIdentifier Extension</i>	16
4.4.10 <i>AuthorityInfoAccessSyntax Extension</i>	16

List of Figures

FIGURE 4-1 LENGTH 3 AND 4 DEVICE CERTIFICATE CHAINS FOR 2 AND 3 LEVEL CA TREES 8

List of Tables

TABLE 1 – FIELDS REQUIRED IN WIMAX SERVER ROOT CA CERTIFICATES 9
TABLE 2 – EXTENSIONS REQUIRED IN WIMAX SERVER ROOT CA CERTIFICATES 9
TABLE 3 - FIELDS REQUIRED IN WIMAX SERVER CA AND SERVER SUB-CA CERTIFICATES 11
TABLE 4 - EXTENSIONS REQUIRED IN WIMAX SERVER CA CERTIFICATE 12
TABLE 5 - FIELDS REQUIRED IN WIMAX SERVER CERTIFICATE 14
TABLE 6 - EXTENSIONS REQUIRED IN WIMAX SERVER CERTIFICATES 14
TABLE 7 - OPTIONAL EXTENSIONS PERMITTED IN WIMAX SERVER CERTIFICATES 14

Revision History

Dec 15, 2007	V&V comments incorporated
Jan 17, 2008	Remove comments and track changes, insert WiMAX header and formatting, minor cleanup. Remove WiMAXServerInfo extension, per x509 group agreement on Jan 16, 2008.
Jan 28, 2008	Renamed “Operator” to “Service Provider” and “realm” to “FQDN”, to be consistent with Device Profile. Modified text to allow both length 2 and 3 CA chains. Inserted text on NSPID.
Feb 28, 2008	Replaced “FQDN” with “DN”, removed references to private NSP ID, added definition of NSP ID. Editorial proofreading and cleanup.
March 6, 2008	Editorial cleanup. Clarification of key lengths in Sect 4.4.6 and 4.4.8
March 31, 2008	Headers fix and DN disambiguation. Refer to RFC 5216 as EAP-TLS spec. Fixed abbreviation RDN. Fixed copyright year to 2008.
April 8, 2008	Release 1.0. Changed headers to reflect approved release.
April 18, 2008 April 22, 2008	Changed title and headers to reflect draft spec. Fixed version numbering inconsistency.
June 3, 2009	Added certificatePolicies to Server, Server Sub-CA, and Server certificates in Tables 4 and 7 and new section 4.2.1.3.5 and 4.3.1.3.5. Updated AIA text in Tables 4 and 7 and the text in 4.4.10. Updated CRLDP text in Table 4 and section 4.3.1.3.2. Corrected clientAuth OID in Table 6 and Section 4.3.1.3.2. Added note in 4.2.1 and 4.3.1 about other non-critical extensions. Added references for RFC 2119, 3986, and 3647.

1. Introduction and Scope

The purpose of this document is to specify the format of the X.509 Server Root Certificate Authority (CA) and Server 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 [10].

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

3. Abbreviations and Definitions

AIA	Authority Information Access
BS	Base Station
CA	Certificate Authority
DN	Distinguished Name
HAAA	Home AAA Server
MS	Mobile Station
NAI	Network Access Identifier
NSP ID	Network Service Provider ID
NWG	Network Working Group
RDN	Relative Distinguished Name
SIA	Subject Information Access
SPWG	Service Provider Working Group
SS	Subscriber Station

4. Certificates

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

The WiMAX Server certificate hierarchy assumes a two or three level tree that is rooted in the WiMAX Server Root CA, with Server CA, and, optionally, Server Sub-CA as its subordinates at lower levels.

Device Certificates (see WiMAX Device Certificate Profiles) and server certificates SHALL be issued by separate CAs and SHALL terminate at separate trust anchor public keys.

