智慧 CA CPS

智慧 CA 认证业务声明

版本 1.0

生效日期：2018 年 11 月

智慧 CA CPS

Certification Practice Statement

Version 1.0

目录

1 概括性描述.....1

1.1 概述.....1

1.2 文档名称与标识.....2

1.3 电子认证活动参与者.....2

1.3.1 电子认证服务机构.....3

1.3.2 注册机构.....3

1.3.3 注册分支机构（Registration Authority Branch）.....3

1.3.4 受理点（Business Terminal）.....4

1.3.5 订户（Certificates Applicant）.....4

1.3.6 依赖方（Relying Party）.....4

1.3.7 其他参与者（Other Participants）.....4

1.4 证书应用.....4

1.4.1 适合的证书应用.....4

1.4.2 限制的证书应用.....5

1.5 策略管理.....6

1.5.1 策略文档管理机构.....6

1.5.2 联系人.....6

1.5.3 决定 CPS 符合策略的机构.....6

1.5.4 CPS批准程序.....7

1.5.5 CPS修订.....7

1.6 定义和缩写.....7

2 信息发布与信息管理.....10

2.1 智慧 CA 信息库.....10

2.2 认证信息的发布.....10

2.3 发布的时间或频率.....10

2.4 信息库访问控制.....10

2.4.1 信息的发布与处理.....10
2.4.2 信息访问控制和安全审计.....11
3 身份识别与鉴别.....12
3.1 命名.....12
3.1.1 名称类型.....12
3.1.2 对名称意义化的要求.....12
3.1.3 订户的匿名或假名.....13
3.1.4 理解不同名称形式的规则.....13
3.1.5 名称的唯一性.....13
3.1.6 商标的识别、鉴别和角色.....13
3.2 初始身份确认.....13
3.2.1 证明拥有私钥的方法.....13
3.2.2 组织机构身份的鉴别.....13
3.2.3 个人身份的鉴别.....15
3.2.4 没有验证的订户信息.....15
3.2.5 授权确认.....15
3.2.6 互操作准则.....15
3.3 密钥更新请求的标识与鉴别.....16
3.3.1 常规密钥更新的标识与鉴别.....16
3.3.2 注销后密钥更新的标识与鉴别.....16
3.4 注销请求的标识与鉴别.....16
4 证书生命周期操作要求.....18
4.1 证书申请.....18
4.1.1 证书申请实体.....18
4.1.2 申请过程与责任.....18
4.2 证书申请处理.....19
4.2.1 执行识别与鉴别功能.....19
4.2.2 证书申请批准和拒绝.....19
4.2.3 处理证书申请的时间.....19

4.3 证书签发.....20
4.3.1 证书签发中注册机构和电子认证服务机构的行为.....20
4.3.2 用户证书签发的通知.....20
4.4 证书接受.....20
4.4.1 构成接受证书的行为.....20
4.4.2 电子认证服务机构对证书的发布.....20
4.4.3 电子认证服务机构对其他实体的通告.....21
4.5 密钥对和证书的使用.....21
4.5.1 订户私钥和证书的使用.....21
4.5.2 依赖方公钥和证书的使用.....22
4.6 证书更新.....22
4.6.1 证书更新的情形.....22
4.6.2 请求证书更新的实体.....23
4.6.3 证书更新请求的处理.....23
4.6.4 颁发新证书时对订户的通告.....23
4.6.5 构成接受更新证书的行为.....23
4.6.6 电子认证服务机构对更新证书的发布.....23
4.6.7 电子认证服务机构对其他实体的通告.....23
4.7 证书密钥更换.....24
4.7.1 证书密钥更换的情形.....24
4.7.2 请求证书密钥更换的实体.....24
4.7.3 证书密钥更换请求的处理.....24
4.7.4 订户新证书签发的通知.....24
4.7.5 构成接受密钥更换证书的行为.....24
4.7.6 电子认证服务机构对密钥更换证书的发布.....24
4.7.7 电子认证服务机构对其他实体的通告.....24
4.8 证书变更.....25
4.8.1 证书变更的情形.....25
4.8.2 请求证书变更的实体.....25

4.8.3 证书变更请求的处理.....25
4.8.4 颁发新证书时对订户的通告.....25
4.8.5 构成接受变更证书的行为.....25
4.8.6 电子认证服务机构对变更证书的发布.....25
4.8.7 电子认证服务机构对其他实体的通告.....25
4.9 证书注销和挂起.....25
4.9.1 证书注销的情形.....25
4.9.2 请求证书注销的实体.....26
4.9.3 注销请求的流程.....26
4.9.4 注销请求宽限期.....26
4.9.5 电子认证服务机构处理注销请求的时限.....27
4.9.6 依赖方检查证书注销的要求.....27
4.9.7 CRL发布频率.....27
4.9.8 CRL发布的最大滞后时间.....27
4.9.9 在线状态查询的可用性.....27
4.9.10 注销状态查询要求.....27
4.9.11 注销信息的其他发布形式.....27
4.9.12 密钥损害的特别要求.....27
4.9.13 证书挂起的情形.....28
4.9.14 请求证书挂起的实体.....28
4.9.15 挂起请求的流程.....28
4.9.16 挂起的期限限制.....28
4.9.17 证书解挂.....28
4.10 证书状态服务.....29
4.10.1 操作特征.....29
4.10.2 服务可用性.....29
4.10.3 可选特征.....29
4.11 订购结束.....29
4.12 密钥生成、备份与恢复.....30

4.12.1 密钥备份与恢复的策略与行为.....30
4.12.2 会话密钥的封装与恢复的策略与行为.....30
5 认证机构设施、管理和操作控制.....31
5.1 物理控制.....31
5.1.1 场地位置与建筑.....31
5.1.2 物理访问.....32
5.1.3 电力与空调.....32
5.1.4 水患防治.....33
5.1.5 火灾防护.....33
5.1.6 介质存储.....33
5.1.7 废物处理.....33
5.1.8 异地备份.....33
5.2 程序控制.....33
5.2.1 可信角色.....33
5.2.2 每项任务需要的人数.....34
5.2.3 每个角色的识别与鉴别.....34
5.2.4 需要职责分割的角色.....34
5.3 人员控制.....34
5.3.1 资格、经历和无过失要求.....34
5.3.2 背景审查程序.....35
5.3.3 培训要求.....35
5.3.4 再培训周期和要求.....36
5.3.5 工作岗位轮换周期和顺序.....36
5.3.6 未授权行为的处罚.....36
5.3.7 独立合约人的要求.....36
5.3.8 提供给员工的文档.....36
5.4 审计日志程序.....37
5.4.1 记录事件的类型.....37
5.4.2 处理日志的周期.....37

5.4.3 审计日志的保存期限.....37
5.4.4 审计日志的保护.....37
5.4.5 审计日志备份程序.....37
5.4.6 审计收集系统.....38
5.4.7 对导致事件实体的通告.....38
5.4.8 脆弱性评估.....38
5.5 记录归档.....38
5.5.1 归档记录的类型.....38
5.5.2 归档记录的保存期限.....39
5.5.3 归档文件的保护.....39
5.5.4 归档文件的备份程序.....39
5.5.5 记录时间戳要求.....39
5.5.6 归档收集系统.....39
5.5.7 获得和检验归档信息的程序.....39
5.6 电子认证服务机构密钥更替.....39
5.7 损害与灾难恢复.....40
5.7.1 事故和损害处理程序.....40
5.7.2 计算资源、软件或数据的损坏.....40
5.7.3 实体私钥损害处理程序.....40
5.7.4 灾难后的业务连续性能力.....41
5.8 电子认证服务机构或注册机构的终止.....41
6 认证系统技术安全控制.....42
6.1 密钥对的生成和安装.....42
6.1.1 密钥对的生成.....42
6.1.2 加密私钥传送给订户.....42
6.1.3 公钥传送给证书签发机构.....42
6.1.4 密钥的长度.....43
6.1.5 公钥参数的生成和质量检查.....43
6.1.6 密钥使用用途.....43

6.2 私钥保护和密码模块工程控制.....43
6.2.1 密码模块的标准和控制.....43
6.2.2 私钥多人控制（5选3）.....43
6.2.3 私钥托管.....44
6.2.4 私钥备份.....44
6.2.5 私钥归档.....44
6.2.6 私钥导入、导出密码模块.....44
6.2.7 私钥在密码模块的存储.....44
6.2.8 激活私钥的方法.....44
6.2.9 解除私钥激活状态的方法.....44
6.2.10 销毁私钥的方法.....45
6.2.11 密码模块的评估.....45
6.3 密钥对管理的其他方面.....45
6.3.1 公钥归档.....45
6.3.2 证书操作期和密钥对使用期限.....45
6.4 激活数据.....45
6.4.1 激活数据的产生和安装.....45
6.4.2 激活数据的保护.....45
6.4.3 激活数据的其他方面.....46
6.5 计算机安全控制.....46
6.5.1 特别的计算机安全技术要求.....46
6.5.2 计算机安全评估.....46
6.6 生命周期技术控制.....46
6.6.1 系统开发控制.....46
6.6.2 安全管理控制.....46
6.6.3 生命周期的安全控制.....47
6.7 网络的安全控制.....47
6.8 时间戳.....47
7 证书、证书注销列表和在线证书状态协议.....48

7.1 证书.....48
7.1.1 版本号.....48
7.1.2 证书标准项及扩展项.....48
7.1.3 算法对象标识符.....49
7.1.4 名称形式.....49
7.1.5 名称限制.....49
7.1.6 证书策略对象标识符.....49
7.1.7 策略限制扩展项的用法.....49
7.1.8 策略限定符的语法和语义.....49
7.1.9 关键证书策略扩展项的处理规则.....49
7.2 证书注销列表.....50
7.2.1 版本号.....50
7.2.2 CRL和CRL条目扩展项.....50
7.3 在线证书状态协议.....50
7.3.1 版本号.....50
7.3.2 OCSP 扩展项.....50
8 认证机构审计和其他评估.....51
8.1 评估的频率或情形.....51
8.2 评估者的资质.....51
8.3 评估者与被评估者之间的关系.....51
8.4 评估内容.....51
8.5 对问题与不足采取的措施.....52
8.6 评估结果的传达与发布.....52
9 法律责任和其他业务条款.....53
9.1 费用.....53
9.1.1 证书签发和更新费用.....53
9.1.2 证书查询费用.....53
9.1.3 证书注销或状态信息的查询费用.....53
9.1.4 其他服务费用.....53

9.1.5 退款策略.....53
9.2 财务责任.....53
9.2.1 保险范围.....53
9.2.2 其他资产.....54
9.2.3 对最终实体的保险或担保.....54
9.3 业务信息保密.....54
9.3.1 保密信息范围.....54
9.3.2 不属于保密的信息.....55
9.3.3 保护保密信息的责任.....55
9.4 个人隐私保密.....55
9.4.1 隐私保密方案.....55
9.4.2 作为隐私处理的信息.....56
9.4.3 不被视为隐私的信息.....56
9.4.4 保护隐私的责任.....56
9.4.5 使用隐私信息的告知与同意.....56
9.4.6 依法律或行政程序的信息披露.....56
9.4.7 其他信息披露情形.....56
9.5 知识产权.....56
9.6 陈述与担保.....57
9.6.1 电子认证服务机构的陈述与担保.....57
9.6.2 注册机构的陈述与担保.....58
9.6.3 订户的陈述与担保.....58
9.6.4 依赖方的陈述与担保.....58
9.6.5 其他参与者的陈述与担保.....58
9.7 担保免责.....58
9.8 有限责任.....59
9.9 赔偿.....59
9.10 有效期限与终止.....61
9.10.1 有效期限.....61

