ICS
CCS

T/CMA

中 国 计 量 协 会 团 体 标 准

T/CMA ZK 158—2024

计量实体的数字身份证书要求

Regulations of Digital Certificates for metrology entities

2024－XX－XX 发布　　2024－XX－XX 实施

中 国 计 量 协 会　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国计量协会提出。

本文件由中国计量协会智库工作委员会归口。

本文件起草单位：

本文件主要起草人：

计量实体的数字身份证书要求

1 范围

本文件规定了计量数字化后各实体的数字身份证书的应用要求。
本文件适用于采用数字证书实现计量实体数字化身份认证的系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式
GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范
GB/T 25069 信息安全技术 术语
GB-T 28447 信息安全技术 电子认证服务机构运营管理规范
GB/T 32905 信息安全技术 SM3密码杂凑算法
GB/T 32918.1 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分 总则
GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分 数字签名算法
GB/T 32918.3 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分 密钥交换协议
GB/T 32918.4 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分 公钥加密算法
GB/T 32918.5 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分 参数定义
GB/T 35276 信息安全技术 SM2密码算法使用规范

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

证书认证机构 Certificate authority

对数字证书进行全生命周期管理的实体，也称为电子认证服务机构。

3.2

数字证书 Digital certificate

由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

注1：数字证书按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.3

证书注册机构　Registration authority

受理数字证书的申请、更新、恢复和注销等业务的实体。

3.4

SM2 算法　SM2 algorithm

由GB/T 32918（所有部分）定义的算法。

3.5

SM3 密码杂凑算法　SM3 cryptographic hash algorithm

由GB/T 32905定义的算法。

4　计量实体特征

计量实体分为人员、机构和设备三类。数字证书中应体现的各实体的特征字段见图 1。

人员	机构	设备
姓名	机构名称	设备名称
证件类型	法定代表人	设备用途
证件号码	机构证件类型	所有者
联系电话	证书颁发机构	所有者证件类型
电子邮件	机构证件号码	所有者证件号码
……	联系电话	所有者联系电话
	联系地址	……
	邮政编码	
	……	

图1　计量实体的特征字段

5　数字证书字段

计量实体的数字证书应符合GB/T 20518定义的格式。计量实体特征信息应写入主体和扩充域中。

主体项应包含一个X.500的甄别名称（DN），至少包含下列条目：

a）cn：Common Name，通用名称；

b）b）o：Organization，机构；

c）ou：Organizational Unit，部门；

d）title：职位；

e）c：Country，国家；

f）st：State or Province，州或省；

g）l：Locality，地区。

个人实体的数字证书扩充域中应至少包含下列扩展：

a）identifyCode：个人身份标识码；

b）insuranceNumber：个人社会保险号。

机构实体的数字证书扩充域中应至少包含下列扩展：

a）iCRegistrationNumber：企业工商注册号；

b）organizationCode：企业组织机构代码；

c）taxationNumber：企业税号。

6 数字身份证书申请、签发、使用的流程和规章制度

6.1 业务流程类型

计量实体数字证书涉及三项业务流程：

a）新证书申请流程：申请人向证书认证机构申请新的数字证书；

b）证书主动吊销流程：证书所有者向证书认证机构主动申请吊销其持有的数字证书；

c）证书被动吊销流程：证书认证机构有证据表明证书所有者违规使用其持有的数字证书，单方面吊销证书。

详细业务流程见附录A。业务流程由申请材料提交和审核两阶段组成。

在新证书申请流程和证书主动吊销流程中，申请材料包括：

a）申请表；

b）授权书；

c）机构证件复印件；

d）身份证件复印件。

在新证书申请流程和证书主动吊销流程中，审核阶段由形式审查和真实性审查两部分组成。形式审查的是为了确保申请人提交的材料在内容格式方面没有错误；真实性审查是在形式审查的基础上，对申请人提交信息的真实性进行核实。

所有审核操作均应在数字化的Web系统中完成。

6.2 审核系统设计

审核系统由三个子系统组成：

a）证书注册中心（RA）：负责与外部用户交互和具体业务流程的实现；

b） 密钥管理中心（KMC）：与服务器密码机交互，完成基本的密钥操作；
c） 证书授权中心（CA）：位于上述两个子系统之间，完成证书签发、吊销等居间操作。
三个子系统的关系如图 2 所示。

