

# **HUNCA CPS**

# **电子认证业务规则**

版本 V5.0

生效日期：2026 年 11月 1 日

**HUNCA CPS**  
**Certification Practice Statement**

**Version 5.0**  
**Effective Date: Nov 1 2026**

湖南省数字认证服务中心有限公司

**Copyright©2026**

**HUNAN Certification Authorit**

## 湖南 CA 电子认证业务规则 湖南省数字认证服务中心有限公司版权所有

### 版权声明

湖南省数字认证服务中心有限公司拥有本规则的完全版权。

其他任何个人和团体可准确完整地转载、粘贴或发布本规则。

任何个人和团体不得部分的转载、粘贴或发布本规则，更不得更改本规则的部分词汇进行转贴。

本规则的最新版本请参见本公司网页[www.hunca.com.cn](http://www.hunca.com.cn), 或者联系湖南省数字认证服务中心有限公司。

地址： 湖南省长沙市岳麓区潇湘南路一段368号中盈广场C座13楼

邮编： 410006

电话： 0731-88590261

电子邮件： [service@hunca.com.cn](mailto:service@hunca.com.cn)

本规则如有改动，对特定对象不再另行通知。

#### 注意：

《湖南 CA 电子认证业务规则》服从于中国的法律法规，包括且不限于：《中华人民共和国刑法》、《中华人民共和国人大常委会颁发的关于互联网安全防护措施的决定》、《中华人民共和国计算机安全管理条例》、《中华人民共和国商用密码管理条例》、《电子认证服务密码管理办法》、《中华人民共和国电子签名法》、《电子认证服务管理办法》。

对任何已经或即将涉嫌犯罪而影响湖南 CA 证书服务的组织、单位和个人，湖南 CA 将保留依法追诉的权利。

## 目 录

|                       |    |
|-----------------------|----|
| 1. 概括性描述 .....        | 1  |
| 1.1 承诺 .....          | 1  |
| 1.2 基本信息 .....        | 1  |
| 1.2.1 概要介绍 .....      | 1  |
| 1.2.2 证书层级架构 .....    | 2  |
| 1.3 文档名称与标识 .....     | 3  |
| 1.4 电子认证活动参与者 .....   | 4  |
| 1.4.1 电子认证服务机构 .....  | 4  |
| 1.4.2 注册机构 .....      | 4  |
| 1.4.3 订户 .....        | 4  |
| 1.4.4 依赖方 .....       | 5  |
| 1.4.5 其他参与者 .....     | 5  |
| 1.5 证书应用 .....        | 5  |
| 1.5.1 证书应用分类 .....    | 5  |
| 1.5.2 证书应用限制 .....    | 6  |
| 1.6 策略管理 .....        | 7  |
| 1.6.1 策略管理机构 .....    | 7  |
| 1.6.2 联系人 .....       | 7  |
| 1.6.3 策略文档的批准程序 ..... | 7  |
| 1.7 定义和缩写 .....       | 8  |
| 1.7.1 术语和定义 .....     | 8  |
| 1.7.2 缩略语 .....       | 11 |
| 2. 信息发布与信息管理 .....    | 12 |

|                          |    |
|--------------------------|----|
| 2.1 网站发布的内容 .....        | 12 |
| 2.2 信息更新 .....           | 13 |
| 2.3 监管备案 .....           | 13 |
| 2.4 证书信息对接 .....         | 13 |
| 2.5 信息库访问控制 .....        | 13 |
| 3. 身份标识与查验 .....         | 13 |
| 3.1 电子签名证书身份查验通用要求 ..... | 13 |
| 3.1.1 通用要求 .....         | 13 |
| 3.1.2 订户告知 .....         | 14 |
| 3.2 电子签名证书初始身份确认 .....   | 15 |
| 3.2.1 证明拥有私钥的方法 .....    | 15 |
| 3.2.2 个人身份的查验 .....      | 15 |
| 3.2.3 机构身份的查验 .....      | 17 |
| 3.3 订户意愿记录 .....         | 18 |
| 3.3.1 订户意愿记录内容 .....     | 18 |
| 3.3.2 个人高等级证书的意愿记录 ..... | 19 |
| 3.3.3 个人基础级证书的意愿记录 ..... | 19 |
| 3.3.4 机构高等级证书的意愿记录 ..... | 19 |
| 3.3.5 机构基础级证书的意愿记录 ..... | 20 |
| 3.4 订户协议 .....           | 20 |
| 3.5 未验证的订户信息 .....       | 20 |
| 3.6 互操作要求 .....          | 20 |
| 3.7 命名 .....             | 20 |
| 3.7.1 名称类型 .....         | 20 |

|                          |    |
|--------------------------|----|
| 3.7.2 对名称意义化的要求 .....    | 23 |
| 3.7.3 订户的匿名或伪名 .....     | 23 |
| 3.7.4 理解不同名称的形式的规则 ..... | 23 |
| 3.7.5 名称的唯一性 .....       | 23 |
| 3.7.6 商标的识别、鉴别与角色 .....  | 23 |
| 4. 证书生存周期操作要求 .....      | 23 |
| 4.1 通用要求 .....           | 24 |
| 4.2 证书申请 .....           | 24 |
| 4.2.1 证书申请实体 .....       | 24 |
| 4.2.2 处理流程与责任 .....      | 24 |
| 4.2.3 申请批准与拒绝 .....      | 25 |
| 4.2.4 处理申请时限 .....       | 25 |
| 4.3 证书签发 .....           | 25 |
| 4.3.1 签发过程 .....         | 25 |
| 4.3.2 结果通告 .....         | 25 |
| 4.4 证书接受 .....           | 26 |
| 4.4.1 证书的交付 .....        | 26 |
| 4.4.2 证书的接受 .....        | 27 |
| 4.4.3 证书接受记录的保存 .....    | 28 |
| 4.4.4 CA 对证书的发布 .....    | 29 |
| 4.4.5 CA 对其他实体的通告 .....  | 29 |
| 4.5 密钥对和证书的使用 .....      | 29 |
| 4.5.1 交付前的安全保护 .....     | 29 |
| 4.5.2 私钥管理服务要求 .....     | 29 |

|                             |    |
|-----------------------------|----|
| 4.5.3 安全事件反馈 .....          | 30 |
| 4.6 证书续期 .....              | 30 |
| 4.6.1 证书续期的情形 .....         | 31 |
| 4.6.2 申请实体 .....            | 31 |
| 4.6.3 处理续期请求时的身份查验方式 .....  | 31 |
| 4.6.4 证书签发与接受 .....         | 31 |
| 4.7 证书密钥更新 .....            | 31 |
| 4.7.1 证书密钥更新的情形 .....       | 31 |
| 4.7.2 申请实体 .....            | 31 |
| 4.7.3 处理密钥更新请求的身份确认方式 ..... | 32 |
| 4.7.4 证书签发与接受 .....         | 32 |
| 4.8 证书变更 .....              | 32 |
| 4.8.1 证书变更的情形 .....         | 32 |
| 4.8.2 申请实体 .....            | 32 |
| 4.8.3 处理证书变更请求的身份确认方式 ..... | 32 |
| 4.8.4 证书签发与接受 .....         | 32 |
| 4.9 证书撤销或冻结 .....           | 32 |
| 4.9.1 审批流程 .....            | 33 |
| 4.9.2 可请求撤销证书的实体 .....      | 33 |
| 4.9.3 证书撤销的情形 .....         | 33 |
| 4.9.4 证书撤销的处理时限 .....       | 34 |
| 4.9.5 CRL 的发布频率 .....       | 34 |
| 4.9.6 撤销信息的发布形式 .....       | 35 |
| 4.9.7 密钥损害的特别要求 .....       | 35 |

