ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 19713-2025

Replacing GB/T 19713-2005

Cybersecurity technology - Public key infrastructure - Online certificate status protocol

网络安全技术 公钥基础设施 在线证书状态协议

Issued on: February 28, 2025 **Implemented on: September 1, 2025**

Issued by: the State Administration for Market Regulation of the People's Republic of China, Standardization Administration of the People's Republic of China

Table of Contents

Foreword

This document was issued on 28 February 2025 by the the State Administration for Market Regulation of the People's Republic of China, Standardization Administration of the

People's Republic of China and takes effect on 1 September 2025.

It is a GB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies.

The document runs to 16 pages in translation. The identification, the dates, the table of contents and the clauses reproduced on this page are taken from the standard itself.

This document is drafted in accordance with GB/T 1.1-2020 Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents.

This document replaces GB/T 19713-2005 Information technology - Security techniques - Public key infrastructure - Online certificate status protocol. In addition to structural adjustments and editorial changes, the following main technical changes have been made with respect to GB/T 19713-2005:

a) The sentence "this standard is applicable to various applications and computing environments based on public key infrastructure" has been modified to "this document is applicable to the construction of public key infrastructure and secure applications based on the online certificate status protocol (OCSP), among others" (see Clause 1 hereof; Clause 1 of Edition 2005);

b) A diagram of relationship among the parties in the OCSP protocol has been added to the "General provisions" (see 5.1 hereof; 5.1 of Edition 2005);

c) The term "hash signature of response" has been modified to "digital signature of response" [see 5.3 b) hereof; 5.3 f) of Edition 2005];

d) The scope of use for the "revoked" status has been modified to allow this response status to be used for certificates that have never been issued [see 5.3 d) hereof; 5.3 of Edition 2005];

e) The response requirements for status requests regarding unissued certificates have been added [see 5.3 e) hereof];

f) The scope of use for the unauthorized error response has been modified (see 5.4 hereof; 5.4 of Edition 2005);

g) The definition of the revocationTime semantic has been added (see 5.5 hereof);

h) The support for SM2 and SM3 algorithms has been added (see 7.1 and 7.2 hereof);

i) The definitions of the Signature, Extensions, CertificateSerialNumber, SubjectPublicKeyInfo, Name, AlgorithmIdentifier, and CRLReason structures in the OCSP ASN.1 syntax have been added (see 7.1 hereof);

j) Annotations for the lightweight OCSP request syntax have been added (see 7.2.2 hereof);

k) The requirements for time in the lightweight OCSP protocol have been added (see

7.3.2.1 hereof);

l) The sentence "the locally configured OCSP signing authority entity contains a certificate that matches the certificate whose status is to be verified" has been modified to "the locally configured OCSP responder certificate matches the OCSP responder certificate" (see 7.3.2.2.2 hereof; 7.3.2.2 of Edition 2005);

m) A method for checking the revocation status of authorized responders in a lightweight OCSP environment has been added [see 7.3.2.2.3 d) hereof];

n) The subclause "7.3.2.3 Basic response" has been added, and it has been clarified that the ResponderID field corresponds to the OCSP responder's signature certificate (see 7.3.2.3 hereof);

o) The requirements for the OCSPResponse structure in lightweight OCSP responses have been added [see 7.3.2.3 e) hereof];

p) The subclause "7.3.2.2.4 Certificate status issuance" has been added, describing the standards that OCSP responders shall follow for obtaining certificate status (see 7.3.2.2.4 hereof);

q) Mandatory and optional cryptographic algorithms have been deleted (see 7.4 of Edition 2005);

r) The ASN.1 syntax for Nonce has been modified, and the length range for Nonce has been specified (see 7.4.2 hereof; 7.5.1 of Edition 2005);

s) The standard to be followed for CRL entry extensions has been modified (see 7.4.6 hereof; 7.5.5 of Edition 2005);

t) The "PreferredSignatureAlgorithms" extension has been added, which can be included in the request message to specify the signature algorithm the requester prefers the responder to use, with SM3WithSM2 recommended as the preferred algorithm (see 7.4.8 hereof);

u) The "extended-revoke definition" extension has been added, which indicates that the responder supports the extended use of the "revoked" response for unissued certificates as defined in 5.3 (see 7.4.9 hereof);

v) The ASN.1 module using the 2008 syntax of ASN.1 has been modified to add support for using SM2 and SM3 algorithms (see Annex A hereto; Annex B to Edition 2005); the syntax specification for lightweight OCSP ASN.1 and support for using SM2 and SM3 algorithms have been added (see Annex A hereto);

w) The construction of lightweight OCSP requests and responses has been added (see Annex B.2 hereto);

x) The clause "Security considerations" has been moved from the main text to Annex D, with the content supplemented and improved (see Annex D hereto; Clause 8 of Edition

2005).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing body of this document shall not be held responsible for identifying any or all such patent rights.

This document was proposed by and is under the jurisdiction of SAC/TC 260 National Technical Committee on Cybersecurity of Standardization Administration of China.

--This document was first issued as GB/T 19713-2005 in 2005;

Cybersecurity technology - Public key infrastructure - Online certificate status protocol

It replaces GB/T 19713-2005, which is superseded.

1 Scope

GB/T 19713-2025 specifies the online certificate status protocol for Chinese public key infrastructure. A certificate can be revoked before it expires, and a relying party that does not check is trusting a credential the issuer has already withdrawn; OCSP is how that check is made in real time rather than by downloading a revocation list. This edition is the Chinese profile of the protocol: the request and response formats and their encoding, the status values and their meaning, the signing of responses and the trust model for the responder, the handling of nonces and of replay, the caching and validity intervals, the error conditions, the transport bindings, and the requirements arising from the Chinese cryptographic algorithms SM2 and SM3, which is what makes a national version necessary rather than a straight adoption. The 2025 edition replaces GB/T 19713-2005 and takes effect on 1 September 2025. For anyone building a PKI, a browser, a signing service or a payment system for the Chinese market, this is the governing specification.

This document presents a mechanism for querying the status of digital certificates without requesting a certificate revocation list (CRL), that is, online certificate status protocol (OCSP), including the content and syntax specifications of the OCSP.

This document is applicable to the construction of public key infrastructure and secure applications based on the online certificate status protocol (OCSP), among others.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 16263.1 Information technology - ASN.1 encoding rules - Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished