ICS 35.040
L 80

中华人民共和国国家标准

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

Information security techniques—Specifications of cryptograph and related security technology for certificate authentication system

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

本标准附录A、附录B、附录C、附录D均为资料性附录。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)归口。

本标准主要起草单位:长春吉大正元信息技术股份有限公司、国家密码管理局商用密码研究中心、国家信息安全工程技术研究中心。

本标准相关参与起草单位:无锡江南信息安全工程技术中心、上海格尔软件股份有限公司、北京信安世纪科技有限公司、济南得安计算机技术有限公司、北京创原天地科技有限公司、卫士通信息产业股份有限公司、天津市国瑞数码安全系统有限公司、兴唐通信科技股份有限公司、中国科学院数据与通信保护研究教育中心、北京格方网络技术有限公司、北京天融信科技有限公司、维豪信息技术有限公司等。

本标准主要起草人:邱泽军、王永传、何立波、谢永泉、姜玉琳、刘海龙、邓开勇、罗鹏、田景成、赵丹、张文建、李大为。

袁文恭、刘平、何良生、邱钢、陈连俊等专家指导了本标准的起草。

信息安全技术　证书认证系统密码及其相关安全技术规范

1　范围

本标准规定了为公众服务的数字证书认证系统的设计、建设、检测、运行及管理规范。本标准为实现数字证书认证系统的互连互通和交叉认证提供统一的依据，指导第三方证书认证机构的数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用。

本标准适用于第三方证书认证机构的数字证书认证系统的设计、建设、检测、运行及管理。非第三方证书认证机构的数字证书认证系统的建设、运行及管理，可参照本标准。

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 2887—2000　电子计算机场地通用规范

GB/T 9361—1988　计算机场地安全要求

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB 50174—2008　电子信息系统机房设计规范

SJ/T 10796—1996　计算机机房用活动地板技术条件

3　术语和定义

下列术语和定义适用于本标准。

3.1

认证机构证书　authority certificate

签发给证书认证机构的证书。

3.2

CA 证书　CA certificate

由一个 CA 给另一个 CA 签发的证书，一个 CA 也可以为自己签发证书，这是一种自签名的证书。

3.3

证书认证系统　certificate authentication system

对生命周期内的数字证书进行全过程管理的安全系统。

3.4

证书策略　certificate policy

是一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和(或)具体应用类的适用性。例如，一个特定的证书策略可以指出一个类型的证书对在一定的价格幅度下商品交易的电子数据处理的认证的适用性。

3.5

证书撤销列表　certificate revocation list；CRL

标记一系列不再被证书发布者所信任的证书的签名列表。