9.10.2 终止.....61
9.10.3 效力的终止与保留.....61
9.11 对参与者的个别通告与沟通.....61
9.12 修订.....61
9.12.1 修订程序.....61
9.12.2 通知机制和期限.....61
9.12.3 必须修改业务规则的情形.....62
9.13 争议处理.....62
9.14 管辖法律.....62
9.15 与适用法律的符合性.....62
9.16 一般条款.....62
9.16.1 完整协议.....62
9.16.2 转让.....62
9.16.3 分割性.....62
9.16.4 强制执行力.....62
9.16.5 不可抗力.....63
9.17 其他条款.....63

1 概括性描述

1.1 概述

电子认证业务规则（ CPS，Certification Practice Statement ）是关于认证机构（ CA, Certification Authority ）在证书服务生命周期中的业务实践（如签发、管理、注销、更新证书或密钥）所必须遵循的规范并详细的描述和声明，同时提供涉及业务、技术和法律方面的细节。智慧 CA 根据 ISO 组织 IETF RFC 3647 规范编写了本单位 CPS，作为智慧 CA 证书相关业务和系统运行的规范。

本文档的编写遵从 IETF RFC 3647 （ Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,公钥基础设施证书策略和证书运行框架 ）、十届全国人大常委会表决通过的并于 2005 年 4 月 1 日正式实施的 《中华人民共和国电子签名法》 以及中华人民共和国工业与信息化部修订并通过的 《电子认证服务管理办法》 。

智慧 CA 是指江苏智慧数字认证有限公司，是经国家工业与信息化部、国家密码管理局批准成立的，全国性、公正可信的第三方认证机构。公司为电子政务外网和电子商务网络提供数字证书安全认证服务。

智慧 CA 自成立以来，严格按照国家规定的各项要求运作。 2018 年 10 月，江苏智慧数字证书认证中心建设实施方案通过了国家密码管理委员会办公室组织的专家论证。2018 年 10 月，智慧 CA 通过了国家密码管理委员会办公室组织的安全性审查。

智慧 CA 为互联网的交易多方建立信任关系以保证交易主体身份的真实性，为信息的保密性、完整性以及交易的不可抵赖性提供全面服务。作为被信任的第三方，智慧 CA 或智慧 CA 授权的发证机构为网上交易和网上安全操作的参与人颁发数字证书。智慧 CA 数字证书（以下简称证书）遵循 X.509V3 规范。智慧 CA 承诺，在证书有效的情况下，保证证书能唯一地与身份明确的实体相关联，公钥能与身份确定的实体唯一相对应。

为配合证书业务的正常开展，智慧 CA 编写了智慧 CA 认证业务声明。认证业

务声明的建立及其正确的贯彻和实施将为江苏省电子政务公共服务、电子交易和其他网上安全服务提供强有力的支持。

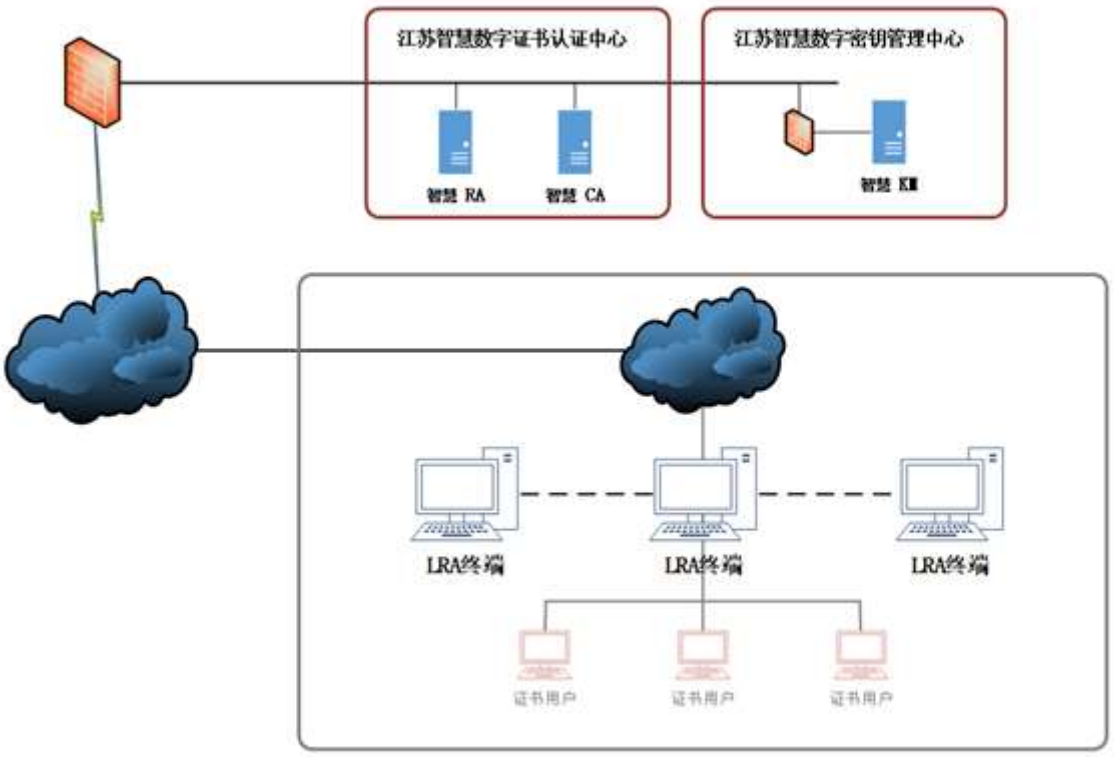
1.2 文档名称与标识

本文为智慧 CA 电子认证业务规则（CPS），并在智慧 CA 网站发布。智慧 CA 网址：

http://www.smartcert.cn 。

1.3 电子认证活动参与者

智慧 CA 认证系统采用国际领先的 PKI 技术，总体为两层 CA 结构，第一层为根CA；第二层为运营 CA，根据电子认证业务规则（CPS）发放证书。以下为智慧 CA 认证系统结构图示：



1.3.1电子认证服务机构

智慧 CA 和智慧 CA 下层 CA 统称为电子认证服务机构。

智慧 CA 是所有智慧 CA 下层机构和实体的根。在十分严密的保密和安全机制控制下，智慧 CA 根据根证书有效的安全策略自己生成密钥对，自己签发根证书。智慧 CA 根据授权和协议，签发下一级证书。智慧 CA 将决定在什么时间、什么地点、由什么人监督、怎么实施智慧 CA 根密钥对的更新和切换。智慧 CA 的动作单位是江苏智慧数字认证有限公司。智慧 CA 已经建立了完善的安全机制，以保证私有密钥的安全性。智慧 CA 还将建立异地备份中心。

智慧 CA 所签发的证书与每一个证书申领实体的公钥绑定。智慧 CA 承诺，在有效期内的证书，将采用证书目录服务器和证书黑名单服务器 CRL SERVER，公布江苏智慧数字认证有限公司证书可以公开的信息和状态。

1.3.2注册机构

注册机构作为电子认证服务机构授权的下属机构，负责证书订户信息的审核、整理汇总、统计分析，与上级CA进行数据交换，管理和服务下层注册分支机构和下层受理点。每个注册机构可以按照行业或行政地域分成多个注册分支机构，或直接连接受理点，可以直接对最终订户提供服务。注册机构有责任妥善保存订户的数据，不允许将订户的数据透露给与证书申请无关的任何机构或个人，不允许用作商业利益方面的用途。

注册机构可以由智慧 CA 自建或授权的第三方机构建立。当注册机构由第三方机构建立时，智慧 CA 必须与其签订协议，明确双方的权利和义务。

1.3.3注册分支机构（Registration Authority Branch）

注册分支机构与注册机构功能类似。当注册机构服务的群体超过一定程度时，在注册机构下面设注册分支机构。注册分支机构的上级是注册机构，下级是受理点。注册分支机构由智慧 CA 授权建立或撤消。注册分支机构是可选项，即根据客户数量决定是否设立。

1.3.4受理点（Business Terminal）

经过智慧 CA 审查，智慧 CA 授权特定机构或实体负责办理和审批数字证书申请。数字证书申请手续、过程和要求，必须与智慧 CA 正在实施的证书策略、电子认证业务规则以及受理点授权协议书相一致。受理点负责向智慧 CA 授权的注册机构或智慧 CA 授权的注册分支机构提供证书申请实体的信息，包括申请实体的名称、可以表明身份的证件号码和联系方法（通信地址、电子邮件、电话等）。受理点根据这些信息为申请实体制作证书或根据申请实体的要求，提供申请实体自行申请的技术支持。

1.3.5订户（Certificates Applicant）

在电子签名应用中，订户即是电子签名人、证书持有人，是智慧 CA 颁发证书的所有最终用户，可以是个人、机构等。

1.3.6依赖方（Relying Party）

指需要验证证书和签名的实体。依赖方可以是、也可以不是订户。

1.3.7其他参与者（Other Participants）

指为智慧 CA 的电子认证活动提供相关服务的其他实体，如第三方权威机构、目录服务提供者等与 PKI 服务相关的参与者。

1.4 证书应用

1.4.1适合的证书应用

证书应用可确保互联网上信息传递双方身份的真实性、信息的保密性和完整性、以及网上交易的不可否认性。

智慧 CA 数字证书可以广泛应用于电子政务社会管理、电子交易、电子办公、电子公证、公共服务等领域，为建设互联网络的信任环境开展了基础性服务。根据证书的功能以及使用证书的实际应用，目前智慧 CA 签发的主要证书类型包括：

个人证书：此类证书通常用于数字签名、加密解密、安全电子邮件以及网上身份认证等，在不违背相关法律法规、本 CPS 以及订户协议的情况下，此类证书也可以用于其他用途；

机构证书：机构包括企事业单位、政府机关、社会团体等。此类证书通常用于数字签名、加密解密以及网上身份认证等，在不违背相关法律法规、本 CPS 以及订户协议的情况下，此类证书也可以用于其他用途；

1.4.2限制的证书应用

证书禁止在任何违反国家法律、法规或破环国家安全的情形下使用。否则，由此造成的法律后果由订户自己承担。

智慧 CA 签发的数字证书禁止的应用范围包括：

1）国家法律法规所规定的不允许使用的范围；

2）破坏国家安全、环境安全和人身安全的危险环境；

3）智慧 CA 与订户约定的证书禁止应用的范围。

1.5 策略管理

智慧 CA 安全策略委员会是智慧 CA 电子认证服务所有策略的最高管理机构，负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

1.5.1策略文档管理机构

策略文档管理机构为智慧 CA 安全策略委员会，作为策略管理机构负责制订、发布、更新本 CPS。智慧 CA 安全策略委员会由来自于公司管理层、行政中心、营销中心、技术中心、运营服务中心等拥有决策权的合适代表组成。

智慧 CA 安全策略委员会的所有成员在就证书策略进行管理和批准时，均享有一票决定权，如果选票相同，委员会主任可拥有双票决定权。

1.5.2联系人

智慧 CA 指定专门的机构和人员负责 CPS 的相关事宜，任何有关 CPS 的问题、建议、疑问等，都可以与此联系人进行联系。

联系人：张循

电话：025-52819801

传真：025-52819800

电子邮件：ca@smartcert.cn

地址：江苏省南京市雨花台区软件大道170-1号 天溯科技园 2幢 6层

邮政编码：210013

1.5.3决定 CPS 符合策略的机构

智慧 CA 成立了安全策略委员会，是公司CPS策略制定的最高权威机构，审定批准 CPS，决定 CPS 是否符合策略。

1.5.4CPS批准程序

按照信息产业部公布的 《电子认证业务规则规范》 的要求，智慧 CA 电子认证业务规则由智慧 CA 安全策略委员会制定、修改、审批。智慧 CA 根据 《电子认证服务管理办法》 中规定，在本机构网站予以公布，并在公布之日前30日内向工业和信息化部备案。