图2 审核系统的组成结构

三个子系统的角色划分和对应权限如表 1 所示。

表 1 三个子系统的角色划分和对应权限

系统	角色	权限
RA	RA 业务管理员	证书申请记录查看，用户管理，RA 日志查看
	形审人员	形式审查(新证书申请、证书主动吊销)，证书被动吊销申请提交
	实审人员	真实性审查(新证书申请、证书主动吊销)，证书被动吊销申请评审
	RA 审计员	RA 日志审计
CA	CA 超级管理员	管理 CA 业务管理员，CA 日志查看
	CA 业务管理员	管理 CA 业务操作员
	CA 业务操作员	证书模板管理、CRL 管理、证书查看、RA 系统授权
	CA 审计管理员	管理 CA 审计员

	CA 审计员	CA 日志审计
KMC	KMC 超级管理员	管理 KMC 业务管理员，KMC 日志查看
	KMC 业务管理员	管理 KMC 业务操作员
	KMC 业务操作员	密钥管理(密钥添加、密钥查询、密钥撤销等)，添加 CA
	KMC 审计管理员	管理 KMC 审计员
	KMC 审计员	KMC 日志审计

三个子系统的详细功能按照附录B的要求执行。

6.3 文档配备

证书认证机构应配备表2所示的文档以确保正常运行。

表 2 证书认证机构应配备的文档

文档类型	文档内容
技术实现类	a） CA 系统设计 b） CA 系统安全 c） CA 系统安装与配置手册 d） CA 系统安全目标 e） CA 系统用户手册
物理建设类	a） 物理场地安全手册 b） 物理场地安全管理规定
人事管理类	a） 可信人员策略 b） 可信人员职位划分原则与鉴别
运行管理类	a） 账号管理 b） CA 管理规范 c） 认证业务声明 d） 操作手册 e） 安全应急预案 f） 客户服务规范
审计与评估类	a） CA 安全与审计规范

	b） 安全审核与评估规范

为实现运营目的，证书认证机构还应配备表3中的文档。

表 3 证书认证机构运营文档配备

文档类型	文档内容
企业管理类	a） 组织管理 b） 财务管理 c） 人事管理 d） 资产与设备管理
安全策略类	a） 人员安全策略 b） 物理环境安全策略 c） 信息系统安全策略 d） 通信系统安全策略 e） 密钥管理策略 f） 审计策略
运营管理类	a） 证书策略（CP） b） 电子认证业务规则（CPS） c） 认证服务流程与规范 d） 客户服务流程与规范 e） 用户协议 f） 依赖方协议 g） 隐私保护协议 h） 应急响应计划 i） 灾难恢复计划 j） 业务连续性计划
客户类	a） 客户合同 b） 客户资料 c） 审批材料

7 使用数字身份证书所需具备的条件、方法

7.1 证书载体

数字证书应存储于具有数字签名/验证、数据加/解密等功能的智能密码钥匙等载体，用于证书存储及相关的密码作业。智能密码钥匙的接口遵循GM/T 0016中的应用接口规范要求。

