



## **WiMAX Forum OCSP Profile Approved Specification**

Version 1.0.1

June 3<sup>rd</sup>, 2009

**WiMAX Forum Proprietary**

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

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

Copyright 2008 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

<b>1.</b>	<b>INTRODUCTION AND SCOPE .....</b>	<b>6</b>
1.1	Terminology .....	6
<b>2.</b>	<b>REFERENCES .....</b>	<b>7</b>
<b>3.</b>	<b>ABBREVIATIONS AND DEFINITIONS.....</b>	<b>8</b>
<b>4.</b>	<b>ASSUMPTIONS .....</b>	<b>9</b>
<b>5.</b>	<b>OCSP RESPONDER CERTIFICATE PROFILE .....</b>	<b>10</b>
5.1	WiMAX OCSP Responder Profile.....	11
<b>6.</b>	<b>ONLINE CERTIFICATE STATUS PROTOCOL PROFILE.....</b>	<b>11</b>
6.1	WiMAX OCSP Request.....	14
6.1.1	<i>WiMAX OCSP Request Field Requirements .....</i>	<i>14</i>
6.2	WiMAX OCSP Responses.....	16
6.2.1	<i>WiMAX OCSP Response Field Requirements .....</i>	<i>16</i>

## List of Figures

## List of Tables

TABLE 5-1 – FIELDS REQUIRED IN WIMAX OCSP RESPONDERS CERTIFICATE .....	11
TABLE 5-2 – EXTENSIONS REQUIRED IN WIMAX OCSP RESPONDERS CERTIFICATE .....	11
TABLE 6-1 – FIELDS REQUIRED IN WIMAX OCSP REQUEST .....	14
TABLE 6-2 – FIELDS REQUIRED IN WIMAX OCSP RESPONSE .....	16
TABLE 6-3 – FIELDS REQUIRED IN RESPONSEVALUE .....	16

## REVISION HISTORY

January 8 <sup>th</sup> , 2008	Initial draft
February 11 <sup>th</sup> , 2008	Added profile for OCSP responder's PKC.
February 27 <sup>th</sup> , 2008	Modified OCSP responder certificate profile to add extended key usage (ocspSigning) and certificate policy extensions.
March 20 <sup>th</sup> , 2008	Changed Tables 5-1 and 5-2 heading to OCSP Responder Certificates. Removed noCheck from OCSP Responder's certificate.
April 2 <sup>nd</sup> , 2008	Added CRLDP in OCSP responder's certificate (to point to CA issued CRL) and made editorial changes.
April 16 <sup>th</sup> , 2008	No changes. Published as Draft Specification Version 1.0.0.
June 8 <sup>th</sup> , 2009	Added note about other non-critical extensions to section 5.1. Updated 3280bis reference to RFC 5480. Removed reference to RFC 3279. Added references for 2119.

# 1. Introduction and Scope

The purpose of this document is to specify the format of the Online Certificate Status Protocol (OCSP) requests and responses as well as the certificate profile for the OCSP responder. This request format shall be used by Devices and Server when requesting certificate status information from OCSP servers and. The response format shall be used by OCSP responders when responding to Device and Server OCSP requests. These profiles are required by RFC 5019 [4], which in turn profiles RFC 2560 [1].

## 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 [5].

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] RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- [2] RFC 5480, Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile.
- [3] 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.
- [4] RFC 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.
- [5] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels

### **3. Abbreviations and Definitions**

CA	Cartification Authority
DN	Distinguished Name
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standards
RFC	Request for Comments
SS	Subscriber Station
CRL	Certificate Revocation List
SHA	Secure Hash Algorithm
OCSP	Online Certificate Status Protocol
OID	Object Identifier

## **4. Assumptions**

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

## 5. OCSP Responder Certificate Profile

This section describes the fields of OCSP Responders certificate issued by WiMAX Device and Server CAs.

The WiMAX certificate hierarchies assumes a two or three level tree that is rooted by two separate the WiMAX Root CAs: a Device Root CA and a Server Root CA. The PKIs have subordinate CAs, and allows one more lower layer Sub-CA. To support revocation status checking OCSP responders are supported. In the WiMAX Device PKI, Device Root CAs and Manufacturer CAs delegate the generation of OCSP responses to OCSP Respoders. In the WiMAX Server PKI, Server Root CAs delegate the generation of OCSP responses to OCSP Respoders. The CA that delegates signs the OCSP Responder's certificate.