|                               |    |
|-------------------------------|----|
| 4.9.8 证书冻结 .....              | 35 |
| 4.10 证书状态信息服务 .....           | 35 |
| 4.10.1 证书状态信息服务方式 .....       | 35 |
| 4.10.2 证书状态信息服务响应时间 .....     | 35 |
| 4.10.3 查询服务连续性与可用性保障 .....    | 36 |
| 4.10.4 提供备用查询机制 .....         | 36 |
| 4.11 停止使用认证服务 .....           | 36 |
| 4.11.1 停止订户服务的情形 .....        | 36 |
| 4.11.2 处理停止服务请求的时限和方式 .....   | 36 |
| 4.11.3 停止服务后可能涉及的责任延续条款 ..... | 37 |
| 4.11.4 完整记录操作过程 .....         | 37 |
| 4.12 密钥托管与恢复 .....            | 37 |
| 4.12.1 密钥托管 .....             | 37 |
| 4.12.2 密钥生成、备份与恢复 .....       | 37 |
| 5. 认证机构设施、管理和操作控制 .....       | 38 |
| 5.1 物理控制 .....                | 38 |
| 5.1.1 基础设施 .....              | 38 |
| 5.1.2 分区管理与访问控制 .....         | 39 |
| 5.1.3 电力保障 .....              | 40 |
| 5.1.4 门禁与监控 .....             | 41 |
| 5.1.5 灾备 .....                | 42 |
| 5.1.6 环境保障措施 .....            | 43 |
| 5.1.7 消防措施 .....              | 43 |
| 5.1.8 设备管理 .....              | 44 |

|                           |    |
|---------------------------|----|
| 5.1.9 存储媒体管理 .....        | 45 |
| 5.2 操作过程控制 .....          | 46 |
| 5.2.1 可信角色 .....          | 46 |
| 5.2.2 职责分离 .....          | 47 |
| 5.3 人员控制 .....            | 48 |
| 5.3.1 可信人员资格要求 .....      | 48 |
| 5.3.2 可信人员培训要求 .....      | 48 |
| 5.3.3 工作轮换的周期和顺序 .....    | 49 |
| 5.3.4 未授权行为的处罚 .....      | 49 |
| 5.3.5 提供给员工的文档 .....      | 49 |
| 5.4 审计日志程序 .....          | 49 |
| 5.4.1 审计日志的记录范围 .....     | 49 |
| 5.4.2 审计日志的记录内容 .....     | 50 |
| 5.4.3 审计日志的保存期限 .....     | 50 |
| 5.4.4 日志审计内容 .....        | 50 |
| 5.4.5 审计周期 .....          | 50 |
| 5.5 记录归档 .....            | 50 |
| 5.5.1 归档范围 .....          | 51 |
| 5.5.2 保存期限 .....          | 51 |
| 5.5.3 保护措施 .....          | 52 |
| 5.5.4 管理机构 .....          | 52 |
| 5.6 电子认证服务机构根证书密钥更替 ..... | 53 |
| 5.6.1 密钥更替程序 .....        | 53 |
| 5.6.2 密钥更替的时间 .....       | 53 |

|                              |    |
|------------------------------|----|
| 5.7 损害和灾难恢复 .....            | 53 |
| 5.7.1 灾难恢复目标 .....           | 53 |
| 5.7.2 恢复流程及应急预案 .....        | 54 |
| 5.7.3 根私钥应急处理 .....          | 54 |
| 5.7.4 事件报告 .....             | 54 |
| 5.7.5 定期验证 .....             | 54 |
| 5.8 电子认证服务机构终止 .....         | 55 |
| 5.9 重大事项报告 .....             | 55 |
| 5.9.1 重大事项范围 .....           | 56 |
| 5.9.2 重大事项报告程序 .....         | 57 |
| 5.9.3 重大事项报告时限 .....         | 57 |
| 5.9.4 重大事项报告内容 .....         | 57 |
| 6. 认证系统技术安全控制 .....          | 57 |
| 6.1 技术安全管理制度要求 .....         | 57 |
| 6.2 密钥对的生成和安装 .....          | 58 |
| 6.2.1 根证书密钥对的生成和安装 .....     | 58 |
| 6.2.2 订户密钥对的生成和交付 .....      | 58 |
| 6.3 私钥保护和密码模块工程控制 .....      | 58 |
| 6.3.1 CA 私钥保护和密码模块工程控制 ..... | 58 |
| 6.3.2 订户私钥保护和密码模块工程控制 .....  | 59 |
| 6.4 密钥对管理的其他方面 .....         | 59 |
| 6.4.1 公钥归档 .....             | 59 |
| 6.4.2 证书操作期和密钥对使用期限 .....    | 60 |
| 6.5 激活数据 .....               | 60 |

|                            |    |
|----------------------------|----|
| 6.5.1 激活数据的产生和安装 .....     | 60 |
| 6.5.2 激活数据的保护 .....        | 60 |
| 6.5.3 激活数据的其他方面 .....      | 61 |
| 6.6 计算机安全控制 .....          | 61 |
| 6.6.1 系统补丁检查与评审 .....      | 61 |
| 6.6.2 无官方支持系统更替与管控 .....   | 61 |
| 6.6.3 杀毒软件安装 .....         | 62 |
| 6.6.4 病毒库更新 .....          | 62 |
| 6.6.5 病毒扫描周期与策略 .....      | 62 |
| 6.7 生存周期安全控制 .....         | 62 |
| 6.7.1 证书认证中心运行管理安全控制 ..... | 62 |
| 6.7.2 密钥管理中心运行管理安全控制 ..... | 62 |
| 6.7.3 证书操作流程安全控制 .....     | 63 |
| 6.8 网络安全控制 .....           | 63 |
| 6.8.1 网络结构设计 .....         | 63 |
| 6.8.2 安全防护 .....           | 63 |
| 6.8.3 网络拓扑图维护 .....        | 63 |
| 6.8.4 网络访问控制 .....         | 64 |
| 6.8.5 网络监控 .....           | 64 |
| 6.9 时间戳 .....              | 64 |
| 6.9.1 使用范围 .....           | 64 |
| 6.9.2 使用方式 .....           | 64 |
| 6.9.3 保障机制 .....           | 64 |
| 6.9.4 相关技术标准 .....         | 65 |

|                             |    |
|-----------------------------|----|
| 7. 证书、证书撤销列表和在线证书状态协议 ..... | 65 |
| 7.1 证书 .....                | 65 |
| 7.1.1 版本号 .....             | 65 |
| 7.1.2 证书标准项 .....           | 65 |
| 7.2 证书撤销列表 .....            | 65 |
| 7.3 在线证书状态协议 .....          | 66 |
| 8. 认证机构审计及相关评估 .....        | 66 |
| 8.1 审计评估制度 .....            | 66 |
| 8.1.1 审计评估的类型 .....         | 66 |
| 8.1.2 审计评估的频率 .....         | 66 |
| 8.1.3 评估者的资质 .....          | 66 |
| 8.1.4 审计评估的主题 .....         | 67 |
| 8.2 认证业务审计 .....            | 67 |
| 8.2.1 审计周期 .....            | 67 |
| 8.2.2 审计内容 .....            | 67 |
| 8.2.3 审计方式 .....            | 68 |
| 8.2.4 对问题与不足采取的措施 .....     | 68 |
| 8.3 全面符合性评估 .....           | 68 |
| 8.3.1 评估周期 .....            | 68 |
| 8.3.2 评估内容 .....            | 68 |
| 8.3.3 审计方式 .....            | 68 |
| 8.3.4 对问题与不足采取的措施 .....     | 68 |
| 8.3.5 评估结果的报送与发布 .....      | 68 |
| 9. 法律责任和其他业务条款 .....        | 69 |