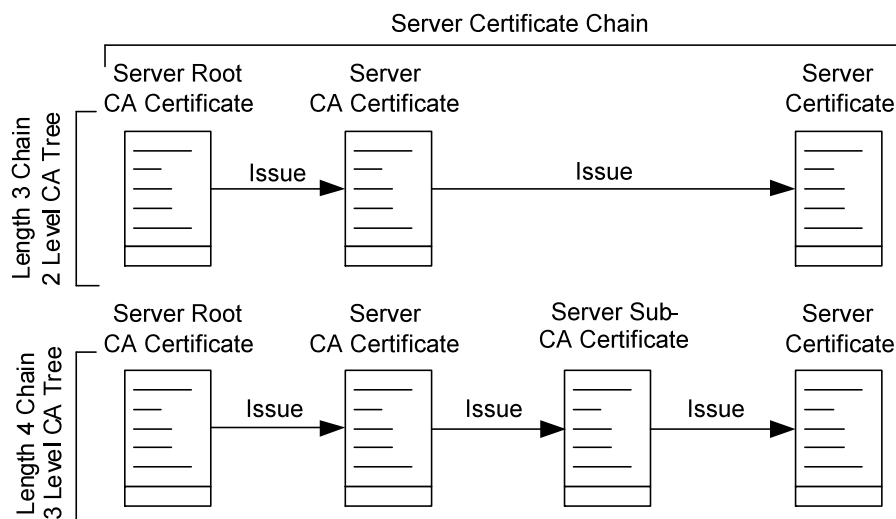


Figure 4-1 Length 3 and 4 Device Certificate Chains for 2 and 3 level CA trees

WiMAX server certificates SHALL be constructed in accordance with IETF RFC 5480 [5] and the type definitions and default values provided in IETF RFC 5480 [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 [7] (PKCS#1 v1.5).
- All certified RSA public keys (including those of Server Root CAs, Server CAs, Server Sub-CAs and Server) SHALL have RSA public key exponent $e = 65537$.
 - This allows for significant computational savings both on the SS 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. Server Root certificates SHALL NOT use AIA or SIA.

4.1 WiMAX Server Root CA Certificate Profile

The WiMAX Server Root CA certificate format is defined in RFC 5480 [5], with additional requirements described in 4.1.1.

4.1.1 WiMAX Server Root CA Certificate Field Requirements

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

Field Name	RFC 5480 type	Value	Reference
TBSCertificate {	SEQUENCE	Certificate contents	N/A
version	INTEGER	v3	4.4.1
serialNumber	INTEGER	Unique positive integer	4.4.2
signature	AlgorithmIdentifier	See 4.4.3	4.4.3
issuer	Name	Name of Issuing CA	4.1.1.2
validity {	SEQUENCE	notBefore and notAfter	
notBefore	Time	Date on which the certificate validity period begins	4.4.5
notAfter }	Time	Date on which the certificate validity period ends.	4.1.1.1
subject	Name	Name of Issuing CA	4.1.1.2
subjectPublicKeyInfo	SubjectPublicKeyInfo	The credential public key and algorithm identifier	4.4.6
extensions }	Extensions	See Table 2	4.1.1.3
signatureAlgorithm	AlgorithmIdentifier	See 4.4.7	4.4.7
signatureValue	BIT STRING	Certificate Signature	4.4.8

Table 1 – Fields Required in WiMAX Server Root CA Certificates

Except where otherwise noted in Table 1, the Extensions field SHALL contain the extensions shown in Table 2.

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.	4.4.9
<i>keyUsage</i>	Y	060x (bits 5 & 6 - keyCertSign & cRLSign)	4.1.1.3.1
<i>subjectKeyIdentifier</i>	N	subjectKeyIdentifier SHALL be generated using RFC 5480 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the issuer's public key.	4.1.1.3.2
<i>basicConstraints</i>	Y	cA=true	4.1.1.3.3

Table 2 – Extensions Required in WiMAX Server Root CA Certificates

A WiMAX server root certificate SHALL NOT include any additional critical extensions.

4.1.1.1 notAfter

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

4.1.1.2 issuer and subject Names

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

4.1.1.3 extensions

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

4.1.1.3.1 keyUsage

The *keyUsage* extension SHALL be present.

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

The *keyUsage* extension SHALL be critical.

4.1.1.3.2 subjectKeyIdentifier

subjectKeyIdentifier SHALL be present.

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

4.1.1.3.3 basicConstraints

The *basicConstraints* extension field SHALL be present.

The *basicConstraints* extension SHALL be marked critical.

The *cA* bit SHALL be true.

