

ICS 35.100.70
CCS L 79



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 19713-2005

**Information Technology - Security Techniques - Public Key
Infrastructure - Online Certificate Status Protocol
(English Translation)**

Issued on: April 19, 2005

Implemented on: October 1, 2005

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine**

Table of Contents

Foreword...	3
1 Scope...	4
2 Normative References...	4
3 Terms and Definitions...	5
4 Abbreviations...	5
5 General Rules...	6
5.1 Overview...	6
5.2 Request...	6
5.3 Response...	6
5.4 Anomalies...	8
5.5 Semantics of thisUpdate, nextUpdate, and producedAt...	8
5.6 Pre-generated response...	9
5.7 OCSP signature agency's commission...	9
5.8 CA key leakage...	9
6 Functional Requirements...	9
6.1 Certificate content...	9
6.2 Receiving requirements for signature response...	10
7 Specific Protocol...	10
7.1 Convention...	10
7.2 Request...	10
7.3 Response...	12
7.4 Mandatory/optional cryptographic algorithms...	15
7.5 Extension...	15
8 Security Consideration...	17
Appendix A (Informative) OCSP on the HTTP...	19
Appendix B (Normative) OCSP Defined by ASN.1...	21

1 Scope

This Standard specifies a mechanism (i.e. Online Certificate Status Protocol - OSCP) for querying the status of a digital certificate without requesting a Certificate Revocation

List (CRL). This mechanism can replace CRL or be used as a supplement to periodically

check CRL; so that timely get the information about the status of the certificate revocation. This Standard mainly describes as follows.

- a) Specify the request form for the online certificate status protocol;
- b) Specify the response form for the online certificate status protocol;
- c) Analyze various anomalies that may occur when processing response to the online certificate status protocol;
- d) Illustrate the application of the online certificate status protocol based on the Hypertext Transfer Protocol (HTTP);
- e) Adopt the Abstract Syntax Notation 1 (ASN.1) to describe the online certificate status protocol.

This Standard is applicable to all types of applications and computing environments based on the public key infrastructure.

2 Normative References

The provisions in following documents become the provisions of this Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions do not apply to this Standard, however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

ISO/IEC 8824-1.2002 Abstract Syntax Notation One (ASN.1) - Part 1.

Specification of Basic Notation

RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

5.1 Overview

As an alternative or complementary method for periodically checking CRL, OCSP is essential in cases where information about the status of certificate revocation must be obtained in a timely manner.

OCSP enables an application to determine the (revocation) status of an identity certificate. OCSP can be used to meet operational requirements that require more timely revocation information than checking CRL; it can also be used to obtain additional status information. The OCSP requester issues a status request to the

OCSP responder, defers accepting the certificate to be queried until the responder provides a response.

This Standard specifies the data that needs to be exchanged between the application that checks the status of the certificate and the server that provides the certificate status query.

5.2 Request

The OCSP request contains the following data.

- a) The version of the protocol;
- b) A service request;
- c) The target certificate identifier;
- d) The optional extensions that the OCSP responder can handle, such as OCSP requester's signature, random number.

In response to a request, the OCSP responder shall determine.

- a) Whether the message format is correct;
- b) Whether the responder is configured with the required service;
- c) Where the request contains the information needed by the responder.

If any of the above conditions are not satisfied, the OCSP responder shall issue an error message; otherwise, an explicit response shall be returned.

5.3 Response

The OCSP response can be of different types; the response consists of the two parts.

response type and response entity. This Standard only specifies one type of OCSP b) Revoked. indicates that the certificate has been revoked (permanently or temporarily).

c) Unknown. indicates that the responder can't authenticate the certificate to be verified (including OCSP responder certificate and the certificate to be verified are not issued by the same CA).

5.4 Anomalies

When an error occurs, the OCSP responder returns an error message. These messages can't be signed. The error can be the following categories.

- a) MalformedRequest (incomplete application). the request received by the OCSP responder (server) does not follow the OCSP syntax;
- b) InternalError. The OCSP responder is in an uncoordinated working state and shall query to another responder again;
- c) TryLater. The OCSP responder is in running state; can't return the status of the requested certificate indicating that the required service exists, but temporarily unable to respond;

- d) SigRequired. The responder requires the requester to sign the request;
- e) Unauthorized. The query was submitted to the responder by an unauthorized requester.

5.5 Semantics of thisUpdate, nextUpdate, and producedAt

Each response can contain three time-fields, namely, thisUpdate, nextUpdate and ProducedAt. The semantics of these fields indicate as follows.

- a) thisUpdate. this update time; the state that requires to be indicated is correct time;
- b) nextUpdate. next update time; indicate that certificate state is correct before this time; and the certificate status update information can be obtained again at this time;
- c) producedAt. the time of issue; the OCSP responder signs the response time.

If the nextUpdate is not set, the responder shall indicate that the revocation information for the update is available at any time. Given that OCSP updates the status of certificates in real time; this Standard recommends not setting the field of nextUpdate;

thisUpdate is defined as the time at which the CA issues the certificate status;

producedAt is the time at which the OCSP issues the response.

6.2 Receiving requirements for signature response

- a) The OCSP client shall acknowledge that OCSP response before it is considered valid;
- b) The certificate identified in the response received shall be consistent with the certificate in the request;
- c) The signature of the responder is valid;
- d) The responder's signer identity shall be consistent with the intended receiver of the request;
- e) The signer has been authorized to sign the response;
- f) The time (thisUpdate) indicating the status of the certificate shall be the current most recent time;
- g) If the field nextUpdate is set, then it shall be later than the current time of the client.

7.1 Convention

This Standard uses abstract syntax notation 1 (ASN.1) to describe the specific protocol content; the syntax of ASN.1 refers to some terms defined by RFC 2459; the complete

OCSP protocol description is given in Appendix B. The OCSP request format and response format for HTTP are described in RFC 2616 and see Appendix A. For signature calculation,