OCSP responder certificates have the following common attributes:

- All OCSP responder certificates SHALL be version 3 X.509 certificates.
- OCSP responders that provide status information on certificate signed with SHA-256 with RSA encryption have certificates that are signed with SHA-256 with RSA encryption, as per RFC 4055 [3] (PKCS#1 v1.5).

## 5.1 WiMAX OCSP Responder Profile

The WiMAX OCSP responder certificate format is defined in RFC 5480 [2], with additional requirements from RFC RFC 2560 [1] and from the text below.

**Table 5-1 – Fields Required in WiMAX OCSP Responders Certificate**

Field Name	RFC5480 type	Value	Reference
<i>TBSCertificate</i> {	SEQUENCE	Certificate contents	N/A
<i>version</i>	INTEGER	v3	5.1.1.1
<i>serialNumber</i>	INTEGER	Unique positive integer	5.1.1.2
<i>signature</i>	AlgorithmIdentifier	Identifies the signature algorithm used by the CA	5.1.1.3
<i>issuer</i>	Name	Name of issuing CA	5.1.1.4
<i>validity</i> {	SEQUENCE	<i>notBefore</i> and <i>notAfter</i>	5.1.1.5
<i>notBefore</i>	Time	Date on which the certificate validity period begins	
<i>notAfter</i>	Time	Date on which the certificate validity period ends.	
}			
<i>subject</i>	Name	Name of OCSP Responder	5.1.1.6
<i>subjectPublicKeyInfo</i>	SubjectPublicKeyInfo	The 1024 or 2048 bit credential public key and algorithm identifier	5.1.1.7
<i>extensions</i>	Extensions	See Table 5-2.	5.1.1.8
}			
<i>signatureAlgorithm</i>	AlgorithmIdentifier	See 5.1.1.9.	5.1.1.9
<i>signatureValue</i>	BIT STRING	Certificate Signature	5.1.1.10

Except where otherwise noted in Table 5-2, the Extensions field SHALL contain the extensions shown in Table 5-2.

**Table 5-2 – Extensions Required in WiMAX OCSP Responders Certificate**

Extension Name	Critical	Contents	Reference
<i>authorityKeyIdentifier</i>	N	KeyIdentifier  Equal to the issuer's subjectKeyIdentifier field	5.1.1.8.1
<i>keyUsage</i>	N	0x005 (bits 0 set – digitalSignature)	5.1.1.8.2
<i>subjectKeyIdentifier</i>	N	<i>subjectKeyIdentifier</i> SHALL be generated using RFC 5480 [2] 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the issuer's public key.	5.1.1.8.3
<i>extendedKeyUsage</i>	N	id-kp-ocspSigning { 1.3.6.1.5.5.7.3.9 }	5.1.1.8.4
<i>certificatePolicies</i>	N	CertPolicyId	5.1.1.8.5
<i>crlDistributionPoints</i>	N	Only distributionPoint with fullName choice. Contains HTTP pointer to location of CRL.	5.1.1.8.6

A WiMAX OCSP responder certificate SHALL NOT include any additional critical extensions.<sup>1</sup>

<sup>1</sup> Other non-critical extensions MAY also be present.

#### **5.1.1.1 version**

WiMAX Certificates SHALL be version 3.

#### **5.1.1.2 serialNumber**

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

RFC 5480 [2] requirements mean that serialNumber shall be unique in the scope of WiMAX certificates signed by the CA.

#### **5.1.1.3 signature**

RFC 5480 [2] states that the signature field *contains the algorithm identifier for the algorithm used by the CA to sign the certificate.*

The WiMAX OCSP responder certificates shall be signed by the CA using SHA-256 algorithm with RSA indicated with the OID sha256WithRSAEncryption as defined in RFC 4055 [3] (PKCS#1 v1.5)

#### **5.1.1.4 issuer**

The issuer field shall be the name of the issuer CA as required by and formatted as defined by RFC 5480 [2].

#### **5.1.1.5 notBefore and notAfter**

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

#### **5.1.1.6 subject**

*subject* contains a valid DN, conformant with RFC 5480 [2], identifying the OCSP responder.