4.2 WiMAX Server CA and Server Sub-CA Certificate Profile

The WiMAX Server Subordinate CA certificate format is defined in RFC 5480 [5], with additional requirements described in 4.2.1. It covers both Server CA and Server Sub-CA

4.2.1 WiMAX Server CA and Server Sub-CA Certificate Field Requirements

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

Field Name	RFC 5480 type	Value	Reference
TBSCertificate {	SEQUENCE	Certificate contents	N/A
version	INTEGER	v3	4.4.1
serialNumber	INTEGER	Unique positive integer	4.4.2
signature	AlgorithmIdentifier	See 4.4.3	4.4.3
issuer	Name	Name of Issuing CA	4.4.4
validity {	SEQUENCE	notBefore and notAfter	
notBefore	Time	Date on which the certificate validity period begins	4.4.5
notAfter }	Time	Date on which the certificate validity period ends.	4.2.1.1
subject	Name	Name of Subject CA	4.2.1.2
subjectPublicKeyInfo	SubjectPublicKeyInfo	The credential public key and algorithm identifier	4.4.6
extensions }	Extensions	See Table 4	4.2.1.3
signatureAlgorithm	AlgorithmIdentifier	See 4.4.7	4.4.7
signatureValue	BIT STRING	Certificate Signature	4.4.8

Table 3 - Fields Required in WiMAX Server CA and Server Sub-CA Certificates

Except where otherwise noted in Table 3, the Extensions field SHALL contain the extensions shown in Table 4.

Extension Name	Critical	Contents	Reference
<i>authorityKeyIdentifier</i>	N	KeyIdentifier Equal to the issuer's subjectKeyIdentifier field	4.4.9
<i>keyUsage</i>	Y	060x (bits 5 & 6 - keyCertSign & cRLSign)	4.2.1.3.1
<i>cRLDistributionPoints</i>	N	Only distributionPoint with fullName choice. Contains HTTP pointer to location of CRL: Server CA: <URL to Root's CRL> Server Sub-CA: <URL to Server CA's CRL>	4.2.1.3.2
<i>subjectKeyIdentifier</i>	N	subjectKeyIdentifier SHALL be generated by using RFC 5480 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the subject's public key.	4.2.1.3.3
<i>basicConstraints</i>	Y	cA=true, pathLenConstraint = 0 or 1.	4.2.1.3.4
<i>authorityInfoAccessSyntax</i>	N	<accessMethod=id-ad-ocsp, accessLocation=URL to OCSP Responder>	4.4.10
<i>certificatePolicies</i>	N	CertPolicyId	Error! Reference source not found.

Table 4 - Extensions Required in WiMAX Server CA Certificate

A WiMAX Server CA certificate SHALL NOT include any additional critical extensions.¹

4.2.1.1 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].

4.2.1.2 subjectName

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

4.2.1.3 extensions

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

4.2.1.3.1 keyUsage

The *keyUsage* extension SHALL be present.

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

The *keyUsage* extension SHALL be critical.

4.2.1.3.2 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 Server CA's PKC, the CRLDP points to a Root CA generated CRL. In a Sub-CA's PKC, the CRLDP points to the Server CA generated CRL. The format for the pointer is as follows:

- Server CA: <http://serverCA#-crl.wimaxforum.org/latest.crl>
- Sub-CA: <http://serverCA#-crl.wimaxforum.org/<Provider Name>/latest.crl>

See RFC 3986 [8] to convert the PKCs <Provider Name> to the CRLDP URI.

4.2.1.3.3 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.

4.2.1.3.4 basicConstraints

The *basicConstraints* extension SHALL be present.

The *basicConstraints* extension SHALL be marked critical.

¹ Other non-critical extensions MAY also be included.

The cA bit SHALL be true

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

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

4.2.1.3.5 certificatePolicies

The certificatePolicies extension SHALL be present and SHALL be defined in accordance with the framework in RFC 3647 [9].

The certificatePolicies extension SHALL NOT be critical.

4.3 WiMAX Server Certificate Profile

The WiMAX Server certificate format is defined in RFC 5480 [5] and RFC 4043 [6], with additional requirements described in 4.3.1 and 4.3.1.3.3.

4.3.1 Wimax Server Certificate Field Requirements

A WiMAX Server certificate SHALL include the fields in Table 5.

Field Name	RFC 5480 type	Value	Reference
TBSCertificate {	SEQUENCE	Certificate contents	N/A
version	INTEGER	v3	4.4.1
serialNumber	INTEGER	positive integer	4.4.2
signature	AlgorithmIdentifier	See 4.4.3	4.4.3
issuer	Name	Name of Issuing CA	4.4.4
validity {	SEQUENCE	notBefore and notAfter	N/A
notBefore	Time	Date on which the certificate validity period begins	4.4.5
notAfter	Time	Date on which the certificate validity period ends.	4.3.1.1
}			
subject	Name	Name of the server	4.3.1.2
subjectPublicKeyInfo	SubjectPublicKeyInfo	The 1024 or 2048 bit credential public key and algorithm identifier	4.4.6
extensions	Extensions	See Table 6	0
}			
signatureAlgorithm	AlgorithmIdentifier	See 4.4.7	4.4.7
signatureValue	BIT STRING	Certificate Signature	4.4.8

Table 5 - Fields Required in WiMAX Server Certificate

The Extensions field SHALL contain the extensions shown in Table 6.

