



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	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 证书认证系统	3
5.1 概述	3
5.2 功能描述	3
5.3 系统设计	5
5.4 数字证书	9
5.5 证书撤销列表	9
6 密钥管理中心	9
6.1 结构描述	9
6.2 功能描述	10
6.3 系统设计	10
6.4 KMC 与 CA 的安全通信协议	12
7 密码算法、密码设备及接口	12
7.1 密码算法	12
7.2 密码设备	13
7.3 密码服务接口	13
8 协议	13
8.1 证书管理协议	13
8.2 证书验证协议	15
8.3 安全通信协议	15
9 证书认证中心建设	15
9.1 系统	15
9.2 安全	17
9.3 数据备份	19
9.4 可靠性	19
9.5 物理安全	19
9.6 人事管理制度	20
10 密钥管理中心建设	20
10.1 建设原则	20
10.2 系统	20
10.3 安全	21
10.4 数据备份	21
10.5 可靠性	21
10.6 物理安全	21

10.7 人事管理制度 21

11 证书认证中心运行管理要求 22

11.1 人员管理要求 22

11.2 CA 业务运行管理要求 22

11.3 密钥分管要求 23

11.4 安全管理要求 23

11.5 安全审计要求 24

11.6 文档配备要求 24

12 密钥管理中心运行管理要求 25

12.1 人员管理要求 25

12.2 运行管理要求 25

12.3 密钥分管要求 25

12.4 安全管理要求 25

12.5 安全审计要求 25

12.6 文档配备要求 25

13 检测 25

13.1 概述 25

13.2 系统初始化 25

13.3 用户注册管理系统 26

13.4 证书/证书撤销列表生成与签发系统 26

13.5 证书/证书撤销列表存储与发布系统 27

13.6 证书状态查询系统 27

13.7 安全审计系统 27

13.8 密钥管理中心检测 27

13.9 系统安全性检测 28

13.10 其他安全产品和系统 28

附录 A (资料性附录) KMC 与 CA 之间的消息格式 29

A.1 概述 29

A.2 协议 29

附录 B (资料性附录) 安全通信协议 36

B.1 符号说明 36

B.2 身份鉴别 36

B.3 密钥交换 36

B.4 安全通信协议 37

附录 C (资料性附录) 密码设备接口函数定义及说明 39

C.1 应用类密码设备接口函数 39

C.2 证书载体接口函数 55

附录 D (资料性附录) 证书认证系统网络结构图 71

D.1 当 RA 采用 C/S 模式时 CA 的网络结构 71

D.2 当 RA 采用 B/S 模式时 CA 的网络结构 72

D.3 CA 与远程 RA 的连接 72

D.4 KMC 与多个 CA 的网络连接 73

参考文献 74

图 1 证书认证系统逻辑结构	4
图 2 用户注册管理系统逻辑结构	6
图 3 密钥管理中心逻辑结构	10
图 D.1 RA 采用 C/S 模式时 CA 的网络结构示意图	71
图 D.2 RA 采用 B/S 模式时 CA 的网络结构示意图	72
图 D.3 CA 与远程 RA 的连接示意图	72
图 D.4 KMC 与多个 CA 的网络连接示意图	73

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。