ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 19713—2025
代替 GB/T 19713—2005

网络安全技术　公钥基础设施 在线证书状态协议

Cybersecurity technology—Public key infrastructure—Online certificate status protocol

2025-02-28 发布　　2025-09-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 19713—2005《信息技术　安全技术　公钥基础设施　在线证书状态协议》，与GB/T 19713—2005相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改“本标准适用于各类基于公开密钥基础设施的应用程序和计算环境”为“本文件适用于公钥基础设施的建设以及基于在线证书状态协议的安全应用等”（见第1章，2005年版的第1章）；
b) 在“通则”中增加了OCSP协议中各方之间的关系图（见5.1，2005年版的5.1）；
c) 更改了“响应的哈希签名”为“响应的数字签名”[见5.3 b)，2005年版的5.3 f)]；
d) 更改了revoked（已撤销）状态的使用范围，允许对从未签发过的证书使用此响应状态[见5.3 d)，2005年版的5.3]；
e) 增加了对未签发证书状态请求的响应要求[见5.3 e)]；
f) 更改了unauthorized（未授权）错误响应的使用范围（见5.4，2005年版的5.4）；
g) 增加了revocationTime（撤销时间）语义的定义（见5.5）；
h) 增加了SM2、SM3算法的支持（见7.1和7.2）；
i) 增加了OCSP ASN.1语法中Signature、Extensions、CertificateSerialNumber、SubjectPublicKeyInfo、Name、AlgorithmIdentifier和CRLReason结构的定义（见7.1）；
j) 增加了轻量级OCSP请求语法的注解（见7.2.2）；
k) 增加了轻量级OCSP协议对时间的要求（见7.3.2.1）；
l) 更改了“本地配置的OCSP签名权威实体中包含了与待验证状态的证书相匹配的证书”为“本地配置的OCSP响应者证书与OCSP响应者证书相匹配”（见7.3.2.2.2，2005年版的7.3.2.2）；
m) 增加了轻量级OCSP环境下授权响应者的撤销状态检查方法[见7.3.2.2.3 d)]；
n) 增加了“7.3.2.3　基础响应”，并阐明了ResponderID字段对应于OCSP响应者签名证书（见7.3.2.3）；
o) 增加了轻量级OCSP响应中对OCSPResponse结构的要求[见7.3.2.3 e)]；
p) 增加了“7.3.2.2.4 证书状态发布”，对OCSP响应者获取证书状态应遵循的标准进行了描述（见7.3.2.2.4）；
q) 删除了强制的密码算法和可选的密码算法（见2005年版的7.4）；
r) 更改了Nonce的ASN.1语法，并规定了Nonce的长度范围（见7.4.2，2005年版的7.5.1）；
s) 更改了CRL条目扩展应遵循的标准（见7.4.6，2005年版的7.5.5）；
t) 增加了“优先使用的签名算法”扩展，该扩展可包含在请求消息中，以指定请求者希望响应者使用的签名算法，建议优先算法使用SM3WithSM2（见7.4.8）；
u) 增加了“扩展撤销定义”扩展，该扩展表明响应者支持对5.3中定义的未签发证书的“revoked（已撤销）”响应的扩展使用（见7.4.9）；
v) 更改了使用ASN.1的2008语法的ASN.1模块，增加支持使用SM2、SM3算法（见附录A，2005年版的附录B）；增加了轻量级OCSP ASN.1的语法规范，并增加支持使用SM2、SM3算法（见附录A）；
w) 增加了轻量级OCSP请求及响应构造（见附录B.2）；
x) 更改正文的“安全考虑”为附录D，并补充完善了内容（见附录D，2005年版的第8章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:普华诚信信息技术有限公司、上海信息安全基础设施研究中心有限责任公司、上海市数字证书认证中心有限公司、北京数字认证股份有限公司、郑州信大捷安信息技术股份有限公司、深圳市电子商务安全证书管理有限公司、中电科网络安全科技股份有限公司、河南金盾信安检测评估中心有限公司、国家密码管理局商用密码检测中心、格尔软件股份有限公司、三六零数字安全科技集团有限公司、数安时代科技股份有限公司、华为技术有限公司。

本文件主要起草人:梁佐泉、顾青、田文晋、王亚红、冯四风、高五星、张子鸣、付丽丽、王志威、黄成杭、赵艳红、石韶博、陈荦祺、赵鹰侠、张永强、刘为华、郑会涛、岳小阳、梁宏、张绍博、郑强、张志磊、杜志强、曾光。

本文件及其所代替文件的历次版本发布情况为:

——2005 年首次发布为 GB/T 19713—2005;

——本次为第一次修订。

网络安全技术　公钥基础设施
在线证书状态协议

1　范围

本文件给出了一种无需请求证书撤销列表(CRL)即能查询数字证书状态的机制,即在线证书状态协议,包括在线证书状态协议的协议内容、语法规范。

本文件适用于公钥基础设施的建设以及基于在线证书状态协议的安全应用等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 16263.1　信息技术 ASN.1 编码规则　第 1 部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范

GB/T 19714—2005　信息技术　安全技术　公钥基础设施　证书管理协议

GB/T 20518—2018　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069　信息安全技术　术语

GB/T 32915　信息安全技术　二元序列随机性检测方法

GB/T 33560—2017　信息安全技术　密码应用标识规范

GB/T 35276—2017　信息安全技术　SM2 密码算法使用规范

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

请求者　requester

申请在线证书状态查询服务的实体或设备。

3.2

响应者　responder

提供在线证书状态查询服务的实体或设备。

3.3

在线证书状态协议　online certificate status protocol;OCSP

一种无需请求证书撤销列表(CRL)即能查询数字证书状态的协议。

4　缩略语

下列缩略语适用于本文件。

CA:证书认证机构(Certification Authority)