1.5.5CPS修订

智慧 CA 根据国家的政策法规、技术要求、标准的变化及业务发展情况及时修订本CPS，CPS 编写小组根据相关的情况拟定 CPS 修订建议，提交智慧 CA 安全策略委员会审核，经该委员会批准后，正式在智慧 CA 官方网站上发布。

修订后的 CPS，从对外发布之日起30日之内向工信部备案。

1.6 定义和缩写

PKI 公钥基础设施（Public Key Infrastructure）

是利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，使得互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务得以实现。

CA 认证中心（Certification Authority）

受用户信任的，负责创建和签发数字证书的权威机构。CA 是认证中心的英文 Certification Authority 的缩写。 CA 中心，又称为数字证书认证中心。CA 中心作为电子交易中受信任的第三方，负责为电子商务环境中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书。

RA 注册机构（Registration authority）

负责用户证书的申请、审批和证书管理部分工作，面向证书用户。可以分为本地 RA 和自建 RA 两种。

本地 RA

指 RA 系统设立在智慧 CA 的 RA 服务器中。

自建 RA

指 RA 系统设立在机构或组织中的 RA服务器中，归机构或组织所有，由机构或组织使用，为证书审核严格或证书管理复杂的机构或组织提供证书申请审批、证书信息录入以及证书发放并进行部分管理服务的 RA 系统。

数字证书（Digital Certificate）

数字证书又称为电子证书，是指经 CA 数字签名的包含证书使用者身份公开信息和公开密钥的电子文件。

由于Internet 中电子商务系统技术使某些敏感或有价值的数据有被滥用的风险，为了保证互联网上电子交易及支付的安全性、保密性等，防范交易及支付过程中的欺诈行为，必须在网上建立一种信任机制。这就要求参加电子商务的各方都必须拥有合法的身份，并且在网上能够有效无误的被进行验证。数字证书提供了一种在 Internet 上验证身份的方式，其作用类似于日常生活中的身份证或护照以及驾驶证。在本标准中，术语“数字证书”与“电子证书”可互换使用。

CRL 证书注销列表（ Certificate Revocation List ）

证书注销列表(Certificate Revocation List，简称 CRL)，是一种包含注销的证书列表的签名数据结构。 CRL 是证书注销状态的公布形式，CRL 就像信用卡的黑名单，它通知其他证书用户及依赖方某些数字证书不再有效。

LDAP （Lightweight Directory Access Protocol）

即轻量级目录访问协议，用于查询、下载数字证书以及数字证书废止列表（CRL）。

OCSP 在线证书状态协议（Online Certificate Status Protocol）

在线证书状态协议是用于检查数字证书在某一交易时间是否有效的标准。

CP 证书策略（Certificate Policy）

一套命名的规则集，用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如，一个特定的 CP 可以指明某类证书适用于鉴别从事机构到机构（B-to-B）交易活动的参与方，针对给定价格范围内的产品和服务。

CPS 电子认证业务规则（ Certif icate practice Statement）

电子认证业务规则（Certif icate practice Statement）是关于 CA 的颁发和管理证书的运作规范的描述。包括 CA 整体运行规范和证书的颁发、管理、注销和密钥以及证书更新的操作规范等事务

用户 （ Subscriber）

被颁发给一个证书的证书主体

依赖方 (Relying party)

证书的接收者，他依赖于该证书或该证书所验证的电子签名。在本标准中，术语“证书使用者”与“依赖方”可互换使用。

私钥（Private Key）

在公钥基础设施（PKI）中为一个密码串，由特定算法与公钥一起生成，用于解密信息或进行数字签名。在数字签名中又称为电子签名制作数据，是在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码数据。在本标准中，术语“电子签名”与“数字签名”可互换使用。

公钥 (Public Key)

在公钥基础设施（PKI）中为一个密码串，由特定算法与私钥一起生成，用于加密信息或验证数字签名。在数字签名中又称为电子签名验证数据，是用于验证电子签名的数据，包括代码、口令等。

DN 惟一甄别名 (Dist inguished Name)

在数字证书的主体名称域中，用来惟一标识用户的 X.500 名称。此域需要填写反映用户真实身份的、具有实际意义的、与法律不冲突的内容。

2 信息发布与信息管理

2.1 智慧 CA 信息库

智慧 CA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。智慧 CA 信息库内容包括但不限于以下内容：CPS 现行和历史版本、证书、CRL、订户协议，以及其它由智慧 CA 不定期发布的信息。智慧 CA 将及时发布包括证书、CPS 修订和其它资料等内容，这些内容必须保持与 CPS 及有关法律法规一致。智慧 CA 信息库可以通过网址：http://www.smartcert.cn 查询，或由智慧 CA 随时指定的其它通讯方法获得。

2.2 认证信息的发布

智慧 CA 在官方网站 http://www.smartcert.cn 发布信息库，该网站是智慧 CA 发布所有信息最主要、最及时、最权威的渠道。

智慧 CA 通过目录服务器发布订户的证书和 CRL，订户或依赖方可以通过访问智慧 CA 的目录服务器获取证书的信息和注销证书列表；智慧 CA 也提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。同时，智慧 CA 也将会根据需要采取其他可能的形式进行信息发布。

2.3 发布的时间或频率

智慧 CA 在订户证书签发或者注销时，通过目录服务器或官方网站自动将证书和 CRL 发布，发布周期为不大于24小时，即在24小时内发布最新 CRL；在紧急的情况下，智慧 CA 可以自行决定证书和 CRL 的发布时间。信息库其他内容的发布时间和频率，由智慧 CA 独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

2.4 信息库访问控制

2.4.1信息的发布与处理

对于以网站方式公布的信息，智慧 CA 允许任何公众进行查询和访问。证书和 CRL 除公司网站外，还可通过 LDAP 方式发布，同时提供 OCSP 在线验证方式。但只有智慧 CA 有权对公布的各类信息进行处理。

2.4.2信息访问控制和安全审计

智慧 CA 设置了信息访问控制和安全审计措施，保证了 CPS、证书、CRL 等 电子认证信息库只有经过授权的智慧 CA 工作人员才能登陆、访问和控制。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

智慧 CA 颁发的数字证书，根据证书对应实体的类型不同，其实体名字可以是人员姓名、组织机构名称、部门名、域名等，证书包含订户和颁发机构主题甄别名，对证书申请者的身份和其他属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。

智慧 CA的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用 X.500 标准命名方式，格式如下：

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	智慧 CA
Organizational Unit （OU） =	组织机构	江苏智慧
State or Province （S） =	省	江苏
Locality （L） =	区	雨花台区
Common Name （CN） =	通用名	江苏智慧
Email=	邮件地址	ca@smartcert.cn

智慧 CA的证书包含颁发者的甄别名称，格式如下：

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	智慧 CA
Common Name （CN） =	通用名	江苏智慧

3.1.2 对名称意义化的要求

智慧 CA 签发的个人实体证书、组织机构通用数字证书等包含的命名应具有通常理解的语义，用它可以确定证书主题中的个人、机构的身份。对于具有特殊要求的应用中，智慧 CA 可以按照一定的规则为订户指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体（个人、机构）唯一联系起来。

3.1.3订户的匿名或假名

订户在证书中的名称可以是假名，但不能使用匿名，并在智慧 CA 的数据库中记录订户的相关信息。

3.1.4理解不同名称形式的规则

智慧 CA 签发的数字证书符合 X.509 标准，甄别名格式遵守 X.500 标准，甄别名的命名规则由智慧 CA 定义与解释。

3.1.5名称的唯一性

在智慧 CA 信任域内，不同订户证书的主题甄别名不能相同，必须是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的密钥用法扩展项不同。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

3.1.6商标的识别、鉴别和角色

证书申请者不应使用任何可能侵犯知识产权的名称。智慧 CA 不对证书申请者是否拥有命名的知识产权进行判断和决定，也不负责解决证书中任何关于域名、商标等知识产权的纠纷。智慧 CA 没有权利，也没有义务拒绝或者质疑任何可能导致产生知识产权纠纷的证书申请。

3.2 初始身份确认

3.2.1证明拥有私钥的方法

智慧 CA 证明拥有私钥的方法是根据证书申请信息进行验证。首先利用数据摘要算法进行计算，再用申请信息中的公钥对申请信息中的签名解密，然后进行比较，如果相等则证明数字证书的申请者拥有与签名验证公钥对应的签名私钥。

3.2.2组织机构身份的鉴别

组织机构申请者填写书面申请表（一式二份），经过机构授权代表的签署及机构盖章，表示接受书面申请的有关条款，并承担相应的责任。智慧 CA 授权的发证机构必须对订户进行以下资料的鉴别：

1）申请机构组织机构代码证的复印件；

2）申请机构的营业执照副本及复印件，如果没有营业执照，则提供书面申请表上可选的其他有效证件的副本及复印件。部分有效证件如下：

- 营业执照
- 企业法人营业执照
- 事业单位法人登记证
- 税务登记证
- 社会团体法人登记证
- 政府批文
- 其他有效证件

3）经办人身份证原件与复印件。

在组织机构申请者身份的鉴别流程中，智慧 CA 将按照每种证书的要求进行不同的验证。证书申请表上有申请者本身或被充分授权的证书申请者代表及经办人的签字。智慧 CA 或其注册机构、受理点等电子认证服务机构必须检查申请者所递交的文件，申请者需向智慧 CA 提供机构确实存在的有效证明，包括但不限于工商营业执照等；申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

智慧 CA 和其授权的电子认证服务机构在规定期限内保存组织机构的全部申请材料，这个规定期限由法律、政策、主管部门的要求或者智慧 CA 自行决定。数字证书登记信息发生变更时，证书持有人或证书依赖方应及时向注册机构提交变更申请。因登记信息与真实信息不符而导致的全部法律责任由证书持有人或证书依赖方自行承担。

3.2.3个人身份的鉴别

智慧 CA 的个人证书签发给合法的个人申请者，智慧 CA 需要严格审核个人申请者的身份。至少需要进行如下的一种鉴别：

1）利用权威第三方提供的身份证明或数据库服务；

2）政府机构发放的合法性文件，如：居民身份证、军官证、护照等证明订户的身份。若委托他人进行证书申请的，应同时提供被委托人的身份证明。

个人申请者填写书面申请表（一式二份），签字确认，表示接受证书申请的有关条款，并承担相应的责任。

数字证书登记信息发生变更，证书持有人或证书依赖方应及时向注册机构提交变更申请。因登记信息与真实信息不符而导致的全部法律责任由证书持有人或证书依赖方自行承担。

3.2.4没有验证的订户信息

在初始身份认证中，不作验证的订户信息列表如下：

个人订户信息	机构订户信息
电话/移动电话 地址/邮政编码 传真	机构英文或拼音 地址/邮政编码 电话/移动电话 联系人、传真

3.2.5授权确认

证书申请者申请某一类型的证书时，智慧 CA 和其授权的证书服务机构还需审核申请经办人的身份和资格，包括必需的身份资料和授权证明文件。组织机构或个人在智慧 CA 数字证书申请文件上签字或加盖公章后，则证明其对办理人员的授权确认。

3.2.6互操作准则

对于智慧 CA 外的其他证书服务机构颁发的证书，可以与智慧 CA 进行互操作，但是必须符合智慧 CA 的证书策略的要求，并且与智慧 CA签署了相应的协议。

3.3 密钥更新请求的标识与鉴别

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。智慧 CA 一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，也允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户证书公钥也不改变。对于智慧 CA 的证书认证业务，在证书有效期到期前只能通过密钥更新或证书更新签发有相同签发者、主体名和证书用途的证书。通常，我们在表述证书更新时包含了密钥更新和证书更新。

3.3.1常规密钥更新的标识与鉴别

对于常规密钥更新，订户可以用原有的私钥对更新请求进行签名。智慧 CA 认证系统会对订户的签名和更新请求进行鉴别。

订户也可以选择一般的初始证书申请流程，按照初始身份验证步骤（详细内容请见第3.2节）进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。

智慧 CA 授权的发证机构的审核人员须合理地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行审查，并进行批准或拒绝的操作。

密钥更新会造成使用原密钥对加密的文件或数据无法解密。因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或数据已经解密。否则，由此造成的损失，智慧 CA 将不承担责任。

3.3.2注销后密钥更新的标识与鉴别

智慧 CA 不提供证书被注销后的密钥更新。订户必须重新进行身份鉴别，按照初始身份验证步骤向智慧 CA 申请重新申请证书。

3.4 注销请求的标识与鉴别

在智慧 CA 的证书业务中，证书注销请求可以来自订户，也可以来自智慧 CA 。当智慧 CA 授权的发证机构有充分的理由注销订户时，有权依法注销证书，这种情

况无须进行鉴证。如果订户主动要求注销证书，则需要递交初始身份验证时的申请材料。如果由于条件的限制无法进行现场审核时，智慧 CA 可以通过电话、传真、邮政信函或其他第三方证明等合理方式对申请者的身份予以鉴别验证。如果是司法机关依法提出注销，智慧 CA 将直接以司法机关提供的书面注销请求文件作为鉴别依据，不再进行其他方式的鉴别。

4 证书生命周期操作要求

智慧 CA 授权的发证机构提供完整的数字证书周期，包括申请、验证、签发、发布、更新、注销、归档等过程，提供身份认证、电子签名、数据加密、密钥管理等与数字证书密切相关的配套服务。自 CA 认证系统签发之日算起，智慧 CA 签发的个人类型证书、机构类型证书的默认有效期为 1 年；智慧 CA 保留根据业务需要重新设置订户证书有限期的权利。

4.1 证书申请

4.1.1证书申请实体

证书申请实体包括个人和具有独立法人资格的组织机构（包括行政机关、事业单位、社会团体和人民团体等）。

4.1.2申请过程与责任

1. 证书的注册过程

订户填写相应的证书申请表单。

订户携带相应的证明材料到智慧 CA 的注册机构（RA 或 LRA）进行证书申请，注册机构审核通过后，录入申请资料。其中审核员和信息录入员分别为两个不同的系统操作人员。

注册机构向智慧 CA 提交证书请求，通过应用安全协议发送至智慧 CA 。

智慧 CA 根据注册机构的请求签发证书。

注册机构通过安全的方式（如面对面提交）将证书交付给订户。

2. 责任

订户有责任向智慧 CA 提供真实、完整和准确的证书申请信息和资料。

注册机构承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

4.2 证书申请处理

4.2.1执行识别与鉴别功能

当智慧 CA 及其注册机构接受到订户的证书申请后，应按本 CPS3.2.2、3.2.3、3.2.4 及 3.2.5 的要求，对订户进行身份识别与鉴别。

智慧 CA 在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

4.2.2证书申请批准和拒绝

依据识别与鉴别的信息，智慧 CA 授权的发证机构有权决定接受或拒绝订户的申请。

如果符合下述条件，智慧 CA 授权的发证机构接受订户的证书申请：

1）成功标识和鉴别了订户的身份信息；

2）订户接受订户协议的内容和要求；

3）订户按照规定支付了相应的费用，另有协议规定的情况除外。

如果发生下列情形之一，智慧 CA 授权的发证机构有权拒绝订户的证书申请：

1）该申请未完成标识和鉴别的过程；

2）订户不能提供所需要的补充文件；

3）订户不接受或者反对订户协议的内容和要求；

4）没有或者不能够按照规定支付相应的费用；

5）智慧 CA 授权的发证机构认为批准该申请将会对智慧 CA 带来争议、法律纠纷或者损失。

4.2.3处理证书申请的时间

智慧 CA 授权的发证机构必须在1个工作日内对证书申请者提交的证书信息进行识别，并完成证书申请处理。

4.3 证书签发

4.3.1证书签发中注册机构和电子认证服务机构的行为

在证书的签发过程中 RA 的管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发至正确的 CA 证书签发系统。

CA 的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发订户证书。

智慧 CA 在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

通常智慧 CA 签发的证书在24小时内生效。

4.3.2用户证书签发的通知

智慧 CA 会选择以下一种通知方式告知订户：

1、电子或纸质的受理回执；

2、电子邮件（E-mail）；

3、通过面对面的方式，通知订户（如申请者到受理点领取等方式）；

4、智慧 CA 认为其他安全可行的方式。

4.4 证书接受

4.4.1构成接受证书的行为

在智慧 CA 数字证书签发完成后，智慧 CA 将把数字证书当面或寄送给订户，订户从获得证书起就被视为已同意接受证书。订户接受数字证书后，应妥善保存其证书对应的私钥。

4.4.2电子认证服务机构对证书的发布

订户接受证书后，智慧 CA 在24小时内将该订户证书发布到智慧 CA 的目录服务系统。

智慧 CA 采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接

发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构对其他实体的通告

智慧 CA 不具有向其他实体进行单独通告的义务，但使用证书的各类实体可以通过智慧 CA 查询服务获得所需证书信息。

4.5 密钥对和证书的使用

智慧 CA 要求订户密钥对和证书的使用不能超过其规定使用范围，否则智慧 CA 不承担由订户违规使用而造成的任何责任。

4.5.1 订户私钥和证书的使用

订户接受到数字证书后，应妥善保存其证书对应的私钥。订户可以从智慧 CA证书目录服务器中下载个人或其他数字证书。

对于签名证书，其私钥仅用于对信息的签名。在可能的情况下，签名证书应同被签名信息一起提交给依赖方。订户使用私钥对信息签名时，应该确认被签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。

证书应用范围：

编号	订户	证书类型	订户私钥与证书的用途
1	个人	**个人高级证书**	订户使用此证书来向对方表明个人的身份，同时应用系统也可以通过证书获得订户的其他身份信息。主要用于：文档签名、个人网上购物、网上炒股等。
2		**个人安全邮件证书**	个人E-mail证书使订户个人可以在重要的邮件通信中对信件内容进行加密和签名操作。
3	机构	**机构高级证书**	颁发给独立的机构、组织，在互联网上证明该机构、组织的身份。 主要用于：文档签名、网上工商事务、网上招标投标、网上签约、安全网上公文传送、网上缴费、网上缴税、网上购物和网上报关等。
4		**机构安全邮件证书**	机构E-mail证书使机构订户可以在重要的邮件通信中对信件内容进行加密和签名操作。

4.5.2依赖方公钥和证书的使用

依赖方只能在接受智慧 CA 协议要求的前提下，才能依赖智慧 CA 订户证书。在信任证书和签名前，依赖方必须根据环境和条件进行合理地判断并做出决定。

在依赖证书前，依赖方必须独立的进行如下评估和判断：

1）证书是否由可信任的 CA 所签发；

2）证书被适当的使用，判断该证书没有被用于电子认证业务规则或者法律法规禁止或限制的使用范围；

3）证书的使用与证书密钥用途包含内容是否一致；

4）查询证书及其证书信任链中的证书状态，如果订户证书或其信任链内的任何证书已经被注销，依赖方必须独立去了解该订户证书对应的私钥所做的签名是否是在注销之前做的，是否可以依赖，并独立承担相应的风险。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密并发送给接受方。

获得对方的证书和公钥，可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

4.6 证书更新

证书更新指在不改变证书订户的公钥或其他任何信息的情况下，为订户签发一张新证书。证书更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，使用原证书的私钥对包含公钥的更新申请信息签名。

4.6.1证书更新的情形

为保证证书及其密钥对的安全有效和订户的权利，智慧 CA 会为签发的证书设置有效期。订户必须在证书有效期到期前一个月内，到智慧 CA 授权的发证机构申请更新证书。证书到期一个月后，如果订户还未申请证书更新，智慧 CA 视情况有权注销该证书。证书注销后订户如需继续使用，必须重新申请新证书。

4.6.2请求证书更新的实体

请求更新的实体为证书订户本人或其授权代表。

4.6.3证书更新请求的处理

订户或其授权人通过已有私钥，在智慧 CA 授权的发证机构通过 PIN 码验证和身份信息核查，进行更新请求；或在智慧 CA 授权的发证机构书面填写 《智慧 CA 数字证书业务申请表》 。智慧 CA 授权的发证机构按照第3章识别与鉴定的规定对订户提交的证书更新申请进行审核。发证机构审核通过后，为订户制作证书；证书签发后，发证机构将证书当面发给订户。订户接受证书（参见第4.4节）；新证书签发后原有证书将被注销（参见第 4.9 节）。智慧 CA 将实时在 LDAP 上发布订户的新证书。订户被注销的原有证书将在24小时内通过 CRL 发布。

订户也可以选择一般的初始证书申请流程进行证书更新，按照本 CPS3.2 的要求提交相应的证书申请和身份证明资料。智慧 CA 在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

提出更新申请的订户在进行证书更新之前应将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行证书的更新。如订户未解密文件而进行证书更新，由此造成的可能损失，智慧 CA 不承担任何责任。

4.6.4颁发新证书时对订户的通告

同第 4.3.2 节“订户证书签发的通知”。

4.6.5构成接受更新证书的行为

同第 4.4.1 节“构成接受证书的行为”。

4.6.6电子认证服务机构对更新证书的发布

同第 4.4.2 节“电子认证服务机构对证书的发布”。

4.6.7电子认证服务机构对其他实体的通告

同第 4.4.3 节“电子认证服务机构对其他实体的通告”。

4.7 证书密钥更换

证书密钥更换是指不改变证书中包含的信息的情况下，产生新的密钥对，并由智慧 CA 签发新证书。

4.7.1证书密钥更换的情形

证书订户申请更换密钥的情形主要有：

证书的密钥泄露。对此，订户负有立即告知智慧 CA 的责任；

证书到期时，要求更换证书密钥；

证书丢失；

其他：例如，由于信息技术的不断更新，为了保证证书的安全性，智慧 CA 有权要求订户更换证书的密钥。

4.7.2请求证书密钥更换的实体

请求密钥更换的实体为证书订户本人或其授权代表。

4.7.3证书密钥更换请求的处理

同第 4.6.3 节“证书更新请求的处理”。

4.7.4订户新证书签发的通知

同第 4.6.4 节“通知订户新证书签发”。

4.7.5构成接受密钥更换证书的行为

同第 4.4.1 节“构成接受证书的行为”。

4.7.6电子认证服务机构对密钥更换证书的发布

同第 4.4.2 节“电子认证服务机构对证书的发布”。

4.7.7电子认证服务机构对其他实体的通告

同第 4.4.3 节“电子认证服务机构对其他实体的通告”。

4.8 证书变更

4.8.1证书变更的情形

证书变更指改变证书中除订户公钥之外的信息而签发新证书的情形。订户证书只有在有效期内，才可能发生证书变更的情况。证书变更的原因有：

证书订户甄别名更改；

证书订户 E-mail 更改；

其他：如通用名、组织、角色改变等原因。

4.8.2请求证书变更的实体

请求证书变更实体为证书订户本人或其授权代表。

4.8.3证书变更请求的处理

证书变更按照初次申请证书的注册过程进行处理。

4.8.4颁发新证书时对订户的通告

同第 4.6.4 节“颁发新证书时对订户的通告”。

4.8.5构成接受变更证书的行为

同第 4.4.1 节“构成接受证书的行为”。

4.8.6电子认证服务机构对变更证书的发布

同第 4.4.2 节“电子认证服务机构对证书的发布”。

4.8.7电子认证服务机构对其他实体的通告

同第 4.4.3 节“电子认证服务机构对其他实体的通告”。

4.9 证书注销和挂起

4.9.1证书注销的情形

当发现以下的情况，证书必须被注销：

1) 私钥失窃、篡改、未经授权的泄露和其它安全威胁；

2) 证书主体（无论是 CA 还是订户）违反了 CPS 规定的重要职责；

3）CPS 中职责的履行被延迟或受不可抗力的阻碍、自然灾害、法律、规章或其它法律的改变、政府行为或其它超过个人控制的原因并且对他人信息构成威胁的；

4）订户主动提出注销请求；

5）智慧 CA 发现订户在申请时提供的证明材料不真实；

6）智慧 CA 已经履行催缴义务后，订户仍未缴纳服务费。

4.9.2请求证书注销的实体

请求证书注销的实体包括：

1）订户本人或其授权代表；

2）智慧 CA 或其授权机构的授权代表；

3）司法机关等公共权力部门的授权代表。

4.9.3注销请求的流程

订户到智慧 CA 授权的发证机构书面填写《智慧 CA 数字证书业务申请表》，并注明注销的原因。智慧 CA 授权的发证机构按照第3章识别与鉴定的规定对订户提交的证书注销申请进行审核。智慧 CA 注销订户证书后，发证机构将当面通知订户证书被注销。