#### **5.1.1.7 subjectPublicKeyInfo**

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

#### **5.1.1.8 extensions**

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

##### **5.1.1.8.1 authorityKeyIdentifier**

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

##### **5.1.1.8.2 keyUsage**

The *keyUsage* extension SHALL be present. The keyUsage extension field SHALL have bits 0 set for digitalSignature.

The keyUsage extension SHALL NOT be critical.

##### **5.1.1.8.3 subjectKeyIdentifier**

*subjectKeyIdentifier* SHALL be present.

*subjectKeyIdentifier* SHALL be generated using RFC 5480 [2] 4.2.1.2 method 1 – the 160 bit SHA-1 hash of the issuer's public key.

##### **5.1.1.8.4 extendedKeyUsage**

The extendedKeyUsage extension SHALL be present. The extendedKeyUsage extension field SHALL indicate id-kp-ocspSigning { 1.3.6.1.5.5.7.3.9 }.

The keyUsage extension SHALL NOT be critical.

#### **5.1.1.8.5 certificatePolicies**

The *certificatePolicies* extension SHALL be present. It MUST include either the Device CP or the Server CP object identifiers.

The *certificatePolicies* extension SHALL NOT be critical.

#### **5.1.1.8.6 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 the OCSP responder's CA.

The *crlDistributionPoint* extension SHALL NOT be critical.

#### **5.1.1.9 signatureAlgorithm**

The signature algorithm field SHALL be identical to the signature field described in 5.1.1.3.

#### **5.1.1.10 signatureValue**

The RSA key length shall be at least 2048 bits.

## 6. Online Certificate Status Protocol Profile

This section describes the fields of OCSP requests and responses.

### 6.1 WiMAX OCSP Request

The WiMAX OCSP request format is defined in RFC 5019 [4], with additional requirements described below.

#### 6.1.1 WiMAX OCSP Request Field Requirements

A WiMAX OCSP requests SHALL include the fields in Table 6-1.

**Table 6-1 – Fields Required in WiMAX OCSP Request**

Field Name	RFC2560 type	Value	Reference
<i>tbsRequest</i> {	SEQUENCE	OCSP request	N/A
<i>version</i>	INTEGER	v1	6.1.1.1
<i>requestorName</i>	GeneralName	Name of signer	6.1.1.2
<i>requestList</i> {	SEQUENCE OF	MUST include only one entry	6.1.1.3
<i>reqCert</i> {	SEQUENCE		6.1.1.1.3.1
<i>hashAlgorithm</i>	AlgorithmIdentifier	Identifies hash algorithm.	6.1.1.1.3.1.1
<i>issuerNameHash</i>	OCTET STRING	Hash of issuer's name.	6.1.1.1.3.1.2
<i>issuerKeyHash</i>	OCTET STRING	Hash of issuer's key.	6.1.1.1.3.1.3
<i>serialNumber</i> }	INTEGER	Certificates's serial number for which status information is requested.	6.1.1.1.3.1.4
<i>singleRequestExtensions</i> }		MUST NOT be present	6.1.1.1.3.2
<i>requestExntesion</i> }		SHOULD NOT be present	N/A
<i>optionalSignature</i> {		OPTIONAL	6.1.1.4
<i>signatureAlgorithm</i>	AlgorithmIdentifier	Identifies signature algorithms.	6.1.1.4.1
<i>signature</i>	BIT STRING	Signature value	6.1.1.4.2
<i>certs</i>	SEQUENCE OF Certificates	Certificate necessary to verify digital signature.	6.1.1.4.3

A WiMAX OCSP response SHALL NOT include any critical extensions.

##### 6.1.1.1 version

WiMAX OCSP requests SHALL be version 1.

##### 6.1.1.2 requestorName

The *requestorName* field contains name of the entity that signs the OCSP request.

This field MUST be present if the OCSP request is signed. It must include the subject name from the signing certificate.

This field SHOULD NOT be included if the OCSP request is not signed.

##### 6.1.1.3 requestList

The *requestList* field includes the certificates for which the OCSP requestor wants certificate status information. There MUST be only one entry in the SEQUENCE OF.

##### 6.1.1.3.1 reqCert

The *reqCert* field includes information necessary to identify the certificate for which the OCSP requestor wants status information. It has four fields: *hashAlgorithm*, *issuerNameHash*, *issuerKeyHash*, and *serialNumber*.

#### **6.1.1.3.1.1 hashAlgorithm**

The *hashAlgorithm* field indicates the hash algorithm used to compute the *issuerNameHash* and *issuerKeyHash* values. Both values MUST be computed using the SHA-1 algorithm. The object identifier for SHA-1 is ( 1 3 14 3 2 26 ).

#### **6.1.1.3.1.2 issuerNameHash**

The *issuerNameHash* field includes the hash of the certificate issuer's name for which the OCSP requestor wants status information. The hash shall be calculated over the DER encoding of the issuer's name field in the certificate being checked.

#### **6.1.1.3.1.3 issuerKeyHash**

The *issuerKeyHash* field includes the hash of the certificate issuer's key for which the OCSP requestor wants status information. It may be taken from the device or server certificate's authority key identifier extension.

#### **6.1.1.3.1.4 serialNumber**

The *serialNumber* field includes the serial number of the certificate for which the requestor wants status information. The value is copied from the certificate's *serialNumber* field.

#### **6.1.1.3.2 signRequestExtension**

This *signRequestExtension* field MUST NOT be present.

#### **6.1.1.4 optionalSignature**

WiMAX OCSP responses SHOULD NOT be signed. If they are signed, then the following fields are included: *signatureAlgorithm*, *signature*, and *certs*.

##### **6.1.1.4.1 signatureAlgorithm**

The *signatureAlgorithm* field indicates the algorithm used to generate the *signature* field. The signature algorithm MUST be *sha256WithRSAEncryption* as identified by ( 1 2 840 113549 1 1 11 ).

##### **6.1.1.4.2 signature**

The *signature* field includes the digital signature of the OCSP request. It is a BIT STRING.

##### **6.1.1.4.3 certs**

The *certs* field includes the certificate used to sign the OCSP request and any other certificates the OCSP signer thinks the OCSP responder might need to validate the certification path.

If the *optionalSignature* field is included in a WiMAX OCSP request, then the signer's certificate MUST be included in the *certs* field.

## 6.2 WiMAX OCSP Responses

The WiMAX OCSP response format is defined in RFC 5019 [4], with additional requirements described below.

Note that the current CRL issued by the CA is an authoritative record .

### 6.2.1 WiMAX OCSP Response Field Requirements

A WiMAX OCSP response SHALL include the fields in Table 6-2 and Table 6-3.

**Table 6-2 – Fields Required in WiMAX OCSP Response**

Field Name	RFC2560 type	Value	Reference
<i>responseStatus</i>	Enumerated		6.2.1.1
<i>responseBytes</i> {	SEQUENCE		N/A
<i>responseType</i>	OBJECT IDENTIFIER	MUST be the BasicOCSPResponse id-pkix-ocsp-basic ( 1 3 6 1 5 5 7 48 1 1 )	6.2.1.2
<i>responseValue</i> }	OCTET STRING	See Table 6-3	6.1.1.3

**Table 6-3 – Fields Required in responseValue**

Field Name	RFC2560 type	Value	Reference
<i>tbsResponseData</i> {	SEQUENCE		
<i>version</i>	INTEGER	v1	6.2.1.3.1
<i>responderID</i>	CHOICE	Hash of responder’s public key.	6.2.1.3.2
<i>producedAt</i>	GeneralizedTime		6.2.1.3.3
<i>responses</i> {	SEQUENCE OF	SHOULD include only one entry.	6.2.1.3.4
<i>certID</i> {			6.2.1.3.4.1
<i>hashAlgorithm</i>	AlgorithmIdentifier	Identifies hash algorithm.	6.2.1.3.4.1.1
<i>issuerNameHash</i>	OCTET STRING	Hash of issuer’s name.	6.2.1.3.4.1.2
<i>issuerKeyHash</i>	OCTET STRING	Hash of issuer’s key.	6.2.1.3.4.1.3
<i>serialNumber</i> }	INTEGER	Certificates’s serial number for which status information is returned.	6.2.1.3.4.1.4
<i>certStatus</i>		good, revoked, or unknown	6.2.1.3.4.2
<i>thisUpdate</i>	GeneralizedTime	Time when the status is known to be correct.	6.2.1.3.4.3
<i>nextUpdate</i>	GeneralizedTime	Time at which or before new information will be available.	6.2.1.3.4.4
<i>singleExtensions</i> }		SHOULD NOT be present	6.2.1.3.4.5
<i>responseExtensions</i>		SHOULD NOT be present	6.2.1.3.5
<i>signatureAlgorithm</i>	AlgorithmIdentifier	Identifies signature algorithms.	6.2.1.3.6
<i>signature</i>	BIT STRING	Signature value	6.2.1.3.7
<i>certs</i>	SEQUENCE OF Certificates	Certificate necessary to verify digital signature.	6.2.1.3.8

A WiMAX OCSP response SHALL NOT include any critical extensions.