|                          |    |
|--------------------------|----|
| 9.1 费用 .....             | 69 |
| 9.1.1 证书颁发或更新费用 .....    | 69 |
| 9.1.2 证书访问费用 .....       | 69 |
| 9.1.3 撤销证书的费用 .....      | 69 |
| 9.1.4 状态信息访问费用 .....     | 69 |
| 9.1.5 电子签名的费用 .....      | 69 |
| 9.1.6 签名验证的费用 .....      | 69 |
| 9.1.7 签名验证报告的费用 .....    | 69 |
| 9.1.8 其他服务的费用 .....      | 70 |
| 9.1.9 收费标准的公布方式 .....    | 70 |
| 9.1.10 退款策略 .....        | 70 |
| 9.1.11 通用退款办理要求与流程 ..... | 70 |
| 9.2 财务责任 .....           | 70 |
| 9.3 业务信息保密 .....         | 70 |
| 9.3.1 保密信息范围 .....       | 71 |
| 9.3.2 不属于保密的信息 .....     | 71 |
| 9.3.3 保护保密信息的信息 .....    | 72 |
| 9.4 个人隐私保护 .....         | 72 |
| 9.4.1 隐私保密方案 .....       | 72 |
| 9.4.2 作为隐私处理的信息 .....    | 73 |
| 9.4.3 不被视为隐私的信息 .....    | 73 |
| 9.4.4 用户个人信息的收集 .....    | 73 |
| 9.4.5 个人信息的存储 .....      | 73 |
| 9.4.6 用户个人信息的使用 .....    | 73 |

|                            |    |
|----------------------------|----|
| 9.4.7 用户个人信息的共享 .....      | 74 |
| 9.4.8 CA 对于用户个人信息的管理 ..... | 74 |
| 9.4.9 个人信息的查阅 .....        | 74 |
| 9.4.10 个人信息的删除和更改 .....    | 74 |
| 9.5 知识产权 .....             | 75 |
| 9.6 陈述和担保 .....            | 75 |
| 9.6.1 电子认证服务机构的陈述与担保 ..... | 75 |
| 9.6.2 注册机构的陈述与担保 .....     | 76 |
| 9.6.3 订户的陈述与担保 .....       | 76 |
| 9.6.4 依赖方的陈述与担保 .....      | 77 |
| 9.6.5 其他参与者的陈述与担保 .....    | 77 |
| 9.7 担保免责 .....             | 77 |
| 9.8 偿付责任规则 .....           | 78 |
| 9.8.1 偿付责任范围 .....         | 78 |
| 9.8.2 赔付计算方式 .....         | 79 |
| 9.8.3 有限责任 .....           | 79 |
| 9.9 赔偿 .....               | 80 |
| 9.10 有效期和终止 .....          | 80 |
| 9.10.1 有效期限 .....          | 80 |
| 9.10.2 终止 .....            | 80 |
| 9.10.3 效力的终止与保留 .....      | 81 |
| 9.11 对参与者的个别通告与沟通 .....    | 81 |
| 9.12 修订和发布 .....           | 81 |
| 9.12.1 修订程序 .....          | 81 |

|                          |    |
|--------------------------|----|
| 9.12.2 通告机制和期限 .....     | 82 |
| 9.12.3 必须修改业务规则的情形 ..... | 82 |
| 9.13 争议处理与举证 .....       | 82 |
| 9.14 管辖法律 .....          | 83 |
| 9.15 与适用法律的符合性 .....     | 83 |
| 9.16 一般条款 .....          | 83 |
| 9.16.1 完整规定 .....        | 83 |
| 9.16.2 分割性 .....         | 83 |
| 9.16.3 强制执行 .....        | 83 |
| 9.16.4 不可抗力 .....        | 83 |
| 9.17 其他条款 .....          | 84 |

## 1. 概括性描述

### 1.1 承诺

湖南省数字认证服务中心有限公司 (Hunan Certification Authority Service Center Co., Ltd, 简称湖南 CA ) 于 2008 年开始运营, 是权威、公正的电子认证服务机构。其宗旨是保证通过互联网络提供服务和享受服务的客户实现安全交易, 为互联网络的客户提供网上身份认证和信任服务。作为依据《中华人民共和国电子签名法》设立的第三方电子认证服务机构, 在此郑重承诺:

a. 开展电子认证经营与服务活动时, 严格遵守《中华人民共和国电子签名法》《电子认证服务管理办法》等法律、行政法规, 树立以人民为中心的服务理念, 承担社会责任;

b. 与客户建立业务关系前, 开展应用业务调研, 建立应用接入业务风险评估及内部定责机制, 严禁为存在违法违规风险的业务提供电子认证服务;

c. 当前用于提供电子认证服务的电子认证服务系统在 2020 年通过国家密码管理局安全性审查, 并取得《电子认证服务使用密码许可证》, 许可证有效期至 2030 年 2 月 28 日;

d. 接受政府和社会监督, 对主管部门检查发现的问题及时整改, 建立问题纠治长效机制, 持续符合整改要求。

### 1.2 基本信息

#### 1.2.1 概要介绍

| 项目   | 内容                                                                       |
|------|--------------------------------------------------------------------------|
| 机构名称 | 湖南省数字认证服务中心有限公司 (Hunan Certification Authority Service Center Co., Ltd.) |
| 简称   | 湖南 CA (HUNCA)                                                            |

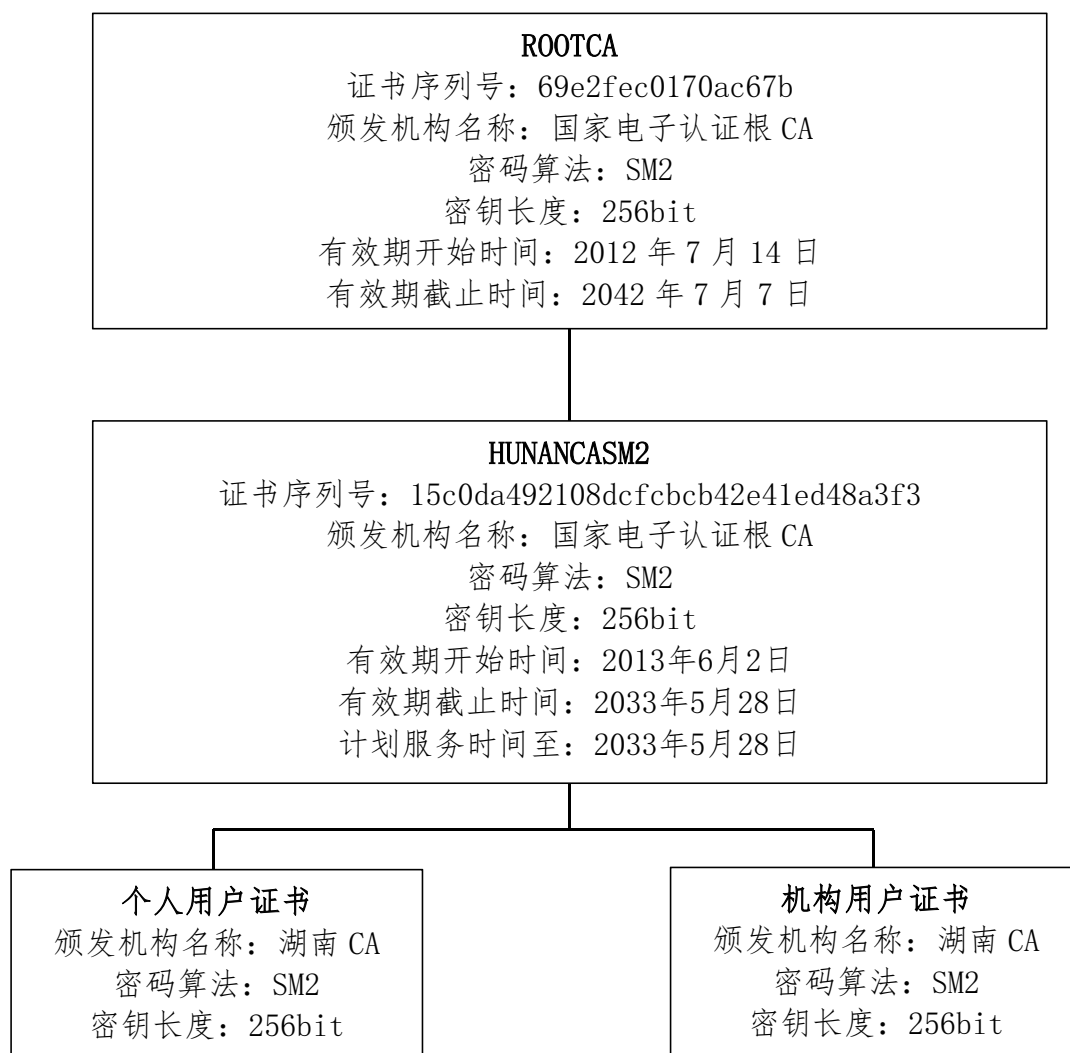
|           |                                    |
|-----------|------------------------------------|
| 成立时间      | 2008 年 4 月                         |
| 法定代表人     | 周湘能                                |
| 机构住所      | 湖南省长沙市岳麓区潇湘南路一段 368 号中盈广场 C 座 13 楼 |
| 经营场所      | 同上                                 |
| 联系电话      | 0731-88590261                      |
| 电子邮件      | cps@hunca.com.cn                   |
| 公司网站      | www.hunca.com.cn                   |
| 邮编        | 410006                             |
| 电子认证服务许可证 | 已取得                                |
| 证书编号      | ECP43010424030                     |
| 发证机关      | 中华人民共和国工业和信息化部                     |
| 首次批准日期    | 2009 年 1 月 23 日                    |
| 有效期       | 2024 年 1 月 23 日至 2029 年 1 月 22 日   |

