

ICS 35.040
L 80
备案号: 38312—2013



中华人民共和国密码行业标准

GM/T 0014—2012

数字证书认证系统密码协议规范

Digital certificate authentication system cryptography protocol specification

2012-11-22 发布

2012-11-22 实施

国家密码管理局 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 相关协议	2
5.1 概述及协议流程	2
5.1.1 内容概述	2
5.1.2 协议流程	2
5.2 CA 与 KM 系统间相关协议	5
5.2.1 概述	5
5.2.2 协议内容	6
5.2.3 密钥申请协议	6
5.2.4 响应	9
5.3 CA 与 LDAP 服务间相关协议	11
5.3.1 协议概述	11
5.3.2 发布协议	11
5.4 用户与 LDAP 服务间相关协议	13
5.4.1 协议概述	13
5.4.2 证书查询与下载协议	17
5.4.3 CRL 查询与下载协议	19
5.5 CA 与 OCSP/SOCSP 服务间相关发布协议	20
5.5.1 证书状态发布协议	20
5.5.2 SOCSP 证书状态查询协议	20
5.6 用户与 OCSP/SOCSP 服务间相关协议	20
5.6.1 OCSP 证书状态查询协议	20
5.6.2 SOCSP 证书状态查询协议	25
6 协议报文语法	25
6.1 加密数据报文	25
6.2 摘要数据报文	25
6.3 数字签名报文	26
6.4 数字信封报文	26
附录 A (规范性附录) 系统与格式定义	27
A.1 证书模板格式	27
A.2 证书撤销列表 CRL 格式	27

A.3	加密值	27
A.4	PKI 消息的状态码和故障信息	28
A.5	证书识别	29
A.6	带外根 CA 公钥	29
A.7	存档选项	30
A.8	发布信息	30
附录 B (资料性附录)	RA 与 CA 间相关协议	31
B.1	RA 的服务模式	31
B.2	RA 前台页面程序	31
B.3	RA 后台服务程序	31
B.4	证书申请协议	35
B.5	证书撤销协议	38
B.6	证书更新协议	38
B.7	证书冻结协议	38
B.8	证书解冻协议	38
B.9	密钥恢复协议	38
附录 C (资料性附录)	协议报文实例	40
C.1	PKIMessage 通用协议实例	40
C.2	证书申请、回应协议报文实例	41
C.3	证书查询下载协议报文实例	46
C.4	OCSP 证书状态查询协议报文实例	48
C.5	密钥恢复协议报文	50
附录 D (规范性附录)	非实时发布证书协议流程	52