



中华人民共和国国家标准

GB/T 19771—2005

信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范

Information technology—Security technology—Public key infrastructure
—Minimum interoperability specification for PKI components

2005-05-25 发布

2005-12-01 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



060609000513

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	2
3 术语和定义	3
4 缩略语	5
5 PKI 组件规范	5
5.1 概述	5
5.2 证书认证机构(CA)	5
5.2.1 概述	5
5.2.2 与互操作性有关的 CA 功能要求	6
5.2.3 电子事务集合	7
5.3 注册机构(RA)	8
5.3.1 概述	8
5.3.2 与互操作性有关的 RA 功能要求	8
5.3.3 事务集合	9
5.4 证书持有者规范	9
5.4.1 概述	9
5.4.2 与互操作性相关的 PKI 证书持有者功能要求	9
5.4.3 证书持有者事务集合	9
5.5 客户规范	10
5.5.1 客户概述	10
5.5.2 与互操作性相关的 PKI 客户功能要求	10
5.5.3 PKI 客户事务集合	10
6 数据格式	10
6.1 数据格式概述	10
6.2 证书格式	10
6.2.1 证书字段	10
6.2.2 加密算法	12
6.2.3 证书扩展	15
6.3 证书撤销列表	17
6.3.1 证书撤销列表概述	17
6.3.2 CRL 字段	18
6.3.3 CRL 扩展	18
6.3.4 CRL Entry 扩展	20
6.4 证书认证路径	21
6.5 事务消息格式	22
6.5.1 事务消息格式概述	22

6.5.2	全体 PKI 消息组件	22
6.5.3	通用数据结构	24
6.5.4	特殊操作的数据结构	28
6.6	PKI 事务	30
6.6.1	PKI 事务概述	30
6.6.2	RA 发起的注册请求	30
6.6.3	新实体的自我注册请求	32
6.6.4	已知实体的自我注册请求	34
6.6.5	证书更新	36
6.6.6	PKCS#10 自我注册请求	38
6.6.7	撤销请求	40
6.6.8	集中产生密钥对和密钥管理证书申请	42
6.6.9	组合证书申请	44
6.6.10	从资料库请求证书	45
6.6.11	从资料库请求 CRL	45
附录 A(规范性附录)	X.509 v3 证书 ASN.1	46
附录 B(规范性附录)	证书和 CRL 扩展 ASN.1	50
附录 C(规范性附录)	ASN.1 Module for transactions	58
附录 D(规范性附录)	证书请求消息格式 ASN.1 Module	65