| 项目            | 内容                              |
|---------------|---------------------------------|
| 电子认证服务密码使用许可证 | 已取得                             |
| 证书编号          | 0030                            |
| 发证机关          | 国家密码管理局                         |
| 首次批准日期        | 2008 年 5 月 14 日                 |
| 有效期           | 2025 年 3 月 1 日至 2030 年 2 月 28 日 |

### 1.2.2 证书层级架构

ROOTCA 证书是国家电子认证根 CA 证书，密码算法为 SM2，根密钥长度为

256bit，下设湖南 CA 机构根证书 HUNANCASM2，密钥长度为 256bit，HUNANCASM2 签发采用国密算法 SM2 的个人用户证书、机构用户证书。



### 1.3 文档名称与标识

本文档名称为《湖南 CA 电子认证业务规则(HUNCA CPS)》，是湖南 CA 对所提供的认证及相关业务的全面描述。

| 项目          | 内容                                         |
|-------------|--------------------------------------------|
| 版本号         | V5.0                                       |
| 发布日期        | 2026 年 7 月 19 日                            |
| 生效日期        | 2026 年 7 月 19 日                            |
| 遵循的证书策略 OID | 2.16.156.339.2.1.1.1、2.16.156.339.2.1.1.2、 |

|      |                                                              |
|------|--------------------------------------------------------------|
|      | 2.16.156.339.2.1.2.1、2.16.156.339.2.1.2.2、<br>1.2.156.115291 |
| 前序版本 | V4.5（生效日期：2025 年 4 月 8 日）                                    |
| 历史版本 | V3.0（生效日期：2013 年 9 月 4 日）                                    |
|      | V4.0（生效日期：2016 年 6 月 23 日）                                   |
|      | V4.1（生效日期：2018 年 9 月 28 日）                                   |
|      | V4.2（生效日期：2019 年 1 月 11 日）                                   |
|      | V4.3（生效日期：2019 年 2 月 18 日）                                   |
|      | V4.4（生效日期：2019 年 9 月 20 日）                                   |

## 1.4 电子认证活动参与者

### 1.4.1 电子认证服务机构

湖南 CA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。电子认证服务机构是受用户信任，负责创建和分配公钥的权威机构，是颁发数字证书的实体。湖南 CA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

### 1.4.2 注册机构

注册机构是受理数字证书的申请、更新、恢复和撤销申请的实体，同时也是标识和鉴别主体身份的实体。

RA 职责由湖南 CA 承担，订户可以直接向湖南 CA 提出证书申请。

### 1.4.3 订户

在电子签名应用中，订户即是电子签名人，是接收 CA 机构签发证书的实体。

湖南 CA 证书持有者可以包括个人、单位、企业、组织、机构、服务器、网站等提供网上服务和享受网上服务的各类实体，以及其他持有湖南 CA 证书的人、

物、对象或单位组织。

#### 1.4.4 依赖方

依赖方是指为某一应用而使用、信任本 CA 机构签发的证书，并验证证书和相应签名的实体。

#### 1.4.5 其他参与者

其他参与者指在湖南 CA 证书应用体系和服务体系中除上述的电子认证服务机构、注册机构、订户、证书依赖方之外的其他实体，包括但不限于身份核验服务机构、密码服务提供商、软硬件介质服务商、运维服务方、监管机构等。相关要求如下：

a. 身份核验合作机构：负责协助完成个人、机构实名核验，保证核验数据真实有效，严格遵守个人信息保护及数据安全规定；

b. 软硬件服务商：提供密码设备、加密介质、签名终端、安全服务器等软硬件产品，保障产品符合国家密码标准，无后门、无安全漏洞；

c. 运维服务方：协助 CA 机构完成系统运维、日志备份、安全加固，严格遵守保密协议，严禁泄露密钥、用户隐私及业务数据；

d. 行业监管机构：依法对本机构电子认证业务开展监督、检查、审计，CA 机构、订户及合作机构须配合监管核查。

### 1.5 证书应用

#### 1.5.1 证书应用分类

湖南 CA 所签发的证书主要有以下类别：

| 证书类型              | 主管部门 OID/<br>湖南 CAOID | 适用的应用场景                       |
|-------------------|-----------------------|-------------------------------|
| 个人高等级电子<br>签名认证证书 | 2.16.156.339.2.1.1.2  | 适用于高风险业务、符合《电子签名法》的个人电子签名认证证书 |

|                   |                      |                               |
|-------------------|----------------------|-------------------------------|
| 个人基础级电子<br>签名认证证书 | 2.16.156.339.2.1.1.1 | 适用于低风险业务、符合《电子签名法》的个人电子签名认证证书 |
| 机构高等级电子<br>签名认证证书 | 2.16.156.339.2.1.2.2 | 适用于高风险业务、符合《电子签名法》的机构电子签名认证证书 |
| 机构基础级电子<br>签名认证证书 | 2.16.156.339.2.1.2.1 | 适用于低风险业务、符合《电子签名法》的机构电子签名认证证书 |
| 设备证书              | 1.2.156.115291       | 不适用于电子签名，适用于低风险业务             |
| SSL 站点证书          | 1.2.156.115291       | 不适用于电子签名，适用于低风险业务             |
| 身份认证证书            | 1.2.156.115291       | 不适用于电子签名，适用于身份认证低风险业务         |

其中站点证书、身份认证证书及设备证书不属于电子签名证书，不适用于电子签名；湖南 CA 还签发其他用于电子政务场景安全认证证书，这些认证证书仅用于电子政务领域不适用于本 CPS。对于仅在电子政务安全认证场景中使用的证书，湖南 CA 发布了《湖南省数字认证服务中心有限公司电子政务电子认证服务业务规则》，可通过公司官网查阅、下载。

### 1.5.2 证书应用限制

湖南 CA 发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。禁止使用证书的场景如下：

- a. 涉及人身关系的，如婚姻、收养、继承等；
- b. 涉及停止公共事业服务的，如停止供水、供热、供气等；
- c. 法律、行政法规规定的其他不适用电子签名的应用场景或类型；
- d. 国家法律法规禁止的活动；
- e. 涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