7.2 密码设备

密码设备应具备如下基本功能：

（1）随机数生成；

（2）非对称密钥的产生；

（3）对称密钥的产生；

（4）非对称密钥密码算法的加解密运算；

（5）对称密码要密码算法的加解密运算；

（6）数据摘要运算；

（7）密钥的存储；

（8）密钥的安全备份和安全导入导出；

（9）多密码设备并行工作时，密钥的安全同步。

密码设备在安全方面应满足GB/T 25056中规定的接口安全、协议安全、密钥安全和物理安全等多项要求。

密码设备的接口应遵循GM/T 0018，GM/T 0019和GM/T 0020 中的接口规范要求。

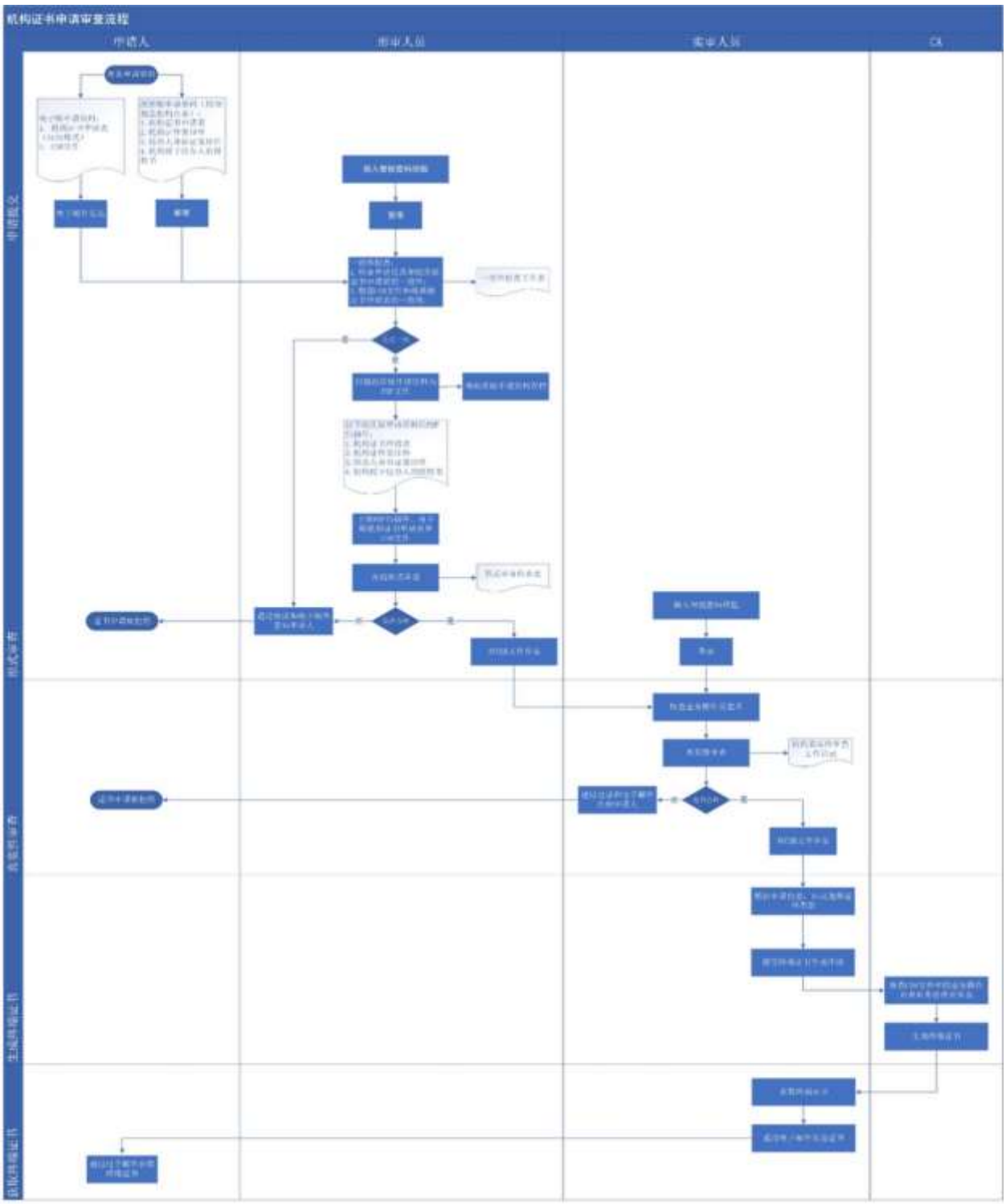
8 与其他计量数字化安全技术之间的接口关系

数字证书文件应至少支持pem和pfx两种类型的格式，可用于数据加/解密和签名/验签等多种应用场景。支持的加密算法包括SM2和RSA算法。支持的密码杂凑算法包括SM3和SHA256算法。