如是强制注销，智慧 CA 授权的发证机关管理员可以对订户证书进行强制注销，注销后立即通知该证书订户。强制注销的命令来自于：智慧 CA、智慧 CA 授权的发证机构或司法机关等公共权力部门。

订户证书在24小时内进入 CRL 或被直接签发 CRL ，向外界公布。

4.9.4注销请求宽限期

当最终订户发现出现第 4.9.1 章节中的情况时，应该尽快提出证书注销请求，注销请求必须在密钥泄密或有泄密嫌疑8小时以内发现提出，其它注销原因从发现需要注销证书到向智慧 CA 或注册机构提出注销请求的时间间隔必须在24小时以内提出。

4.9.5电子认证服务机构处理注销请求的时限

智慧 CA 从收到证书注销请求起24小时内完成请求的处理。

4.9.6依赖方检查证书注销的要求

依赖方在信任证书前，必须对证书的状态进行检查，包括：

1）在使用证书前根据智慧 CA 最新公布的 CRL 检查证书的状态；

2）验证 CRL 的可靠性和完整性，确保它是经智慧 CA 发行并电子签名的。

依赖方应根据智慧 CA 公布的最新 CRL 或提供的 OCSP 服务确认使用的证书是否被注销。如果公布证书已经注销，而依赖方没有检查，由此造成的损失由依赖方本身承担。

4.9.7CRL发布频率

智慧 CA CRL 发布周期为24小时，特殊紧急情况下可以立即签发 CRL 。

4.9.8CRL发布的最大滞后时间

智慧 CA 注销的证书从被注销到被发布到 CRL 上的滞后时间最大为24小时。

4.9.9在线状态查询的可用性

智慧 CA 向证书订户提供 7×24 在线证书状态查询服务（ OCSP ）。

4.9.10注销状态查询要求

依赖方在信赖一个证书前必须通过证书状态查询检查该证书的状态。如果依赖方不希望通过最新的相关证书注销列表来检查证书状态，则应通过可用的 OCSP 服务对证书状态进行在线检查。

4.9.11注销信息的其他发布形式

智慧 CA 网站（http://www.smartcert.cn）提供 CRL 文件下载。

4.9.12密钥损害的特别要求

智慧 CA 所有订户在发现证书密钥受到损害时，应立即通知智慧 CA 注销证书。

4.9.13证书挂起的情形

证书挂起是证书注销的一种特殊情形，由于某种原因暂停使用证书。例如：订户由于某种原因如长期出差，短期内无法使用证书，可以申请证书挂起。

4.9.14请求证书挂起的实体

请求证书挂起的人包括：

1）订户本人或其授权代表；

2）智慧 CA 或其授权机构的授权代表；

3）司法机关等公共权力部门的授权代表。

4.9.15挂起请求的流程

申请者到智慧 CA 授权的发证机构书面填写《智慧 CA 数字证书业务申请表》，并注明挂起的原因。智慧 CA 授权的发证机构按照第3章识别与鉴定对订户提交的证书挂起申请进行审核。如是强制挂起，智慧 CA 授权的发证机关管理员可以依法对订户证书进行强制挂起，挂起后必须立即通知该证书订户。强制挂起的命令来源于：司法机关或智慧 CA 授权的发证机构。智慧 CA 挂起订户证书后，发证机构将当面通知或通过发送 E-mail 邮件或邮寄等方式通知订户证书被挂起。

4.9.16挂起的期限限制

订户证书被挂起后，订户必须在证书有效期到期前解挂证书，否则智慧 CA 或智慧 CA 授权的发证机构有权自行注销证书。对此造成的任何后果，智慧 CA 不负责任。

4.9.17证书解挂

证书挂起订户或其授权者，在需要解挂时到智慧 CA 授权的发证机构书面填写《智慧 CA 数字证书业务申请表》，并注明解挂的原因。智慧 CA 授权的发证机构按照第3章识别与鉴定对订户提交的证书解挂申请进行审核。审核通过之后，为用户解挂证书，并通知用户证书已解挂。

4.10 证书状态服务

智慧 CA 通过 CRL、OCSP、LDAP 提供证书状态服务。

4.10.1操作特征

智慧 CA 提供以下三种方式为证书订户提供证书状态查询。

1）通过发布服务器采用 HTTP 方式发布 CRL ，其可信度及安全性由根证书的签名来保证。订户需要将 CRL 下载到本地后进行验证，包括 CRL 的合法性验证和检查 CRL 中是否包含待检验证书的序列号。

2）提供 OCSP（在线证书状态查询）服务，以网络服务的方式提供证书状态信息，符合 RFC2560 标准。

3）提供 LDAP 目录查询证书状态服务，符合 LDAPv3 标准。

4.10.2服务可用性

智慧 CA 至少24小时发布一次 CRL 。

智慧 CA 的 OCSP （在线证书状态查询）服务，对依赖方提供 7×24 小时服务。

4.10.3可选特征

证书状态的其他可选服务方式为订户利用智慧 CA 指定的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的查询。

4.11 订购结束

订购结束,即服务终止，是指证书订户终止与智慧 CA 的服务，它包含以下两种情况：

1.证书到期时终止与智慧 CA 的服务；当证书到期时，证书订户不再延长证书使用期或者不再重新申请证书时，证书订户可以提出服务终止。

2.证书未到期时中止与智慧 CA 的服务；在证书的有效期内，由于证书订户的原因而单方面要求终止证书服务。

智慧 CA 将根据证书订户的要求注销证书，证书订户与智慧 CA 的服务终止。

4.12 密钥生成、备份与恢复

4.12.1密钥备份与恢复的策略与行为

证书订户的加密密钥由密钥管理中心（ KMC ）托管备份，当证书订户本人、国家执法机关、司法机关或其他管理部门因管理需要提出恢复加密密钥时，由智慧 CA 通过相应程序从 KMC 为其取得相应的加密密钥。加密密钥被加密存放在 KMC 管理中心。

为保证订户签名私钥的安全性，智慧 CA 不保管签名私钥。因此，要求订户妥善保管签名私钥。由于签名私钥遗失所造成的损失由证书订户自己承担，智慧 CA 不负责。

4.12.2会话密钥的封装与恢复的策略与行为

非对称算法组织数字信封的方式来封装会话密钥，数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解密并恢复会话密钥。

5 认证机构设施、管理和操作控制

5.1 物理控制

智慧 CA 电子认证服务机构的物理环境满足以下安全要求：

防止物理非法进入智慧 CA 通过入侵报警、视频监控等安防设施对定义的管理区域进行实时监测，并建立完善的安全管理制度，保护智慧 CA 的电子认证服务设施。

防止未授权访问，智慧 CA 通过门禁系统和权限分割的管理模式，确保不发生未经过授权或越权的区域访问。

5.1.1场地位置与建筑

智慧 CA 电子认证服务业务的运行场地位于南京市雨花台区软件大道172号一楼。根据GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》要求，机房分为以下各区域：

服务区：

该区域是提供证书录入、审批、签发以及证书管理的电子认证服务区域，配备了 RA 管理终端、RA 审计终端。

CA 服务区：

该区域是电子认证 RA、OCSP 系统管理区域，主要用于放置 RA 系统、OCSP 系统的软硬件设备，区域内安装有精密空调和柜式七氟丙烷气体灭火系统，门禁采用双人控制出入。核心区还专门配备了呼吸机防止突发情况的发生。

核心区：

该区域是 CA 系统、 KM 系统、根密钥密码设备、数据库系统软硬件存放的区域。配备有管理终端、审计终端和保险柜。配备有精密空调、柜式七氟丙烷气体灭火系统。核心区还专门配备了呼吸机防止突发情况的发生。

UPS区：

该区域装有市电控制柜，配置了爱克赛模块化 UPS 120KVA（配置40KVA模块）不

间断电源，配有64组电池。市电中断后，可确保机房所有设备持续工作8小时不间断。并配有备用发电机接入接口，保障计算机设备供电可靠性。

5.1.2物理访问

智慧 CA 的核心机房和各功能区域的访问控制系统是与控制各区域进出的门禁系统相结合的，并实现了以下安全功能：

进出每一区域的门都有记录作为审计依据；

核心机房的安全区域采用密码和指纹验证的结合方式控制，采用双人身份鉴别控制每道门的进出；

其他区域只采用身份鉴控制门的进出；

授权人员进出每一道门都会有时间记录；

只有相关授权人员使用授权口令才可以登录访问物理设备；

涉及物理设备密码及重大系统操作的，必须两人以上同时在场才可操作；

高安全级别的重要系统设备的操作与维修，必须在机房内多人现场监控下现场完成且有相关记录。

5.1.3电力与空调

根据《机房建设概算》和《电子计算机机房设计规范》（国标GB50174-2008）的有关规定，中心机房的温湿度控制执行B级标准，即温度为 23℃±5℃，相对湿度为55%±15%，空气洁净度为粒径≥0.5um，个数≤18000/dm3，所采购的空调设备满足上述要求。

为保证系统设备的正常运转，避免服务器在过热的条件下工作，在屏蔽机房内安装了Olywell S40 精密空调。

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。使用不

间断电源（UPS）来保证供电的稳定性和可靠性。

5.1.4水患防治

智慧 CA 在机房设计建设时已充分考虑水患进行防水设计和建设，并采取相应措施，防止水侵蚀，充分保障系统安全。

5.1.5火灾防护

智慧 CA 在设备机房内按照国家标准建设安装有火灾报警系统和消防应急联动处理系统，并通过与专业消防部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，防止明火或者烟雾对系统造成损害或不利影响，充分保障系统安全。

5.1.6介质存储

智慧 CA 对存储有系统程序、订户数据、维护记录、日志文件、备份数据等信息的介质保存到相应的安全区域中，介质得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏，并且只有授权人员才能访问。

5.1.7废物处理

智慧 CA 对作废的相关业务文件和材料按照数据和记录销毁流程经安全中心审批通过后，通过粉碎、焚烧或其它不可恢复的方法处理，废弃的密码设备在销毁处置前根据产品提供商的操作指南将其物理销毁或初始化，其他废物处理按照智慧 CA 的相关处理要求进行，所有处理行为将记录在案。

5.1.8异地备份

智慧 CA 对业务系统中的程序、数据等关键信息按照数据备份策略和流程行成安全备份。备份介质按照备份策略和流程保存在本地机房和异地备份。在异地备份时按照策略和流程由专人送交到银行保险柜保管。以上所有操作流程将记录在案。

5.2 程序控制

5.2.1可信角色

在智慧 CA 提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和注销等涉及密钥操作的职位都被智慧 CA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理员、系统管理员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以智慧 CA 的岗位说明书为准。

