ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25059—2010

信息安全技术　公钥基础设施 简易在线证书状态协议

Information security technology—Public Key Infrastructure—Simple Online Certificate Status Protocol

2010-09-02 发布　　2011-02-01 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

本标准的附录A为资料性附录，附录B为规范性附录。

本标准由全国信息安全标准化技术委员会(TC 260)提出并归口。

本标准主要起草单位：上海信息安全工程技术研究中心、国家信息安全工程技术研究中心。

本标准主要起草人：袁峰、郭晓雷、杨恒亮、谢安明、李增欣、苏瑞丹。

本标准责任专家：袁文恭。

引　言

在基于 PKI 的众多应用中，存在这种情况，某个应用系统的服务器在完成自身的功能时，需要进行大量实时的证书状态查询操作。在这种情况下，应用服务器对证书状态查询操作的性能与效率要求比较高，如果按照标准 OCSP 协议进行操作，协议数据单元复杂，签名和验签操作的开销都使得证书状态的查询操作成为应用服务器性能的瓶颈。而在实际应用的过程中，应用服务器往往和 OCSP 服务器位于同一可信网络或网段中，所以，为消除这一性能瓶颈，我们需要将标准 OCSP 协议进行简化，设计实现一个轻量级的证书状态查询协议。

信息安全技术　公钥基础设施
简易在线证书状态协议

1　范围

本标准规定了一种简易的在线证书状态协议——SOCSP。该协议可作为标准 OCSP 协议的补充。本标准主要描述了以下内容：

a)　具体描述了简易在线证书状态协议的请求形式；

b)　具体描述了简易在线证书状态协议的响应形式；

c)　分析了处理简易在线证书状态协议响应时可能出现的各种异常情况；

d)　说明了简易在线证书状态协议基于超文本传输协议(HTTP)的应用方式。

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引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)或修订版均不使用于本标准，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。

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

3　术语和定义

下列术语和定义适用于本标准。

3.1

证书序列号　certificate serial number

由证书认证机构产生的唯一对应于每个证书的编号。

3.2

哈希　hash

将值从一个大的(可能很大)定义域映射到一个较小值域的(数学)算法。

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。

CRL　证书撤销列表(Certificate Revocation List)

DER　特异编码规则(Distinguished Encoding Rules)

HTTP　超文本传输协议(Hypertext Transfer Protocol)

MAC　信息验证码(Message Authentication Codes)