ICS 35.100.70
L 79

# 中华人民共和国国家标准

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

**Information technology—Security techniques—Public key infrastructure—Online certificate status protocol**

2005-04-19 发布　　2005-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准主要参考 IETF(互联网工程特别工作组)RFC2560 文件制定,其中对某些功能项的实施方法,结合实际经验提出了一些特别的建议。

本标准中凡涉及密码算法相关内容,按国家有关法规执行。

本标准的附录 B 为规范性附录,附录 A 为资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会(TC 260)归口。

本标准主要起草单位:国家信息安全基础设施研究中心、国家信息安全工程技术研究中心、中国电子技术标准化研究所、国瑞数码安全系统有限公司。

本标准主要起草人:顾青、吴志刚、邓琳、陈刚、王于、苏恒、李跃、黄峰、郭晓雷、袁文恭、李丹、上官晓丽、王利。

# 信息技术　安全技术　公钥基础设施 在线证书状态协议

## 1　范围

本标准规定了一种无需请求证书撤销列表(CRL)即可查询数字证书状态的机制(即在线证书状态协议——OCSP)。该机制可代替 CRL 或作为周期性检查 CRL 的一种补充方式,以便及时获得证书撤销状态的有关信息。本标准主要描述了以下内容:

a)　具体描述了在线证书状态协议的请求形式;

b)　具体描述了在线证书状态协议的响应形式;

c)　分析了处理在线证书状态协议响应时可能出现的各种异常情况;

d)　说明了在线证书状态协议基于超文本传输协议(HTTP)的应用方式;

e)　提供了采用抽象语法记法 1(ASN.1)描述的在线证书状态协议。

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。

## 2　规范性引用文件

下列文件中的条款通过本标准的应用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

ISO/IEC 8824-1:2002　抽象语法记法一(ASN.1) 第 1 部分:基本记忆规范

RFC 2459　因特网 X.509 公开密钥基础设施证书和证书撤销列表框架

RFC 2616　超文本传输协议(HTTP 1.1)

## 3　术语和定义

下列术语和定义适用于本标准。

3.1

**证书扩展项　extensions**

在证书的结构中,该域定义了证书的一些扩展信息。

3.2

**证书序列号　certificate serial number**

为每个证书分配的唯一整数值,在 CA 颁发的证书范围内,此整数值与该 CA 所颁发的证书相关联一一对应。

3.3

**请求者　requester**

申请在线证书状态查询服务的主体。

3.4

**响应者　responder**

提供在线证书状态查询服务的主体。

## 4　缩略语

下列缩略语适用于本标准。