ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25055—2010

信息安全技术 公钥基础设施安全支撑平台技术框架

Information security techniques—
Public Key Infrastructure security supporting platform framework

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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
公钥基础设施安全支撑平台技术框架
GB/T 25055—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 44 千字
2010 年 11 月第一版 2010 年 11 月第一次印刷
*
书号:155066·1-40461

目　　次

前　言

本标准的附录A、附录B和附录C为资料性附录。

本标准由全国信息安全标准化技术委员会(SAC/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:袁文恭、刘平、何义大、郭晓雷、袁峰、洪焕健。

引　言

我国信息化的快速发展，使构建安全支撑平台成为国家信息系统安全建设急需解决的重要问题。本标准提出了一个基于PKI技术的安全支撑平台技术框架，规定了各子系统应遵循的通用技术框架标准，为我国信息安全基础设施建设、为应用系统的安全需求提供带共性的安全技术支撑。安全支撑平台以密码技术为基础，为信息系统提供统一、通用的网络信任服务、信息安全保护服务、网络安全保护服务、密码与密钥支撑服务，以满足信息系统实体对网络通信的真实性、保密性、完整性、抗抵赖性等安全保障需求。

本标准与我国已经制定的信息安全国家标准GB/T 20518—2006、GB/T 19714—2005和GB/T 25056—2010等标准紧密结合，能更好地规范我国信息安全基础设施中安全支撑平台的建设，更好地解决信息安全基础设施的互操作性问题，进一步促进我国的信息化建设和国民经济的发展。

在本标准实施过程中，涉及到公钥密码基础设施应用技术体系及其相关接口技术和密码技术的具体应用时，应按照国家密码管理局发布的有关规定和相关技术规范执行。

本标准涉及的数字签名系统的实施与运行应遵守《中华人民共和国电子签名法》。

信息安全技术
公钥基础设施安全支撑平台技术框架

1 范围

本标准规定了基于公钥基础设施的安全支撑平台的技术框架。

本标准适用于网络信息系统中安全支撑平台的设计、建设、检测、运营及管理，为网络信息系统和业务应用系统提供统一可信的软、硬件安全支撑服务。同时，本标准还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考，指导安全产品生产商对安全支撑平台的设计和建设，提高安全产品的可信性与互操作性。对于特定的安全支撑平台的建设，可根据具体的业务需求和情况进行灵活配置。

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。

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

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 20275—2006 信息安全技术 入侵检测系统技术要求和测试评价方法

GB/T 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 20518—2006 信息安全技术 公钥基础设施 数字证书格式

GB/T 20519—2006 信息安全技术 公钥基础设施 特定权限管理中心技术规范

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求

GB/T 25056—2010 信息安全技术 证书认证系统密码及其相关安全技术规范

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

RFC 1777 LDAP 轻量级目录访问协议

国家密码管理局 《数字证书认证系统密码协议规范》，2007 年 8 月 13 日第 11 号公告

3 术语和定义

下列术语和定义适用于本标准。

3.1

属性授权机构 Attribute Authority

通过发布属性证书来分配特权的证书认证机构。

3.2

属性证书 attribute certificate

属性授权机构进行数字签名的数据结构，把持有者的身份信息与一些属性值绑定。

3.3

属性证书注册机构 Attribute Registration Authority

属性证书的审核注册申请机构，又称属性注册权威。