## 1.6 策略管理

### 1.6.1 策略管理机构

湖南 CA 设立安全策略委员会，负责 CPS 以及配套制度的维护；安全策略委员会重大决议的相关文件和会议记录由专人妥善保存；成员名单通过湖南 CA 公司网站进行公示。

安全策略委员有以下工作职责：

- a. 确定维护 CPS 等策略文档的职能分工，建立合理有效的修订和批准流程；
- b. 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；
- c. 每年至少进行一次 CPS 全面评审，根据实际需要及时修订策略文档；
- d. 每年组织运营风险评估并形成报告。

### 1.6.2 联系人

| 项目 | 内容                                    |
|----|---------------------------------------|
| 电话 | 0731-88590261                         |
| 邮箱 | cps@hunca.com.cn                      |
| 地址 | 湖南省长沙市岳麓区潇湘南路一段 368 号中盈广场 C 座<br>13 楼 |
| 邮编 | 410006                                |

### 1.6.3 策略文档的批准程序

湖南 CA CPS 的批准程序包含以下环节：

- a. 起草小组的成立流程：由湖南 CA 安全策略委员会组织“CPS 起草小组”；
- b. 安全策略委员会的审批流程：“CPS 起草小组”起草拟定后，提交湖南 CA 安全策略委员会审核。如需进行变更，由“CPS 起草小组”提交变更报告并

进行修改，湖南 CA 安全策略委员会对提供的变动建议进行研究分析，形成最终决议；

c. 向主管机关的备案流程：CPS 经湖南 CA 安全策略委员会审批通过后，自发布之日起 30 日内向中华人民共和国工业和信息化部备案；

d. 发布流程：在湖南 CA 公司网站公布最新版本的 CPS 正式文档。

## 1.7 定义和缩写

### 1.7.1 术语和定义

| 术语     | 英文                         | 定义                            |
|--------|----------------------------|-------------------------------|
| 加密     | encipherment<br>encryption | 对数据进行密码变换以产生密文的过程。            |
| 密码模块   | cryptographic<br>module    | 实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。 |
| 密码算法   | cryptographic<br>algorithm | 描述密码处理过程的算法。                  |
| 密钥     | key                        | 控制密码变换操作的符号序列。                |
| 私钥     | private key                | 非对称密码算法中只能由拥有者使用的不公开密钥。       |
| 公钥     | public key                 | 非对称密码算法中可公开的密钥。               |
| RSA 算法 | RSA algorithm              | 一种基于大整数因子分解问题的公钥密码算法。         |
| SM2 算法 | SM2 algorithm              | 由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。 |
| SM3 算法 | SM3 algorithm              | 由 GB/T 32905 定义的一种密码杂凑算法。     |
| 公钥基础设施 | public key                 | 基于公钥密码技术，具有普适性，               |

|          |                                          |                                                                                 |
|----------|------------------------------------------|---------------------------------------------------------------------------------|
|          | infrastructure<br>(PKI)                  | 可用于提供机密性、完整性、真实性及抗抵赖性等安全服务的基础设施。                                                |
| 数字签名     | digital signature                        | 签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。 |
| 电子认证服务机构 | certification<br>service provider        | 取得电子认证服务许可证，为需要第三方认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体。                       |
| 数字证书     | digital certificate                      | 也称公钥证书，由认证机构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。                         |
| 电子签名认证证书 | electronic<br>signature<br>certificate   | 由依据《中华人民共和国电子签名法》设立电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。                       |
| 电子签名依赖方  | electronic<br>signature relying<br>party | 是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。                                                 |
| 订户       | subscriber                               | 被颁发给一张证书的证书主体。                                                                  |
| 对象标识符    | object identifier<br>(OID)               | 用于无歧义地标识对象的全局唯一值。                                                               |

|             |                                      |                                              |
|-------------|--------------------------------------|----------------------------------------------|
| 证书策略        | certificate policy<br>(CP)           | 指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。          |
| 证书策略对象标识符   | CP OID                               | 对某个证书策略进行唯一标识的OID                            |
| 证书链         | certificate chain                    | 证书链是一个用于证书验证的证书序列。                           |
| 身份查验        | entity authentication                | 证实某个实体就是所声称身份的过程。                            |
| 激活数据        | activation data                      | 用于使密码模块进入可操作状态的数据。可为口令、生物特征等。                |
| 时间戳         | time stamp (TS)                      | 对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。            |
| 证书续期        | certificate renewal                  | 指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。               |
| 密钥更新        | key re-key                           | 用新密钥替换旧密钥的过程。                                |
| 密钥恢复        | key recovery                         | 将归档或备份的密钥恢复到可用状态的过程。                         |
| 证书撤销列表      | certificate revocation list<br>(CRL) | 由电子认证服务机构签发并发布的被撤销证书的列表。                     |
| 证书认证系统      | CA system                            | 对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生命周期进行管理和服务的系统。 |
| 高等级电子签名认证证书 | enhanced electronic signature        | 适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。               |

|             |                                                     |                                                                                                               |
|-------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|             | certificate                                         |                                                                                                               |
| 基础级电子签名认证证书 | qualified<br>electronic<br>signature<br>certificate | 适用于除高等级证书规定场景外的其他电子签名场景的证书。                                                                                   |
| 通用介质证书      | —                                                   | 订户签名密钥对由订户持有的符合国家安全标准的密码模块（智能密码钥匙，俗称 USBKey 或 UKey，密码设备，密码模块）产生，并作为数字证书的载体，用于身份认证和电子签名的数字证书。                  |
| 云签协同证书      | —                                                   | 适用于证明订户在移动化和云服务的应用场景中所进行的远程身份认证与电子签名。采用双端（终端和云端）协同机制，终端（订户终端）和云端（云签平台）一同配合才能完成一次可靠的电子签名，通过安全授权认证保证私钥仅由订户持有或控制 |
| 云签平台        | —                                                   | 云签平台是指在云端或服务器端，与订户终端共同配合完成电子签名或数字证书应用的平台系统。面向订户或依赖方提供数字证书和电子签名服务。                                             |

### 1.7.2 缩略语

下列缩略语适用于本文件。

CA：电子认证服务机构（Certification Authority）

CPS: 电子认证业务规则 (Certification Practice Statement)

CP: 证书策略 (Certification Policy)

CRL: 证书撤销列表 (Certificate Revocation List)

DN: 甄别名称 (Distinguished Name)

LDAP: 轻量级目录访问协议 (Lightweight Directory Access Protocol)

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

OID: 对象标识符 (Object Identifier)

RT0: 恢复时间目标 (Recovery Time Objective)

RP0: 恢复点目标 (Recovery Point Objective)

## 2. 信息发布与信息管理的

湖南 CA 通过目录服务 (LDAP) 发布证书状态的相关信息, 订户可以通过访问湖南 CA 的目录服务器获取证书的信息。湖南 CA 同时提供在线证书状态查询 (OCSP) 和证书废除列表查询 (CRL) 服务。

湖南 CA 系统成功签发证书后, 将订户证书和 CRL 发布到目录服务器, 供订户在线查询证书。湖南 CA 证书订户可以通过 LDAP 查询、下载并验证订户证书, 同样也可以通过 OCSP 验证证书有效性。

湖南 CA 通过公司网站 (www.hunca.com.cn) 发布电子认证相关信息。

### 2.1 网站发布的内容

湖南 CA 在网站上发布以下内容:

- a. CPS 的所有版本 (包括历史版本和当前版本);
- b. 证书链 (根证书、中间证书等);
- c. 证书信息、状态信息等查询服务 (包括 CRL、OCSP、LDAP 查询入口);
- d. 详细的业务办理指南 (包括但不限于服务网点地址、营业时间、联系电话等);

e. 依赖方协议；

f. 投诉处理政策及投诉方式（包括投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称）。

## 2.2 信息更新

湖南 CA 信息发布内容如有变化，将在变化生效后 1 个工作日内更新。

## 2.3 监管备案

本 CPS 已按照国家电子认证服务管理平台的要求进行了备案。

## 2.4 证书信息对接

湖南 CA 完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询湖南 CA 已签发证书列表的功能。

## 2.5 信息库访问控制

对于湖南 CA 官网公布的信息，公众均可查询，没有限制。湖南 CA 通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能修改。只有经过审批的 RA/CA 管理员可以查询 CA 和 RA 数据库中的其他数据。