5.2.2每项任务需要的人数

智慧 CA 确保单个角色不能接触、导出、恢复、更新、废止智慧 CA 的 CA 系存储的根证书对应的私钥。对于关键的操作进行物理与逻辑上的分割控制，使掌握设备物理权限的人不能再拥有逻辑权限。至少两个可信角色才能使用一项对参加操作人员保密的密钥分割和合成技术来进行任何钥匙恢复的操作。

智慧 CA 对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制，保证至少一人操作，一人监督记录。

5.2.3每个角色的识别与鉴别

所有智慧 CA 的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用密码加指纹识别；进入系统需要使用数字证书进行身份鉴别。智慧 CA 将独立完整地记录其所有的操作行为。

5.2.4需要职责分割的角色

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。智慧 CA 人员职责分割的角色包括（但不限于）以下几种：

- 安全管理员；
- 密钥管理员；
- 证书申请录入员；
- 证书申请审核员；
- 证书制证员；
- 审计管理员；
- 系统维护员。

5.3 人员控制

5.3.1资格、经历和无过失要求

智慧 CA 员工的录用需经过严格的核实和审查，根据岗位需要增加相应可信员工。

员工一般需要有2-3个月的考察期，根据考察的结果安排相应的工作或辞退。根据需要对员工进行职责、岗位、技能、政策、法律、安全等方面的培训。

智慧 CA 会对关键的 CA 员工进行背景调查。背景调查主要包括：

1）身份验证；

2）学历等其他资格、资历证书；

3）个人履历，包括教育经历、工作经历及相关证明人等；

4）无犯罪记录证明材料。

受理点责任机构可以参照智慧 CA 对可信任员工的考察方式，可以在此基础上增加考察和培训条款，但不得违背智慧 CA 认证业务声明。

智慧 CA 确立流程管理规则，所有员工与智慧 CA 签订保密协议，据此 CA 员工受到合同和章程的约束，不得泄露智慧 CA 证书服务体系的敏感信息。

5.3.2背景审查程序

智慧 CA 制定了员工背景审查程序，对可信员工进行背景调查。身份背景调查过程中，存在（但不限于）下列情形之一，不得通过可信审查：

1）伪造相关证件材料的；

2）伪造工作经历及工作证明人虚假的；

3）虚假声称具有某种技能、能力的证件；

4）以往工作中存在重大不诚实行为的；

5）有犯罪记录的。

5.3.3培训要求

智慧 CA 对不同岗位 CA 员工有针对性的进行以下有关内容的培训：

智慧 CA 操作的系统和网络；

智慧 CA 质量控制体系；

智慧 CA 安全管理策略和机制；

PKI 基础知识；

智慧 CA 电子认证业务规则；

智慧 CA 管理政策、制度及办法等；

国家关于电子认证服务的法律、法规及标准、程序；

其他需要进行的培训等。

5.3.4再培训周期和要求

根据智慧 CA 策略调整、系统更新等情况，将对员工进行继续培训，以适应新的变化。对于公司安全管理策略，每年对员工进行一次以上的培训，对于相关业务技能培训应每年进行一次以上的业务技能培训。

5.3.5工作岗位轮换周期和顺序

根据岗位人员和业务上的实际情况内部自行安排。

5.3.6未授权行为的处罚

当智慧 CA 员工进行了未授权或越权操作，在确认后将立即中止该员工进入智慧 CA 证书服务体系，根据情节严重程度实施包括提交司法机关处理等措施。

一旦发现上述情况，智慧 CA 立即作废或终止该人员的安全令牌。

5.3.7独立合约人的要求

智慧 CA 的独立合约人及顾问执行与普通员工一致的可信资格确认，不安排其接触系统核心软/硬件及网络设施并对其按照合同进行审计和监察。

5.3.8提供给员工的文档

为使得系统正常运行，必须提供给具有权限的相关人员各种文档，这些文档包括：

- 软/硬件、网络设备安全操作手册
- 加密机、密钥管理安全操作手册
- RA 系统相关安全操作手册
- 智慧 CA 运行策略、运行规范
- 系统备份与恢复安全操作规范和手册等其他文档。

5.4 审计日志程序

5.4.1记录事件的类型

智慧 CA 的 CA 和 RA 运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

智慧 CA 应记录的内容包括（但不限于）：

1）系统安全事件，包括：CA 系统、 RA 系统和其他服务系统的活动，系统崩溃，硬件故障和其他异常。

2）电子认证服务系统操作事件，包括系统的启动和关闭。

3）认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进入认证机构设施及陪同人和安全存储设施的访问。

4）证书生命周期相关事件。

5.4.2处理日志的周期

对于 CA 和订户证书生命周期内的管理事件日志，智慧 CA 将一个季度进行一次内部检查、审计。

对系统安全事件和系统操作事件日志，智慧 CA 将每月进行一次检查、处理。对物理设施的访问日志，智慧 CA 将每月进行一次检查、处理。

5.4.3审计日志的保存期限

智慧 CA 会妥善保存认证服务的审计日志，本地保存期限至少两个月，离线存档为五年。

5.4.4审计日志的保护

智慧 CA 执行严格的保护和管理，确保只有智慧 CA 授权的人员才能访问这些审查记录。并且实现异地备份，并禁止访问、阅读、修改和删除等操作。

5.4.5审计日志备份程序

智慧 CA 保证所有的审查记录和审查总结都按照智慧 CA 备份标准和程序进行。

根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

5.4.6审计收集系统

智慧 CA 审查采集系统涉及：

证书签发系统；

证书注册系统；

证书目录系统；

证书审批受理系统；

访问控制系统（包括防火墙）；

网站、数据库安全保障系统；

其他智慧 CA 认为有必要审查的系统。

5.4.7对导致事件实体的通告

智慧 CA 将依据法律、法规的监管要求，对一些恶意行为，如网络攻击等，通知相关的主管部门，并且智慧 CA 保留进一步追究责任的权利。

5.4.8脆弱性评估

CA 安全程序根据政策、技术和管理的变化及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补，属于不可弥补的薄弱环节，智慧 CA 每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1归档记录的类型

智慧 CA 按照制度和流程定期对电子生成和（或者）手工生成的重要数据定期存档。存档的内容包括订户资料、电子认证系统签发的系统证书和订户证书、证书注销列表 CRL 、电子认证系统维护操作记录、可信人员进出机房操作记录、外来人员进出记录、数据备份记录、涉及电子认证安全的事件记录及审计数据等。

5.5.2归档记录的保存期限

智慧 CA 归档存档期限一般规定为五年。订户资料保存期限为订户证书过期后五年。

5.5.3归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能获取。智慧 CA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

5.5.4归档文件的备份程序

所有纸质归档记录按照备份策略和流程由专人定期执行，备份介质在智慧 CA 公司本地备份管理。按照备份策略和流程，电子存档文件除了在智慧 CA 内本地备份外，还将在异地保存其备份。

5.5.5记录时间戳要求

所有5.5.1条款所述的存档内容都按照归档策略和流程分别由专人收集、归档、审核和保管。所有归档记录上均有参与归档操作的人员与时间记录。

5.5.6归档收集系统

智慧 CA 的档案收集系统由人工操作和自动操作两部分组成。

5.5.7获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。所有记录被访问后，需验证其完整性。此外，智慧 CA 每年验证存档信息的完整性。

5.6 电子认证服务机构密钥更替

在 CA 的密钥对遭受攻击或因为密钥生命期而需要更新密钥对的情况下，由安全策略委员会授权，所有密钥管理员在场，共同启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥。密钥更换及自签名证书按照规定报告上级管理机构。

5.7 损害与灾难恢复

5.7.1事故和损害处理程序

智慧 CA 已制定各种应急处理方案，规定了相应的事故和损害处理程序，应急处理方案包括：

认证系统应急方案；

电力系统应急方案；

消防应急方案；

网络与信息系统应急方案；

安全事故应急处理方案等。

涉及电子认证机构的重大事故应按照规定及时上报管理机构。

5.7.2计算资源、软件或数据的损坏

智慧 CA 对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程。当出现计算机资源、软件或数据的损坏时，能在最短的时间内恢复被损害的资源、软件和/或数据。

5.7.3实体私钥损害处理程序

对于实体私钥的损害，智慧 CA 有如下处理要求和程序：

1）当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即通知智慧 CA 或注册机构注销其证书。智慧 CA 按 CPS 4.9 发布证书注销信息。

2）当智慧 CA 或注册机构发现证书订户的实体私钥受到损害时，智慧 CA 或注册机构将立即注销证书，并通知证书订户，订户必须立即停止使用其私钥。智慧 CA 按 CPS 4.9 发布证书注销信息。

3）当智慧 CA 的证书出现私钥损害时，智慧 CA 将立即注销CA证书并及时通过途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

5.7.4灾难后的业务连续性能力

除非物理场地出现了毁灭性的、无法恢复的灾难，智慧 CA 能够在出现灾难后最短时间内恢复其业务能力。

5.8 电子认证服务机构或注册机构的终止

当智慧 CA 打算终止经营时，会在终止经营前三个月给智慧 CA 授权的发证机构、垫付商和证书持有者书面通知，并在终止服务六十日前向国务院信息产业主管部门报告,按照相关法律规定的步骤进行操作。

智慧 CA 会按照相关法律的规定来安排好档案和证书的存档工作。在 CA 终止期间，采用以下措施终止业务：

起草 CA 终止声明；

通知与 CA 停止相关的实体；

关闭主从目录服务器；

证书注销；

停止认证中心的服务；

存档主目录服务器；

处理智慧 CA 系统管理员和业务管理员；

处理加密密钥；

处理和存储敏感文档；

清除 CA 主机硬件。根据智慧 CA 与 RA 签订的协议终止 RA 的业务。

由于密钥受损和非密钥受损原因而终止智慧 CA，要完成相似的操作，唯一不同在发送智慧 CA 终止通知的时间限制上：由于密钥受损原因终止智慧 CA ，要求智慧 CA 通知订户的过程尽快完成；由于非密钥受损的原因终止智慧 CA ，在通知所有订户后，采取适当的步骤减轻智慧 CA 终止对订户的影响。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在电子认证业务规则中制定了相应的规定，通过物理安全控制和密钥安全存储控制来确保密钥对的产生、传送、安装等过程中符合保密性、完整性和不可否认性的需求。

6.1.1密钥对的生成

加密密钥对是由中华人民共和国国家密码管理局许可的密钥管理中心控制管理。签名密钥对是由中华人民共和国国家密码管理局许可的、智慧 CA 数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证智慧 CA 无法复制签名密钥对。智慧 CA 支持多种介质。智慧 CA 可根据证书申请者要求或自身选择签名密钥对生成介质。

6.1.2加密私钥传送给订户

订户自己生成的密钥对的情况下，不需要将私钥传给订户。证书订户的加密私钥是在智慧密钥管理中心产生的，该私钥只保存在密钥管理中心。在加密私钥从智慧密钥管理中心到订户的传递时，采用国家密码管理局许可的对称密钥算法加密，其他人或机构无法获得，这样就保证了证书订户加密私钥的安全。

6.1.3公钥传送给证书签发机构

智慧 CA 从密钥管理中心取得订户加密公钥后为其签发证书，在此过程中采用国家密码管理局许可的对称密钥算法加密，保证了传输中密钥的安全。自生成密钥对证书订户向智慧 CA 提交证书申请时，该请求信息内的公钥，使用安全通道保证信息的机密性和完整性。

电子认证服务机构公钥传送给依赖方智慧 CA 的根公钥包含在智慧 CA自签发的根证书中。证书订户可以从智慧 CA 的网站（http://www.smartcert.cn）上下载智慧 CA 根证书，也可以由智慧 CA 通过目录系统、业务系统的安装、电子邮件和软件绑定等方式提供给依赖方。