#### 6.2.1.1 responseStatus

The *responseStatus* field indicates the status of the response. The values *success*, *malformedRequest*, *internalError*, *tryLater*, *sigRequired*, and *unauthorizaed* all must be supported.

### 6.2.1.2 responseBytes

The *responseBytes* field includes the responses. Each response is identified by an object identifier in the *responseType* field, which MUST be the BasicOCSPResponse as identified by id-pkix-ocsp-basic ( 1 3 6 1 5 5 7 48 1 1 ).

### 6.2.1.3 responseValue

The *requestorvalue* field contains BasicOCSPResponse included in an OCTET STRING.

#### 6.2.1.3.1 version

The version field identifies the version of the response. It MUST be version 1.

#### 6.2.1.3.2 responderID

The *responderID* field identifies the OCSP responder. It MUST use the *byKey* CHOICE. *byKey* includes the SHA-1 hash of the OCSP responder's public key.

#### 6.2.1.3.3 producedAt

The *producedAt* field indicates when this response was produced. GeneralizedTime shall be encoded as per RFC 5480 [2].

#### 6.2.1.3.4 responses

The *response* field includes the responses. It has four fields: *certID*, *certStatus*, *thisUpdate*, *NextUpdate*, and *singleExtensions*.

##### 6.2.1.3.4.1 certID

The *certID* field includes information necessary to identify the certificate for which the OCSP response was generated. It has four fields: *hashAlgorithm*, *issuerNameHash*, *issuerKeyHash*, and *serialNumber*.

###### 6.2.1.3.4.1.1 hashAlgorithm

The *hashAlgorithm* field indicates the hash algorithm used to compute the issuerNameHash and issuerKeyHash values. Both values MUST be computed using the SHA-1 algorithm. The object identifier for SHA-1 is ( 1 3 14 3 2 26 ).

###### 6.2.1.3.4.1.2 issuerNameHash

The *issuerNameHash* field includes the hash of the certificate issuer's name for which the OCSP requestor wanted status information. The hash shall be calculated over the DER encoding of the issuer's name field in the certificate being checked.

###### 6.2.1.3.4.1.3 issuerKeyHash

The *issuerKeyHash* field includes the hash of the certificate issuer's key for which the OCSP requestor wanted status information. It may be taken from the device or server certificate's authority key identifier extension.

###### 6.2.1.3.4.1.4 serialNumber

The *serialNumber* field includes the serial number of the certificate for which the requestor wanted status information. The value is copied from the certificate's *serialNumber* field.

###### 6.2.1.3.4.2 certStatus

The *certStatus* field indicates the status of the certificate: *good*, *revoked*, or *unknown*.

###### 6.2.1.3.4.3 thisUpdate

The *thisUpdate* field indicates when the status is known to be correct. GeneralizedTime shall be encoded as per RFC 5480 [2].

#### **6.2.1.3.4.4 nextUpdate**

The *nextUpdate* field indicates the time at which or before new information will be available. This field **MUST** be included. GeneralizedTime shall be encoded as per RFC 5480 [2].

#### **6.2.1.3.4.5 singleExtension**

WiMAX OCSP responses **SHOULD NOT** include *singleExtensions*.

#### **6.2.1.3.5 responseExtensions**

WiMAX OCSP responses **SHOULD NOT** include *responseExtensions*.

#### **6.2.1.3.6 signatureAlgorithm**

The *signatureAlgorithm* field indicates the algorithm used to generate the *signature* field. The signature algorithm **MUST** be sha256WithRSAEncryption as identified by ( 1 2 840 113549 1 1 11 ).

#### **6.2.1.3.7 signature**

The *signature* field includes the digital signature of the OCSP response. It is a BIT STRING.

#### **6.2.1.3.8 certs**

The *certs* field includes the certificate used to sign the OCSP response and any other certificates the OCSP signer think the client might need to validate the certification path.