# 3. 身份标识与查验

## 3.1 电子签名证书身份查验通用要求

### 3.1.1 通用要求

湖南 CA 在受理证书申请时，对订户和/或受托人进行告知、身份确认、意愿记录和协议签署。

湖南 CA 的身份查验义务未委托给外部机构或个人（非属同一法人主体的机构视为外部机构），湖南 CA 依托自身的核验体系完成身份查验，而非仅形式上参与。

### 3.1.2 订户告知

#### 3.1.2.1 告知内容

受理证书申请时，湖南 CA 向订户完整告知以下事项：

a. 订户的权利义务：订户享有证书申请、续期、撤销等权利，同时承担如实提交材料、及时报备信息变更、妥善保管私钥、合规用证、私钥异常立即申请撤销或冻结等义务。

b. 服务收费项目和标准：收费标准以业务页面公示内容、双方协商约定内容为准。湖南 CA 有权变更收费标准并通过官方平台、业务系统、公示页面等合理方式进行告知。

c. 电子签名认证证书、电子签名的使用条件：订户应按照约定的合法用途使用证书及电子签名，不得将其用于法定禁止使用电子签名的场景。

d. 信息安全保障措施：湖南 CA 遵循合法必要原则处理订户信息；资料留存不少于证书失效后 5 年，并依法承担保密责任。

e. 湖南 CA 与订户责任划分

湖南 CA 责任：依法完成身份查验、保障证书内容在有效期内完整准确；因湖南 CA 过错造成订户直接损失的，按规则承担赔偿责任；因不可抗力、外部故障等非湖南 CA 原因导致的损失，不承担赔偿责任。

订户责任：保证申请资料及信息真实、完整、有效，信息变更的应在两个工作日内书面告知；因违规用证、提交虚假材料引发的全部损失由订户自行承担。

f. 订户签名私钥的存储方式及安全要求：

订户自行保管签名私钥的，订户负责妥善保管签名私钥、存储介质、相关密码口令等安全要素信息；因订户原因导致私钥泄露、损毁或丢失的，损失由订户自行承担；发现异常应立即告知湖南 CA 并进行处置。

订户委托湖南 CA 保管签名私钥的，湖南 CA 采用安全技术手段及必要措施存储私钥，未经授权湖南 CA 不得使用订户签名私钥。

g. 证书使用禁止条款：严禁将证书用于违法违规、违背公序良俗，或损害国家、公共及第三方合法权益的活动。

### 3.1.2.2 告知方式

湖南 CA 按照证书安全保障等级，采取差异化告知方式，所有告知操作均留存可追溯记录：

a. 高等级证书：采用面对面现场告知、电话语音告知、视频远程告知，或行业主管部门认可的其他合规方式完成告知，完整留存沟通记录、确认凭证。

b. 基础级证书：可选用高等级证书全部告知方式；也可采用业务页面强制阅读弹窗、短信告知、邮件书面告知等形式，同步留存用户已阅读、已确认的电子存证记录。

## 3.2 电子签名证书初始身份确认

### 3.2.1 证明拥有私钥的方法

证书订户向湖南 CA 申请证书时，可自主选择 § 1.5 规定的证书类型，湖南 CA 按照 § 6.2.2 规定的方式生成订户密钥对，通过数字签名的方式来确认证书订户拥有某个公钥对应的签名私钥。湖南 CA 在签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和证书请求数据的完整性，通过证书请求中所包含的数字签名来证明订户拥有某个公钥对应的私钥。

### 3.2.2 个人身份的查验

#### 3.2.2.1 个人身份信息有效性的确认

湖南 CA 在受理个人证书申请时，对个人身份信息的查验方式及内容如下：

a. 受理个人证书申请时，要求订户出示其有效身份证件或有效身份证件信息，有效证件类型仅限法律法规和国家有关文件规定的身份证件，包括：居民身份证、居住证、港澳台居民身份证、户口簿、护照、外国人永久居留证；

b. 通过证件机读工具、权威数据库（如公安人口库）或主管部门认可的其他方式查验订户身份证件的真实性和有效性；

c. 当订户委托他人代为办理时，查验订户本人签署的有效书面授权证明，要求受托人出示其有效身份证件或有效身份证件信息，并按照 b) 款方式查验订户和受托人的身份证件或身份资料。

订户提出证书申请时，需持个人有效身份证件，到湖南 CA 指定的办理地点提交书面数字证书申请表和上述有效身份证件的复印件等申请资料；湖南 CA 指定的办理地点对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

湖南 CA 保留根据最新国家政策法规的要求更新个人身份信息有效性确认的查验方式和内容的权利。更新后的个人身份信息有效性确认的查验方式和内容将发布在湖南 CA 的网站上：[www.hunca.com.cn](http://www.hunca.com.cn)

### 3.2.2.2 个人高等级证书的实人查验

湖南 CA 对个人高等级证书订户开展实人查验采用下列方式之一：

- a. 面对面查验；
- b. 远程人工面对面查验；
- c. 生物特征验证（如活体人脸、指纹、声纹、掌纹等生物识别技术的应用）；
- d. 通过主管部门认可的其他方式。

湖南 CA 以可追溯的方式完整记录并保存身份查验过程和结果，每张证书建立独立的身份验证记录。

### 3.2.2.3 个人基础级证书的实人查验

湖南 CA 对个人基础级证书订户开展实人查验采用下列方式之一：

- a. 通过 § 3.2.2.2 规定的方式；
- b. 电信运营商三要素：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；
- c. 银行卡四要素：核对姓名、证件号码、银行卡号、银行预留手机号在银行的一致性，并通过预留手机号的随机短信验证码核验；

- d. 由申请人持有的有效电子签名认证证书签名验证；
- e. 通过主管部门认可的其他方式（如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等）。

湖南 CA 完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

### 3.2.3 机构身份的查验

#### 3.2.3.1 机构身份信息有效性的确认

湖南 CA 在受理机构证书申请时，对机构身份信息的查验方式及内容如下：

- a. 查验机构有效证件方式，有效证件类型仅限法律法规和国家有关文件规定的证件；
- b. 法定代表人或受托人的身份查验方式：
  - i. 法定代表人或受托人身份证件信息查验方式参见 § 3.2.2.1；
  - ii. 受托人办理时，应查验机构加盖公章的有效书面授权证明。

订户提出证书申请时，需持统一社会信用代码证书或事业单位法人证书等有效证件，以及机构给经办人的授权文件和经办人身份证件，向湖南 CA 提出申请。

经办人经机构授权，并携带授权文件及本人身份证的原件和复印件，到湖南 CA 指定的办理地点提交书面数字证书申请表及机构证明文件等申请资料。

湖南 CA 指定的办理地点按照各等级机构证书实人查验要求对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝操作。

湖南 CA 保留根据最新国家政策法规的要求更新机构身份鉴别规范的权利。更新后的机构身份鉴别要求将发布在湖南 CA 的网站上：[www.hunca.com.cn](http://www.hunca.com.cn)