时间戳信息可与证书认证机构的签名信息一并存储于数字证书文件的签名域中。

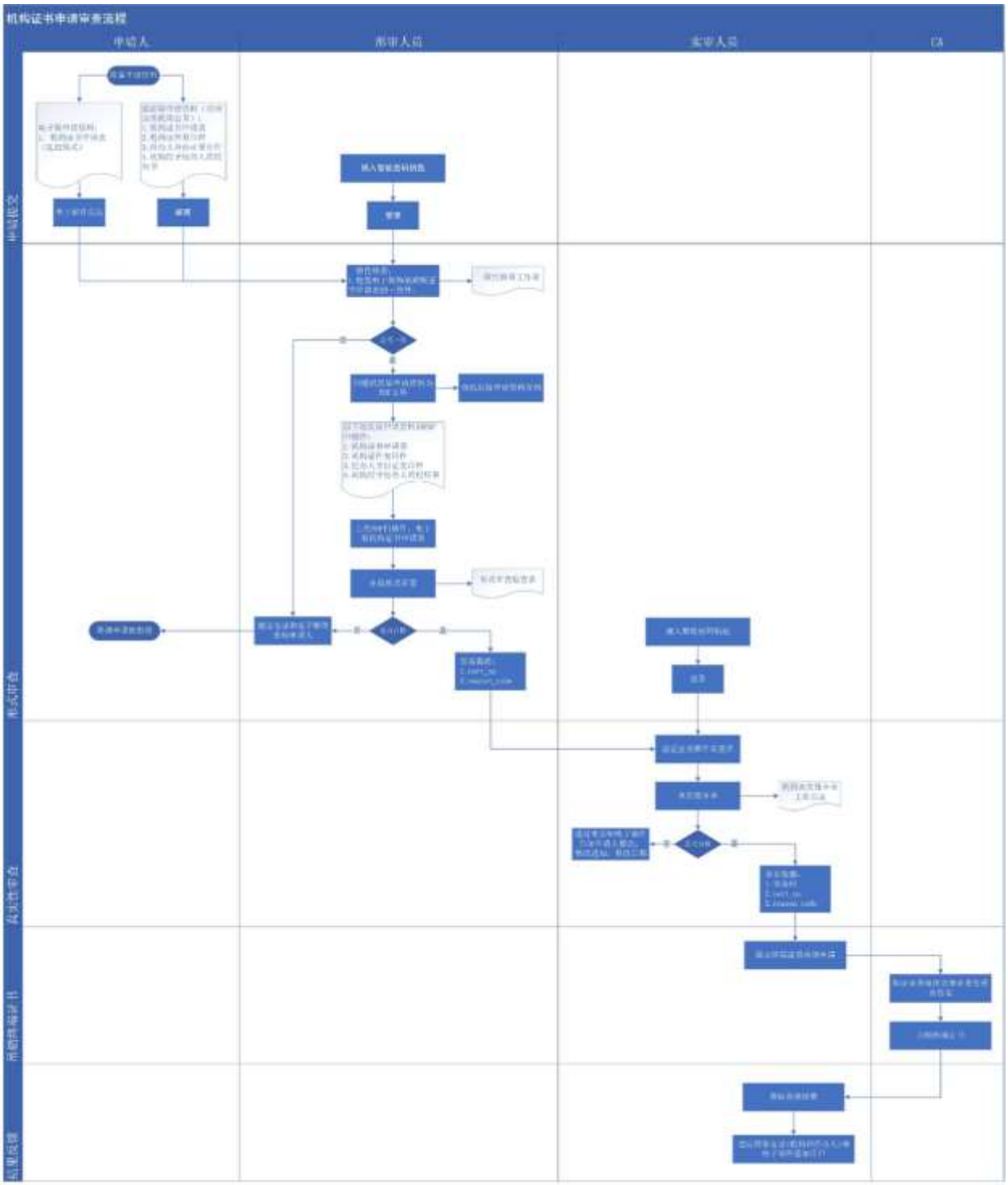
附 录 A
（资料性）
详细业务流程

A.1 新证书申请业务流程（以机构证书为例）见图A.1。



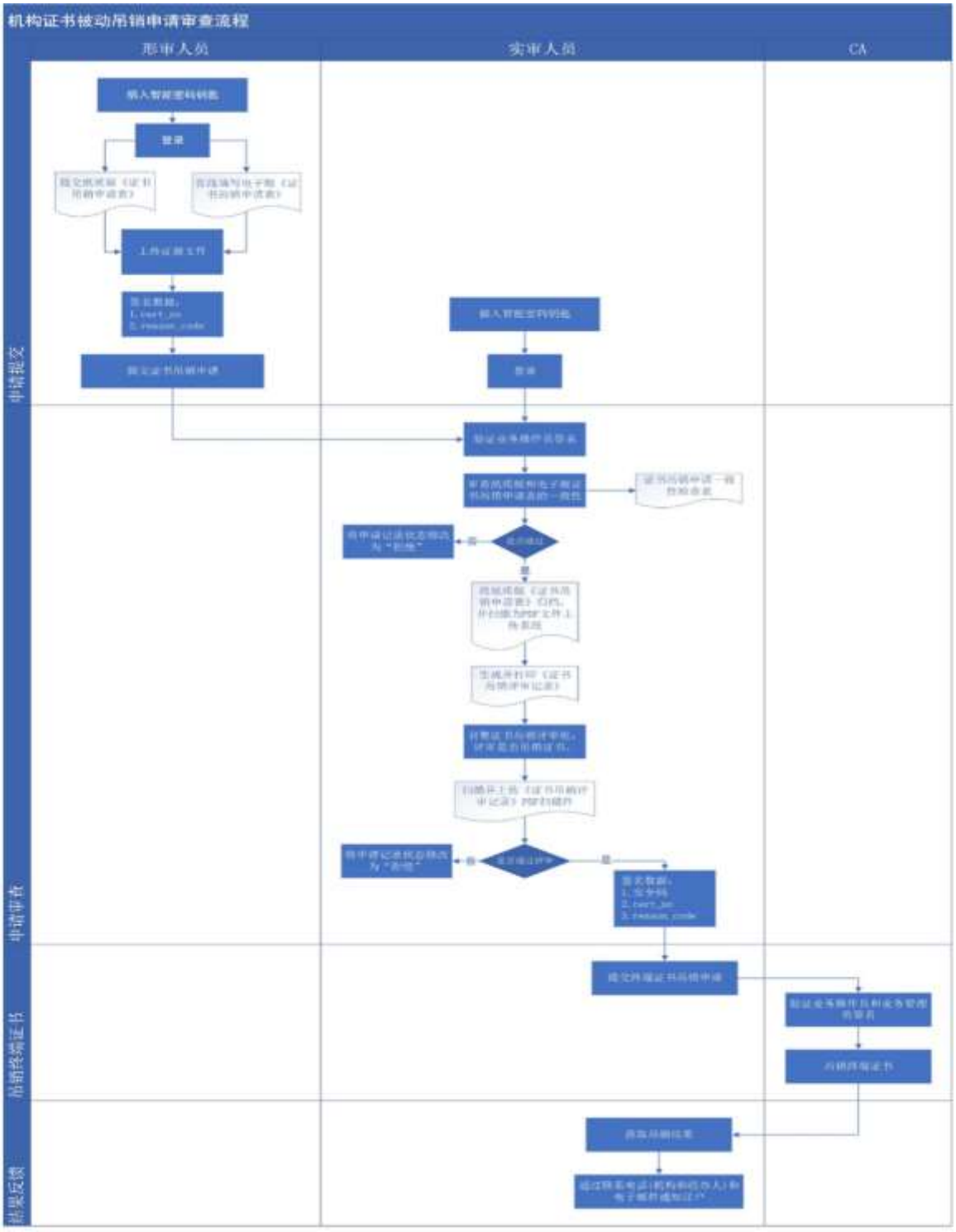
图A.1 新证书申请业务流程（以机构证书为例）

A.2 证书主动吊销流程（以机构证书为例）见图A.2。



图A.2 证书主动吊销流程（以机构证书为例）

A.3 证书被动吊销流程（以机构证书为例）见图A.3。



图A.3 证书被动吊销流程（以机构证书为例）

附 录 B

（规范性）

审核系统功能

B.1 RA系统功能见表B.1。

表B.1 RA系统功能

序号	测试内容	测试方法	预期结果
1	初始化注册系统	进行注册系统初始化操作	正确进行注册系统初始化
2		授权注册系统业务管理员	正确产生业务管理员
3		授权注册系统审计员	正确产生审计员
4	登录	使用已授权业务管理员证书和正确PIN码登录	登录成功并进入登录界面