Extension Name	Critical	Contents	Reference
<i>keyUsage</i>	N	0x005 (bits 0&2 set – digitalSignature & keyEncipherment)	4.3.1.3.1
<i>authorityKeyIdentifier</i>	N	KeyIdentifier Hash of the value of the issuer’s public key bit string	4.4.9
<i>extKeyUsage</i>	N	serverAuth (1.3.6.1.5.5.7.3.1) and clientAuth (1.3.6.1.5.5.7.3.2)	4.3.1.3.2
<i>certificatePolicies</i>	N	CertPolicyId	4.3.1.3.3

Table 6 - Extensions Required in WiMAX Server Certificates

The Extensions field MAY contain the extensions shown in Table 7.²

Extension Name	Critical	Contents	Reference
<i>authorityInfoAccessSyntax</i>	N	See 4.4.10<accessMethod=id-ad-ocsp, accessLocation=URL to OCSP Responder>	4.4.10

Table 7 - Optional extensions Permitted in WiMAX Server Certificates

4.3.1.1 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].

4.3.1.2 subject

subject contains a valid DN as required by RFC 5480 [5]. Standard RDN fields are permitted as per RFC 5480 [5]. Additional requirements are given in 4.3.1.2.1 and 4.3.1.2.2.

4.3.1.2.1 Domain Name of Service Provider

The domain name of Service Provider SHALL be specified with the X520CommonName RDN and it SHALL use either the printableString or utf8 string choice.

The value SHALL contain the realm of the Service Provider, equal to the domain name from the operator’s NAI.

4.3.1.2.2 Service Provider

The Service Provider SHALL be specified with the X520OrganizationName RDN and it SHALL use the printableString or utf8string choice. The value SHALL contain the human readable name of the Service Provider.

² Other non-critical extensions MAY also be included.

4.3.1.2.3 NSP ID

The NSP ID SHALL be specified with the X520OrganizationName RDN and it SHALL use the printableString or utf8string choice. Its value SHALL contain the NSP ID of the service provider.

4.3.1.3 Extensions

The *extensions* field in WiMAX certificates MAY contain the following extension field described below.

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

4.3.1.3.1 keyUsage

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

The *keyUsage* extension SHALL NOT be critical.

4.3.1.3.2 extKeyUsage

The *extKeyUsage* extension SHALL be present. The *extKeyUsage* SHALL include serverAuth (1.3.6.1.5.5.7.3.1) and clientAuth (1.3.6.1.5.5.7.3.2).

The *extKeyUsage* extension SHALL NOT be critical.

4.3.1.3.3 certificatePolicies

The certificatePolicies extension SHALL be present and SHALL be defined in accordance with the framework in RFC 3647 [9].

The certificatePolicies extension SHALL NOT be critical.

4.4 Field Requirements Common to all WiMAX Certificates

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

4.4.1 Version

WiMAX Certificates SHALL be version 3.

4.4.2 serialNumber

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

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

4.4.3 Signature

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

The WiMAX certificate SHALL be signed by the CA using the SHA-256 algorithm with RSA indicated with the OID sha256WithRSAEncryption as defined in RFC 4055 [7] (PKCS#1 v1.5).

4.4.4 issuer

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

4.4.5 notBefore

notBefore is defined as per RFC 5480 [5].

4.4.6 subjectPublicKeyInfo

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

4.4.7 signatureAlgorithm

The signature algorithm field SHALL be identical to the signature field described in 4.4.3.

4.4.8 signatureValue

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

4.4.9 authorityKeyIdentifier Extension

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

4.4.10 AuthorityInfoAccessSyntax Extension

In Server PKCs, the *AuthorityInformationAccessSyntax* extension field MAY be present.

In Server CA PKCs, the *AuthorityInformationAccessSyntax* extension MUST be present. In Server Sub-CA, the *AuthorityInformationAccessSyntax* extension MUST be present, if OCSP support for certificates issued by Server CA and server sub-CA PKCs is required; else it MAY be present.

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