#### 3.2.3.2 机构高等级证书的实人查验

湖南 CA 对机构高等级证书订户开展实人查验采用下列方式之一：

a. 法定代表人实人查验，方法见 § 3.2.2.2;

b. 受托人实人查验，方法见 § 3.2.2.2，并通过机构对公账户随机金额打款验证或主管部门认可的其他方式。

湖南 CA 以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

说明：机构对公账户随机金额打款验证是指：

a. 湖南 CA 通过银行渠道向机构订户的对公账户进行小额随机金额的打款，机构订户通过网银/银行回单查询到该笔打款并准确回填金额，以证明机构订户对本次证书申请的真实意愿确认。

b. 机构订户通过其对公账户向湖南 CA 的银行账户进行小额随机金额的打款，机构订户通过该打款证明对本次证书申请的真实意愿确认。

同时湖南 CA 提供机构订户对公账户全额打款验证方式，机构订户通过银行渠道使用机构对公账户对湖南 CA 银行账户进行全额证书服务费用缴纳，通过该打款证明对本次证书申请的真实意愿确认。

### 3.2.3.3 机构基础级证书的实人查验

湖南 CA 对机构基础级证书订户开展实人查验采用下列方式之一：

a. 法定代表人实人查验，方法见 § 3.2.2.3;

b. 受托人实人查验，方法见 § 3.2.2.3;

c. 由订户持有的同等级或者更高级的有效机构证书签名验证。

湖南 CA 完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

## 3.3 订户意愿记录

### 3.3.1 订户意愿记录内容

湖南 CA 订户意愿记录内容包括：

a. 订户身份信息；

- b. CA 的信息；
- c. 签名私钥保存方及其保存义务；
- d. 订户对电子签名的法律责任；
- e. 订户对上述 a) 至 d) 项内容已充分知晓并同意的明确意愿表示。

### 3.3.2 个人高等级证书的意愿记录

湖南 CA 对个人高等级证书订户意愿的确认采用下列方式之一：

- a. 现场办理时，通过面对面确认或手抄提示语的方式，并采用录音录像或通过主管部门认可的其他方式记录订户意愿；
- b. 远程办理时，通过音视频或通过主管部门认可的其他方式确认并记录订户意愿。

在通过以上方式之一对个人高等级证书的意愿进行记录后，湖南 CA 保留完整、可追溯的订户意愿记录。

### 3.3.3 个人基础级证书的意愿记录

湖南 CA 对个人基础级证书订户意愿的确认采用下列方式之一：

- a. 与高等级证书相同的方式，方法见 § 3.3.2；
- b. 采用强制阅读、短信或邮件确认等电子方式。

在通过以上方式之一对个人基础级证书的意愿进行记录后，湖南 CA 保留完整、可追溯的订户意愿记录。

### 3.3.4 机构高等级证书的意愿记录

湖南 CA 对机构高等级证书订户意愿的确认采用下列方式之一：

- a. 法定代表人申请时，按照 § 3.3.2 的方式确认机构法定代表人的意愿；
- b. 受托人申请时，查验加盖机构公章的授权文件，并按照 § 3.3.2 的方式确认受托人的意愿。

湖南 CA 采用录音录像或通过主管部门认可的其他方式记录订户意愿，并保

留完整、可追溯的订户意愿记录。

### 3.3.5 机构基础级证书的意愿记录

湖南 CA 对机构基础级证书订户意愿的确认采用下列方式之一：

- a. 法定代表人申请时，按照 § 3.3.3 的方式确认机构法定代表人的意愿；
- b. 受托人申请时，查验加盖机构公章的授权文件，并按照 3.3.3 的方式确认受托人的意愿。

在通过以上方式之一对机构基础级证书的意愿进行记录后，湖南 CA 保留完整、可追溯的订户意愿记录。

## 3.4 订户协议

湖南 CA 订户协议包含 § 3.1.2.1 中规定的全部告知内容（共 7 项）。订户协议的具体条款内容详见湖南 CA 与订户签订的《数字证书服务协议》。

## 3.5 未验证的订户信息

湖南 CA 明确：

- a. 证书载明信息的查验方法、查验流程按照 § 3.2 规定执行；
- b. 证书中不包含未经验证的订户信息。

## 3.6 互操作要求

湖南 CA 数字证书服务体系暂不涉及互操作。

## 3.7 命名

### 3.7.1 名称类型

湖南 CA 颁发的数字证书，含有颁发机构和证书订户主体甄别名，对证书申请者的身份和其它属性进行鉴别，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。湖南 CA 的证书符合 X.509 V3 标准，分配给证书持有者

实体的甄别名，采用 X.501 标准命名方式。证书主体 DN 项结构严格遵循 GB/T 16264.8 国家标准要求，编码规则见下表：

| 代码 | 说明                | 示例       |
|----|-------------------|----------|
| C  | 国家                | CN       |
| S  | 省份（可选）            | 湖南省      |
| L  | 城市（可选）            | 长沙市      |
| O  | 订户所在机构信息（可选）      | XX 公司    |
| OU | 订户所在机构部门信息（可选）    | XX 部门    |
| CN | 订户名称（个人姓名或机构法定名称） | 张三/XX 公司 |

湖南 CA 证书颁发机构的主体甄别名命名规则如下：

| 属性      | 值               |
|---------|-----------------|
| 通用名（CN） | HUNANCASM2      |
| 机构（OU）  | HUNCA           |
| 机构部门（O） | 湖南省数字认证服务中心有限公司 |
| 城市（L）   | 长沙市             |
| 省份（S）   | 湖南省             |
| 国家（C）   | CN              |

湖南 CA 个人类型证书的主体甄别名命名规则如下：

| 属性        | 值                                  |
|-----------|------------------------------------|
| 通用名 (CN)  | 个人姓名                               |
| 机构 (OU)   | 发证机构所在城市，由湖南 CA 定义，或不填             |
| 机构部门 (O)  | 证书所属项目信息，由湖南 CA 定义，不代表订户身份信息       |
| 城市 (L)    | 订户或证书主体所在城市，或不填                    |
| 省份 (S)    | 订户或证书主体所在省份，或不填                    |
| 国家 (C)    | CN，表示中国                            |
| 证件信息 (T)  | 个人有效证件编号或其散列值                      |
| 描述 (Desc) | 证书所属类型，个人证书，由湖南 CA 定义，描述该证书类型为个人证书 |

湖南 CA 机构类型证书的主体甄别名命名规则如下：

| 属性       | 值                            |
|----------|------------------------------|
| 通用名 (CN) | 机构名称                         |
| 机构 (OU)  | 发证机构所在城市，由湖南 CA 定义，或不填       |
| 机构部门 (O) | 证书所属项目信息，由湖南 CA 定义，不代表订户身份信息 |
| 城市 (L)   | 订户或证书主体所在城市，或不填              |

|           |                                        |
|-----------|----------------------------------------|
| 省份 (S)    | 订户或证书主体所在省份，或不填                        |
| 国家 (C)    | CN，表示中国                                |
| 证件信息 (T)  | 机构有效证件编号或其散列值                          |
| 描述 (Desc) | 证书所属类型，机构证书，由湖南 CA 定义，<br>描述该证书类型为机构证书 |

### 3.7.2 对名称意义化的要求

湖南 CA 使用 DN 项来标识证书主体及证书签发者实体，DN 项中的名称具有一定的代表性意义，可以与使用证书的最终实体的身份或特有的属性相关。证书主体名称标识本证书所提到的最终实体的特定名称。

### 3.7.3 订户的匿名或伪名

本 CPS 规定，湖南 CA 的订户在进行数字证书申请时不能使用匿名或伪名。

### 3.7.4 理解不同名称的形式的规则

湖南 CA 签发的数字证书符合 X.509 V3 标准，甄别名格式遵守 X.501 标准。甄别名的命名规则由湖南 CA 定义。

### 3.7.5 名称的唯一性

在湖南 CA 信任域内，不同订户的证书的主体甄别名不能相同，必须是唯一的。但对于同一订户，湖南 CA 可以用其唯一的主体甄别名为其签发多张证书。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。