5		使用未授权业务管理员证书或错误PIN码登录	拒绝登录
6		拔掉登陆者的证书介质	拒绝操作
7	业务操作员管理	在业务操作员管理界面进行增加业务操作员操作	业务操作员被增加
8		在业务操作员管理界面进行删除业务操作员操作	业务操作员被删除
9		在业务操作员管理接麦按进行对业务操作员授权操作	正确对业务操作员授权
10	申请信息录入	在申请信息录入界面进行申请信息录入操作	申请信息被正确录入
11		支持批量证书申请信息的录入操作	批量证书申请信息被正确录入
12	申请信息审核	在申请信息审核界面进行申请信息审核通过操作	审核通过
13		在申请信息审核界面进行申请信息拒绝操作	审核未通过
14	证书下载	提供可以进行证书下载的操作	证书被正确下载
15	证书模板更新	提供将CA给RA授权的证书模板进行更新的操作	授权模板被正确更新
16	日志	在日志管理界面执行对事件、人员、操作类型等信息的查询操作	可以显示相应页面
17	审计	在审计界面对事件发生的事件、事件的操作者、操作类型及操作结果等信息进行审计操作	可以显示相应页面
18		对记录的签名进行验证	可以进行验证
19		审计过的记录有明显标记	显示明显标记