6.1.4密钥的长度

为了保证加密/解密的安全性，智慧 CA 所使用的加密和签名的非对称密钥对的模长是256比特，对称密钥的长度是128比特。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，智慧 CA 将会完全遵从。

6.1.5公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、智慧 CA 数字证书签发系统支持的硬件生成；质量检查由国家密码管理局具体实施。

6.1.6密钥使用用途

在智慧 CA 证书服务体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

智慧 CA 的签名密钥用于签发 RA 证书和证书注销列表（CRL）；

RA 的签名密钥用于确认 RA 所做的审批证书等操作；

订户的签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；

订户加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。更多与协议和应用相关的密钥使用限制请参阅 X.509 标准中的密钥用途扩展域。

6.2 私钥保护和密码模块工程控制

6.2.1密码模块的标准和控制

智慧 CA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

6.2.2私钥多人控制（5选3）

智慧 CA 采用多人控制策略，激活、使用、备份、停止和恢复智慧 CA 的签名密钥，采取5个管理人员中至少3个在场才可进行操作的原则。

6.2.3私钥托管

密钥管理中心可以根据客户和法律的需要，对加密密钥进行托管。签名私钥由订户自己保管，以保证其不可否认性。

6.2.4私钥备份

用户的签名密钥智慧 CA 都不备份。加密私钥由密钥管理中心备份，备份数据以密文形式存在。

6.2.5私钥归档

密钥管理中心提供过期的托管私钥的存档服务；保存期为五年。当私钥过了保存期，将依据相关规定对其进行销毁。

6.2.6私钥导入、导出密码模块

在智慧 CA 业务系统中，可以把订户的私钥导入指定的密码模块中。私钥应从硬件密码模块中导出，必须通过密码验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

智慧 CA 的根 CA 私钥在硬件密码模块上生成，保存和使用。智慧 CA 对根 CA 私钥进行严格的密钥管理和备份、恢复控制，有效防止了根 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

6.2.7私钥在密码模块的存储

智慧 CA 私钥以加密的形式存放在硬件密码设备中，并在该设备中使用。

6.2.8激活私钥的方法

智慧 CA 将订户证书的私钥保存在 USB Key 或智能卡等硬件密码模块中，只有输入 PIN 码，私钥才能被激活使用。

6.2.9解除私钥激活状态的方法

对于存放在软件密码模块中的证书的私钥，当软件密码模块被下载、订户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。对于存放在硬件密码模块中的订户证书私钥，通过 PIN 码激活私钥后仅活动一次后即解除其激活状态。

6.2.10 销毁私钥的方法

对于智慧 CA 签发的订户加密证书私钥，在其生命周期结束后，智慧密钥管理中心对该密钥进行归档妥善保存一定期限，以便于解开加密信息。对于智慧 CA 签发的订户签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

6.2.11 密码模块的评估

智慧 CA 使用国家密码主管部门批准和许可的密码产品。

6.3 密钥对管理的其他方面

6.3.1公钥归档

对于生命周期外的 CA 和订户证书，智慧 CA 将进行归档。归档的证书存放在归档数据库中。

6.3.2证书操作期和密钥对使用期限

证书操作期终止于证书过期或者被注销。智慧 CA 为订户颁发的证书操作周期通常与密钥对的使用周期是相同的。对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。为了保证能够验证在证书有效期内的签名的信息，公钥的使用期限可以在证书的有效期限外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

6.4 激活数据

6.4.1激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质出厂时设置了缺省的PIN值，证书制作时激活证书存储介质的PIN码。

6.4.2激活数据的保护

智慧 CA 采取加解密机制等多种方式保护激活数据，以避免未授权的使用。未

授权用户尝试使用激活数据时，尝试达到预定的次数，激活数据会自动锁定。

6.4.3激活数据的其他方面

只有在拥有证书介质并知道证书介质的PIN值时才能激活证书存储介质，进而使用私钥。

6.5 计算机安全控制

6.5.1特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

对于设备有一套完整的保管和维护制度：

1) 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。

2) 对设备定期进行检查、清洁和保养维护。

3) 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。

4) 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。

5) 设备维修时，必须有派专人在场监督。

6.5.2计算机安全评估

智慧 CA 电子认证系统已通过国家密码管理局组织的安全性审查和安全技术鉴定。

6.6 生命周期技术控制

6.6.1系统开发控制

按照智慧 CA 内部系统开发流程进行控制。

6.6.2安全管理控制

智慧 CA 的配置以及任何修改和升级都会记录在案并进行控制，并且智慧 CA 采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。认证系

统只开放与业务相关的功能，只有智慧 CA 授权的员工能够进入智慧 CA 的系统或设备。

6.6.3生命周期的安全控制

智慧 CA 的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查和技术鉴定。

6.7 网络的安全控制

智慧 CA 网络中有防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制保护，其配置只允许已授权的机器访问。只有经过授权的智慧 CA 员工才能够进入智慧 CA 签发系统、智慧 CA 注册系统、智慧 CA 目录服务器、智慧 CA 证书发布系统等设备或系统。所有授权订户必须有合法的安全令牌，并且通过密码验证。

CA 系统只开放与申请证书、查询证书等相关操作功能，其他端口和服务全部关闭。 CA 系统的边界控制设备拒绝一切非电子认证业务的服务。

6.8 时间戳

智慧 CA 认证系统的各种系统日志、操作日志有对应的记录时间。

7 证书、证书注销列表和在线证书状态协议

7.1 证书

智慧 CA 签发的证书均符合 X.509 V3 证书格式，遵循 RFC3280 标准。

7.1.1版本号

X.509 V3

7.1.2证书标准项及扩展项

1. 证书标准项：

C=×× C（Country）应为CN，表示中国；

S=×× S（state）应为证书主体或证书主体所属单位所在省、自治区、直辖市的名称全名

L=×× L（Location）为证书主体或证书主体所属单位的所在城市的全称；

O=×× O（Organization）证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；（非必选）

OU=×× OU（Organization Unit）应为证书主体或者证书主体所属单位的全称；（非必选）

CN=×× CN（Common Name）中的内容分为2种：

1)个人证书中应为证书主体的姓名；

2)单位机构证书中应为证书主体单位的名称或企业税务登记号；

2.证书扩展项：

智慧 CA 证书扩展项除使用IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

智慧 CA 采用的IETF RFC 3280 中定义的证书扩展项：

- 颁发机构密钥标识符 Authority Key Identifier
- 主体密钥标识符Subject Key Identifier

- 密钥用法Key Usage
- 扩展密钥用途Extended Key Usage
- 主体可选替换名称Subject Alternative Name
- 基本限制Basic Constraints
- 证书撤销列表分发点CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份识别码Identify Card Number
- 企业工商注册号IC Registration Number
- 企业组织机构代码Organization Code

7.1.3算法对象标识符

智慧 CA 签发的证书按照 RFC 3280 标准，用 SM2 算法签名。

7.1.4名称形式

智慧 CA 签发证书的甄别名符合 X.500 关于甄别名的规定。详情参见第3.1节内容。

7.1.5名称限制

订户在证书中的名称可以是假名，但不能使用匿名，并在智慧 CA 的数据库中记录订户的相关信息。智慧 CA 可以按照一定的规则为订户指定特殊名称，并且能够把该类特殊的名称与一个确定的实体（个人、机构）唯一联系起来。

7.1.6证书策略对象标识符

没有定义。

7.1.7策略限制扩展项的用法

没有使用。

7.1.8策略限定符的语法和语义

没有规定。

7.1.9关键证书策略扩展项的处理规则

与X.509和PKI相关规定一致。

7.2 证书注销列表

智慧 CA 定期签发证书注销列表（ CRL ），其所签发的 CRL 遵循 RFC3280 标准。

7.2.1版本号

采用 X.509 V2 格式。

7.2.2CRL和CRL条目扩展项

CRL 扩展项：颁发机构密钥标识符。

CRL 条目扩展项：不使用 CRL 条目扩展项。

7.3 在线证书状态协议

7.3.1版本号

OCSP 版本：V3.5.2。

7.3.2OCSP 扩展项

未使用OCSP扩展项。

8 认证机构审计和其他评估

8.1 评估的频率或情形

根据情况而定，有年度评估、运营前评估、安全时间发生后的评估和随时进行评估。

智慧 CA 本身也需要对智慧 CA 的关联机构（包含智慧 CA 授权的注册机构、注册分支机构、受理点等证书体系成员）所有的流程和操作进行审计，检验其是否符合本电子认证业务规则和相应的证书政策的规定，其频率可由智慧 CA 决定或由法律制定的监管机构决定。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等的要求，每年一次接受上级主管部门的合规性审计。

根据审计结果，需要整改后复审的，应接受复审。

8.2 评估者的资质

对智慧 CA 实施规范审计的第三方所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且在业界享有良好的声誉；了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作；具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

对智慧 CA 进行审计的第三方，必须是一个独立于智慧 CA 的合法审计实体。智慧 CA 内部审计员不能与系统管理员、业务管理员、业务操作员等岗位重叠。

8.4 评估内容

审计工作包括：

安全策略是否得到充分实施；

运营工作流程和制度是否严格遵守；

电子认证业务规范是否符合证书策略的要求；

是否严格按照本 CPS、业务规范和安全要求开展业务；

各种日志、记录是否完整，是否存在问题；

是否其它可能存在的安全风险；

智慧 CA 支持的证书认证操作规程是否完全与本电子认证业务规则表达一致，包括智慧 CA 的技术、手续和员工的相关管理政策和电子认证业务规则；

智慧 CA 是否实施了相关技术、管理、相关政策和电子认证业务规则；

审计者或智慧 CA 认为有必要审计的其他方面。

8.5 对问题与不足采取的措施

如果在审计过程中发现执行有不足之处，由安全策略委员会监督这些问题的责任职能部门进行业务改进和完善的情况，完成对评估结果的改进后，各职能部门必须向安全中心提交业务改进工作总结报告。

如果在外部评估过程中发现执行有不足之处，智慧 CA 必须根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改方案，并接受对整改方案的审查，以及对整改情况的再次评估。

8.6 评估结果的传达与发布

除非法律明确要求，智慧 CA 一般不公开审计结果。在必要的情况下，智慧 CA 可依照与关联机构（例如垫付商、注册机构、注册分支机构、受理点）签订的协议中有关规定，向关联机构通知审计结果。

9 法律责任和其他业务条款

9.1 费用

证书相关费用在智慧 CA 的网站上公布（ http://www.smartcert.cn ）。价目表按智慧 CA 明确指定的时间生效，若没有指定生效时间的，自价目表公布之日起生效。智慧 CA 也可以通过其他方法通知证书持有者或其他各方费用变化。

9.1.1证书签发和更新费用

根据智慧 CA 的价目确定。

9.1.2证书查询费用

智慧 CA 目前不对证书查询收取专门的费用。

9.1.3证书注销或状态信息的查询费用

证书注销列表（CRL）的获取不收取任何费用。智慧 CA 有可能根据需要收取 OCSP 服务费用。

9.1.4其他服务费用

根据智慧 CA 的价目确定。

9.1.5退款策略

在实施证书操作和签发证书的过程中，智慧 CA 遵守并保持严格的操作程序和策略。一旦用户接受数字证书，智慧 CA 将不办理退证、退款手续。

如果用户在证书服务期内退出数字证书服务体系， 智慧 CA 将不退还剩余时间的服务费用。

9.2 财务责任

智慧 CA 保证具有维持、运作和履行其责任的经济基础，有能力承担对订户、依赖方因合法使用数字证书时而造成的责任风险，并依据本电子认证业务规则规定的方式和范围进行有过错时的赔偿。

