

《证书认证系统密码及其相关安全技术规范》

（目 次）

前言	VI
1 范围	1
2 规范性引用文件	1
3 术语和缩略语	1
3.1 术语	1
3.2 缩略语	3
4 证书认证系统	3
4.1 功能描述	4
4.2 系统设计	5
4.3 数字证书	9
4.4 证书注销列表	9
5 密钥管理系统	9
5.1 功能描述	9
5.2 系统设计	10
5.3 KMC 与 CA 的安全通信协议	12
6 密码算法、密码设备及接口	12
6.1 密码算法	12
6.2 密码设备	12
6.3 密码服务接口	13
7 协议	13
7.1 证书管理协议	13
7.2 证书验证协议	14
7.3 安全通信协议	15
8 证书认证中心建设	15
8.1 系统	15
8.2 安全	16
8.3 数据备份	18
8.4 可靠性	18
8.5 物理安全	18
8.6 人事管理制度	19
9 密钥管理中心建设	19
9.1 系统	19
9.2 安全	20
9.3 数据备份	20
9.4 可靠性	20
9.5 物理安全	20
9.6 人事管理制度	20
10 证书认证中心运行管理要求	20
10.1 人员管理要求	20
10.2 CA 业务运行管理要求	21
10.3 密钥分管要求	22

10.4 安全管理要求	22
10.5 安全审计要求	23
10.6 文档的配备	23
11 密钥管理中心运行管理要求	24
11.1 人员管理要求	24
11.2 运行管理要求	24
11.3 密钥分管	24
11.4 安全管理	24
11.5 安全审计	24
11.6 文档配备	24
12 检测	24
12.1 系统初始化	24
12.2 用户注册管理系统	24
12.3 证书/证书注销列表生成与签发系统	25
12.4 证书/证书注销列表存储与发布系统	25
12.5 证书状态查询系统	26
12.6 安全审计系统	26
12.7 密钥管理系统检测	26
12.8 系统安全性检测	26
12.9 其他安全产品和系统	27
附录 A KMC 与 CA 之间的消息格式 (资料性附录)	28
A.1 概述	28
A.1.1 请求	28
A.1.2 响应	28
A.1.3 回执	28
A.1.4 异常情况	28
A.2 协议	28
A.2.1 约定	28
A.2.2 请求	29
A.2.3 响应	31
A.2.4 回执	33
附录 B 安全通信协议 (资料性附录)	35
B.1 符号说明	35
B.2 身份认证	35
B.3 密钥交换	35
B.4 安全通信协议	36
附录 C 密码设备接口函数定义及说明 (资料性附录)	38
C.1 应用类密码设备接口函数	38
C.1.1 接口组成部分	38
C.1.2 宏定义	38
C.1.3 数据结构定义	39
C.1.4 错误码	41
C.1.5 函数定义及说明	44
C2 证书载体接口函数	54
C.2.1 宏定义	54

C.2.2 数据结构定义	54
C.2.3 函数定义和说明	56
C.2.4 返回代码	68
附录 D 证书认证系统网络结构图（资料性附录）	70
D.1 当 RA 采用 C/S 模式时 C.A 的网络结构	70
D.2 当 RA 采用 B/S 模式时 C.A 的网络结构	71
D.3 CA 与远程 RA 的连接	71
D.4 KMC 与多个 CA 的网络连接	72
附录 E 证书申请和下载格式（资料性附录）	73
E.1 证书申请格式	73
E.2 证书下载格式	73
参考文献	75