B.2 CA系统功能见表B.2。

表B.2 CA系统功能

序号	测试内容	测试方法	预期结果
1	初始化签发系统	进行签发系统初始化操作	正确进行签发系统初始化
2		产生超级管理员	正确产生超级管理员
3		产生审计管理员	正确产生审计管理员
4	登录	使用已授权管理员证书何正确PIN码登录	登录成功并进入登录界面
5		使用未授权管理员证书或错误PIN码登录	拒绝登录
6		拔掉登陆者的证书介质	拒绝操作
7	多层结构	支持根证书和下级CA证书导入到证书存储区操作	根证书和下级CA证书被成功导入
8		正确识别出根证书和下级CA证书，建立正确的认证路径	建立正确的认证路径
9	业务管理员管理	增加业务操作员操作	业务操作员被增加
10		删除业务操作员操作	业务操作员被删除
11		对业务操作员授予相应的权限	正确对业务操作员授权
12	证书签发	使用CA签名密钥签发各类证书	证书被正确签发
13		提供证书查询和下载服务	正确查询和下载证书
14	CRL签发	根据CRL签发策略正确签发CRL文件	正确签发CRL
15		提供CRL查询和下载服务	正确查询和下载CRL
16	CA证书更新	支持CA证书更新功能，通过新CA证书与旧CA证书的认证链，实现新旧证书更替	新CA证书生成成功,并生成新旧证书认证链
17	证书更新	执行证书更新操作,通过CRL和证书状态查询查看证书状态	证书被正确更新
18	证书撤销	执行证书撤销操作,通过CRL和证书状态查询查看证书状态	证书被正确撤销
19	证书状态查询	通过OCSP服务器或者SOCSP服务器提供实时证书状态查询服务	查询到正确的证书状态
20	RA管理	签发RA服务器证书，对RA管理员进行授权	RA服务器证书被正确签发，RA管理员被正确授权
21	证书模板管理	在证书模板管理界面进行增加证书模板操作	证书模板被增加
22		在证书模板管理界面进行删除证书模板操作	证书模板被删除
23		在证书模板管理界面进行修改证书模板操作	证书模板被正确修改
24	日志	在日志管理界面执行对时间、人员、操	可以显示相应页面

		作类型等信息的查询操作	
25	审计	在审计界面对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计操作	可以显示相应页面
26		对记录的签名进行验证	可以进行验证
27		审计过的记录有明显标记	显示明显标记

B.3 密钥管理系统功能见表B.3。

表B.3 密钥管理系统功能

序号	测试内容	测试方法	预期结果
1	初始化密钥管理系统	进行密钥管理系统初始化操作	正确进行密钥管理系统初始化
2		产生超级管理员	正确产生超级管理员
3		产生审计管理员	正确产生审计管理员
4	登录	使用已授权业务管理员证书和正确PIN码登录	登录成功并进入登录界面
5		使用未授权业务管理员证书或错误PIN码登录	拒绝登录
6		拔掉登录者证书介质	拒绝操作
7	支持多CA	2个以上CA机构从密钥管理系统申请密钥	每个CA均可正确申请加密密钥
8	业务管理员管理	增加业务操作员操作	业务操作员被增加
9		删除业务操作员操作	业务操作员被删除
10		对业务操作员授权操作	正确对业务操作员授权
11	密钥生成	定时产生备用密钥：执行制定数量的密钥预生成操作，查看备用库密钥数量	正确预产生密钥,密钥数量相应增加
12		即时产生备用密钥：执行指定数量的密钥即时预产生密钥操作，查看备用库密钥数量	正确预产生密钥,密钥数量相应增加
13	密钥恢复	在密钥恢复页面由经过授权的司法取证人员和有密钥恢复权限的操作员进行密钥恢复	成功进行密钥恢复
14	密钥撤销	CA提供密钥撤销服务后，查看在用库状态	在用库状态随之改变
15	密钥统计	在用密钥统计：执行在用密钥统计	显示统计结果,获得当前在用密钥数量
16		备用密钥统计：执行备用密钥统计，获得当前备用密钥数量	显示统计结果,获得当前备用密钥数量
17	日志	分别按事件、人员、操作类型等对日志进行分类或综合查询取得查询结果	可以显示相应页面
18	审计	任意组合设置条件进行查询：如果存在符合条件的业务日志,则返回日志列表;如果不存在符合条件的业务日志，则返回空结果	可以显示相应页面
19		对记录的签名进行验证	可以进行验证
20		对审计过的记录设置标记	可以设置标记