9.2.1保险范围

出现下列情形并经公司确认后，证书订户、依赖方等实体可以申请赔偿（法定或约定免责除外）。

1）智慧 CA 在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发，并导致订户或依赖方遭受损失的；

2）智慧 CA 将证书错误的签发给订户以外的第三方，导致订户或者依赖方遭受损失的；

3）由于智慧 CA 的原因导致证书私钥被破译、窃取，导致订户或者依赖方遭受损失的；

4）智慧 CA 未能及时注销证书，导致订户或者依赖方遭受损失的。

9.2.2其他资产

智慧 CA 目前有能力维护运营和应对可能出现的赔付。

9.2.3对最终实体的保险或担保

智慧 CA 承担订户或依赖方在使用证书过程中造成损失时的举证责任，如无证据证明订户或依赖方使用过程中存在错误操作，则智慧 CA 将按照发布的赔偿办法予以赔偿。

9.3 业务信息保密

智慧 CA 有专门的信息保密制度，保护自身和订户的敏感信息、商业秘密。

9.3.1保密信息范围

智慧 CA 保密的信息包括（但不限于）：

1.系统方面

- 认证系统结构、配置，包括系统、网络、数据库等；

- 认证系统安全策略和方案；

- 系统操作、维护记录；

- 各类系统操作口令。

2.运营管理方面

- 物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；

- 密钥管理策略与操作记录；

- CA 或 RA 批准或拒绝的申请纪录；

- 可信人员名单；

- 内部安全管理策略与制度。

- 审计记录。

3.订户信息

- 订户的注册信息；

- 订户系统、应用访问 CRL、OCSP 的记录（时间、频度）；

- 订户与认证机构、注册机构签订的协议。

9.3.2不属于保密的信息

智慧 CA 电子认证业务规则、证书申请流程、手续、申请操作指南、证书注销列表等。

当智慧 CA 在任何法律、法规或规章条款的要求下，或在法院的要求下必须披露本认证业务声明中具有保密性质的信息时，智慧 CA 可以按照法律、法规或规章条款以及法院的总协定的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

9.3.3保护保密信息的责任

智慧 CA 有各种严格的管理制度、流程和技术手段保护自身的商业秘密，每个员工都必须接受信息保密方面的培训，并与公司签订保密协议。任何参与方有责任保证不泄露保密信息。

9.4 个人隐私保密

9.4.1隐私保密方案

智慧 CA 制定有隐私保护制度并签订保密协议，保证证书订户的个人信息不被滥用、未授权使用或出售，同时采取必要措施防止客户资料被遗失、盗用与篡改。

9.4.2作为隐私处理的信息

作为隐私处理的信息包括：最终订户注册申请证书中提交的信息，包括联系电话、地址等；订户与智慧 CA、注册机构签订的协议。

9.4.3不被视为隐私的信息

不被认为是隐私信息包括：用来构成证书内容的信息，证书及证书状态。

9.4.4保护隐私的责任

除非执法、司法方面的强制需要，智慧 CA 及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。

9.4.5使用隐私信息的告知与同意

智慧 CA 或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知订户并获得订户同意和授权，订户同意和授权信息以下列方式之一传送给智慧 CA 或其注册机构：

1）将手写签名的同意和授权文件邮寄、快递到智慧 CA 或其注册机构；

2）将手写签名的同意和授权文件传真到智慧 CA 或其注册机构；

3）以签名电子邮件的形式同意并授权。

9.4.6依法律或行政程序的信息披露

当智慧 CA 在任何法律、法规或规章条款的要求下，或在司法机关的要求下必须披露本电子认证业务规则中具有保密性质的信息时，智慧 CA 可以按照法律、法规或规章条款以及司法机关的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

9.4.7其他信息披露情形

对其他信息的披露受制于法律、订户协议。

9.5 知识产权

智慧 CA 保留对本 CPS 的所有知识产权。智慧 CA 保留其签发的证书和证书注销信息的所有知识产权。任何人可以免费地复制、分发证书和证书注销列表，只要他们进行完整复制并且证书和证书注销列表的使用符合相应的依赖方协议。证书申

请者保留证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发给该证书申请者的证书中的可辨识名的所有权利。证书所有者拥有其证书相关的密钥对的知识产权。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

除非智慧 CA 做出特别约定，若本电子认证业务规则的规定与其他智慧 CA 制定的相关规定、指导方针相互抵触，订户必须接受本电子认证业务规则的约束。在智慧 CA 与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本电子认证业务规则的规定执行；对协议中有不同于本电子认证业务规则内容的约定，按双方协议中约定的内容执行。

智慧 CA 承担的责任和义务是：

保证电子认证服务机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破；保证智慧 CA 的签名私钥在智慧 CA 内部得到安全的存放和保护；智慧 CA 建立和执行的安全机制符合国家政策的规定。智慧 CA 不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。针对上述内容补充解释如下：

第一：除上述所规定的职责条款，智慧 CA 的服务机构、智慧 CA 授权的发证机构、智慧 CA 的雇员不承担其它任何义务。必须指出，本电子认证业务规则的内容，没有任何信息可以暗示或解释成智慧 CA 必须承担其它的义务或智慧 CA 必须对其行为做出其它的承诺。

第二：在上述内容中所罗列不可抗力的任何情况下，智慧 CA 由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

第三：由于技术的进步与发展，为保证证书的安全性，智慧 CA 会要求证书持有者及时更换证书以保证智慧 CA 能更好地履行本节所述之责任。

9.6.2注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由智慧 CA 决定，并在本电子认证业务规则或相应的注册机构协议中规定，以后智慧 CA 可以根据情况修改有关内容，并及时公布。注册机构必须遵守和符合本电子认证业务规则的条款。具体内容详见本文档9.6.1。

9.6.3订户的陈述与担保

所有的订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序：

订户在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供智慧 CA 或受理点检查和核实；

订户必须严格遵守和服从电子认证业务规则规定的或者由智慧 CA 推荐使用的安全措施；订户需熟悉本电子认证业务规则的条例和与证书相关的证书政策，遵守订户证书使用方面的有关限制；

一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘或泄密以及其他情况，订户应立刻通知智慧 CA 或智慧 CA 授权的发证机构，申请采取挂失、废除等处理措施。

9.6.4依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。

9.6.5其他参与者的陈述与担保

遵守本CPS的所有规定。

9.7 担保免责

有下列情形之一的，应当免除智慧 CA 之责任：

1）订户在申请和使用智慧 CA 数字证书时，有违反如下义务之一的：

- 订户提供不真实、完整、准确的材料和信息，提供虚假或无效的材料和信息；

- 订户未妥善保管智慧 CA 所签发的数字证书载体和保护 PIN 码，泄漏 PIN 码或将数字证书载体随意交付他人；
- 订户在应用自己的密钥或使用数字证书时，未使用可依赖的、安全的系统；
- 订户知悉电子签名制作数据已经失密或者可能已经失密时，未及时告知智慧 CA 及相关各方，未终止使用该电子签名制作数据；
- 订户在使用数字证书时未遵守国家的法律、法规和行政规章制度，将数字证书在智慧 CA 规定使用范围之外的其他用途使用；
- 订户未在证书有效安全期内使用该证书，使用已失密或可能失密、已过有效期、被挂起、被注销的数字证书；订户未根据规定按时向智慧 CA 及当地业务受理点缴纳服务费用。

2）由于不可抗力原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“不可抗力”，是指不能预见、不能避免并不能克服的客观情况，包括（但不限于）：

- 自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、台风等；
- 社会异常或者政府行为，包括政府颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

3）智慧 CA 已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8 有限责任

在与订户和依赖方签订的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

1）对于由如下原因造成的订户或依赖方损失，智慧 CA 对订户或依赖方进行赔偿：

（1）智慧 CA 在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

（2）由于智慧 CA 的原因，使得证书中出现了错误信息。

2）在如下情况，订户对自身原因造成的智慧 CA、依赖方损失承担责任：

（1）订户在证书申请中对事实的虚假或错误描述；

（2）在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

（3）订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全措施，如：损害、丢失、泄漏、修改或非授权的使用；

（4）订户使用的名字（包括但不限于通用名、域名和 E-mail 地址）破坏了第三方的知识产权法。

3）在如下情况，依赖方对自身原因造成智慧 CA 损失承担责任：

（1）依赖方没有执行依赖方职责义务；

（2）依赖方在不合理的环境下信赖一个证书；

（3）依赖方没有检查证书状态确定证书是否过期或注销。

4）智慧 CA 承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

（1）如智慧 CA 违反了前文第 9.6 款条例规定的职责，智慧 CA 承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

智慧 CA 所有的赔偿义务不得高于这种证书适用的赔偿责任上限。赔偿责任上限为智慧 CA 收取该种证书服务费的十倍，最高不超过五万元人民币。

智慧 CA 对任何证书订户、依赖方等实体有关证书赔偿的合计责任限制偿上限可以由智慧 CA 根据情况重新制定，智慧 CA 将重新制定后的情况进行发布。

（2）对于由订户或依赖方的原因造成的损失，智慧 CA 不承担责任，由订户或依赖方自行承担。

（3）智慧 CA 只有在其证书有效期限内承担损失损害赔偿。

9.10 有效期限与终止

9.10.1有效期限

本CPS自发布之日起生效。

9.10.2终止

当新版本的智慧 CA CPS 生效时，旧版本智慧 CA CPS 自动终止；当智慧 CA 中止业务时，智慧 CA CPS 自动终止。

9.10.3效力的终止与保留

本 CPS 终止后，已签发符合本证书策略的证书，效力作用直到证书到期或撤消。当由于某种原因，如内容修改、与适用法律相冲突，证书策略、电子认证业务规则、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

9.11 对参与者的个别通告与沟通

智慧 CA 及其注册机构在必要的情况下，如在主动注销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等通知个别订户、依赖方。

9.12 修订

9.12.1修订程序

CPS 由智慧 CA 安全策略委员会根据情况进行审查，任何时候智慧 CA 安全策略委员会认为有必要时即组织修订。修订后的版本经智慧 CA 安全策略委员会审批后发布到智慧 CA 网站，并报送工信部备案。

9.12.2通知机制和期限

修改后的 CPS 经批准后将立即在智慧 CA 网站更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，智慧 CA 将在合理的时间内通知有关各方，合理的时间保证有关方面受到的影响最小。

智慧 CA 保留随时对 CPS 进行修订的权利，进行下列（但不限于）不重要的修订后将不作通知：如对印刷错误的更正、 URL 的改变和联系人信息的变更等。

9.12.3必须修改业务规则的情形

当管辖法律、适用标准、操作规范、认证系统有重大改变或现有 CPS 有重要缺陷时，必须修改 CPS 。由智慧 CA 安全策略委员会根据公司业务情况提出，智慧 CA 安全策略委员会审批。

9.13 争议处理

如果各参与方之间无法协商解决出现的问题和争端，可通过法律途径解决。

9.14 管辖法律

本规则在各方面服从《中华人民共和国电子签名法》、《电子认证服务管理办法》等中华人民共和国法律、规则、规章、法令和政令的约束和解释。智慧 CA 的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

9.15 与适用法律的符合性

本 CPS 的使用也必须遵从使用地的相关法律和法规。

9.16 一般条款

9.16.1完整协议

CP、CPS、订户协议及依赖方协议及其补充协议将构成智慧 CA 信任域参与者间的完整协议。

9.16.2转让

智慧 CA、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3分割性

法律允许的范围内，在智慧 CA 订户协议、依赖方协议和其他订户协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力。

9.16.4强制执行力

在智慧 CA、注册机构、订户和依赖方之间出现纠纷、诉讼时，胜诉方可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿，不

意味着免除对其他合同违约的赔偿。

9.16.5不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成智慧 CA、注册机构无法提供正常的服务时，智慧 CA、注册机构不承担由此给客户造成的损失。

9.17 其他条款

智慧 CA 对本 CPS 具有最终解释权。