### 3.7.6 商标的识别、鉴别与角色

湖南 CA 签发的证书的主体甄别名中不包含商标名。

## 4. 证书生存周期操作要求

## 4.1 通用要求

湖南 CA 在证书生存周期操作中各方责任如下：

- a. 湖南 CA 承担建立、运营和维护注册通道的责任；
- b. 湖南 CA 承担与订户签订电子认证服务协议的责任；
- c. 订户承担提供准确信息的责任；
- d. 湖南 CA 承担妥善记录并保存相关信息的责任。

## 4.2 证书申请

### 4.2.1 证书申请实体

证书申请实体包含个人、企业单位、事业单位、政府机构、社会团体等各类组织机构。任何合法的组织和个人以及有明确身份归属的其他网络主体均可申请证书，以保证网络作业的安全和可靠。

### 4.2.2 处理流程与责任

证书申请人按照本电子认证服务规则所规定的要求，填写证书申请表，并准备相关的身份证明材料。湖南 CA 依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

湖南 CA 证书申请处理流程：按照 § 3.1-3.4 章节规定，完成对订户的告知、身份确认、意愿记录、协议签署等动作，并依据既定准则批准或拒绝该申请。

湖南 CA 数字证书申请流程为：

- a. 证书申请应由证书申请人或相应的授权人提交，申请者可以从湖南 CA 的网站下载或到湖南 CA 指定的办理地点领取相应的证书申请表，按表格要求填写申请表；或通过湖南 CA 的在线服务系统提交申请信息；
- b. 按照 § 3.1-3.4 章节身份查验要求提交对应的证书申请表格及相关身份证明材料，到湖南 CA 指定的办理地点进行注册、身份审核和缴费。

申请过程中各方责任为：订户要按照本电子认证服务规则 § 3.2 章节所述的要求准备证书申请材料，并确保申请材料真实准确。

根据《中华人民共和国电子签名法》的规定，证书申请者未向湖南 CA 提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、湖南 CA 造成损失的，订户应承担相应的法律及赔偿责任。

#### 4.2.3 申请批准与拒绝

湖南 CA 根据本《电子认证业务规则》所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定接受或拒绝证书申请。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，湖南 CA 将接受证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，湖南 CA 将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律禁止的除外)。被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

#### 4.2.4 处理申请时限

湖南 CA 收到了证书申请所有必须的相关资料，将在接受用户申请 2 个工作日内对证书申请者提交的信息进行鉴别和审核，并作出批准或者拒绝的决定。因特殊情况确需超期的，湖南 CA 将与订户协商确定处理时限。

### 4.3 证书签发

#### 4.3.1 签发过程

湖南 CA 在接受证书申请并验证申请信息予以审核通过之后，将签发证书。证书的签发表明电子认证服务机构最终完全正式地受理了证书申请。证书从订户接受证书那天起将被视为有效证书。

#### 4.3.2 结果通告

证书申请处理完毕后，湖南 CA 向订户通告处理结果的方式包括但不限于：

- a. 通过认证应用工具进行信息提示；
- b. 通过信函、站内信或电子邮件发送；

- c. 通过短信通知；
- d. 通过电话通知；
- e. 当面通知或通过实时视频等相当于面对面的方式通知；
- f. 通过主管部门认可的其他方式。

## 4.4 证书接受

### 4.4.1 证书的交付

湖南 CA 根据证书类型、安全等级与应用场景采用差异化交付方案，在线交付通道启用加密传输机制，确保证书交付过程的机密性、完整性与可追溯性。

#### 4.4.1.1 硬件证书交付

- a. 现场交付：订户或其受托人持有效身份证明文件，到湖南 CA 自有服务网点完成身份核验后，现场领取存储证书的介质（如智能密码钥匙等）；
- b. 物流交付：通过具备全程物流追踪能力的渠道，将硬件证书寄送至订户预留的收件地址，并要求收件人本人签收。

#### 4.4.1.2 非硬件证书交付

- a. 在线自助下载：订户通过身份二次核验后，登录湖南 CA 官方服务平台、指定认证服务工具在线下载证书文件，下载过程通过加密通道传输；
- b. 云端定向推送：湖南 CA 系统通过加密通道将证书推送至订户授权的云服务节点或设备终端，推送结果实时回执留痕；
- c. 加密邮件交付：将证书下载链接与安装指引通过加密邮件发送至订户预留的授权电子邮箱；
- d. 通过主管部门认可的其他方式交付。

## 4.4.2 证书的接受

### 4.4.2.1 构成接受证书的行为

符合以下任一情形的，视为订户有效接受证书：

#### a. 明示接受

- 1) 订户在湖南 CA 官方服务平台、指定认证服务工具中通过点击、勾选等操作主动完成接受证书的；
- 2) 现场领取硬件证书时，订户或受托人签署证书接受凭证；
- 3) 订户使用有效数字签名签署证书接受凭证并反馈至湖南 CA。

#### b. 默示接受

- 1) 订户首次使用证书完成电子签名、身份认证、数据加密等密码运算行为；
- 2) 订户成功下载/接收证书后，未在 2 个工作日内提出书面拒绝申请；
- 3) 通过物流渠道收取介质的，自渠道反馈本人签收状态之日起未在 2 个工作日内未提出书面异议。
- 4) 非硬件证书推送至指定终端后，订户未在 2 个工作日内提出书面异议。
- 5) 证书签发完成满 7 个自然日，订户未提交书面拒绝材料的，视作接受证书。

证书接受即代表订户确认证书所载信息无误，充分知晓并认可全部证书使用义务与法律责任。

### 4.4.2.2 拒绝接受证书的行为

#### a. 拒绝接受证书的适用情形

订户有正当理由的，可在异议期内申请拒绝接受证书，适用情形包括：

- 1) 证书所载信息与申请内容不符，存在信息录入错误、主体信息偏

差等问题；

- 2) 证书文件损坏无法正常安装使用，或通用介质证书硬件故障、无法正常识别；
- 3) 订户确认非本人/本机构提交证书申请，存在冒领、误发情形。

b. 拒绝接受证书的办理流程

- 1) 申请提交：订户需在证书交付后的 2 个工作日内，通过湖南 CA 官方服务渠道提交书面拒绝申请，说明拒绝理由并附上对应证明材料；
- 2) 核验处理：湖南 CA 收到申请后 2 个工作日内完成材料核验与事实核查。拒绝理由成立的，立即对该证书执行注销操作，同步告知订户后续方案（如免费重新签发或按协议退费）；拒绝理由不成立的，向订户出具书面说明并告知依据，证书维持正常状态；
- 3) 结果生效：订户逾期未提出异议的，视为默认接受证书；已生效的拒绝申请，订户无需承担该证书对应的使用责任。

#### 4.4.3 证书接受记录的保存

湖南 CA 对证书的交付、接受与拒绝全流程留存完整可追溯记录，以满足监管审计与司法举证要求。

##### 4.4.3.1 记录内容

- a. 证书标识信息：如证书序列号；
- b. 交付与接受信息：交付方式、交付时间、接受时间、操作人信息；
- c. 异常处理信息：如存在拒绝、异议流程，同步留存申请材料、核验结果、处理节点与最终结论。

##### 4.4.3.2 记录管理要求

- a. 电子记录存储方式：应采取安全技术手段保障记录不可篡改、可追溯；
- b. 记录保存期限：不少于证书有效期届满后 5 年，法律法规、行业规范

对保存期限有更长要求的，从其规定；

c. 记录查阅与调取：严格执行权限管控与审批流程，仅授权合规、审计与法务人员可按规定访问，保障订户信息安全与隐私。

#### 4.4.4 CA 对证书的发布

湖南 CA 提供基于 LDAP 协议的目录服务，湖南 CA 根据订户需求决定是否将其证书发布到目录系统或者数据库中。

#### 4.4.5 CA 对其他实体的通告

对于湖南 CA 签发的证书，湖南 CA 不通知其他实体。

### 4.5 密钥对和证书的使用

#### 4.5.1 交付前的安全保护

湖南 CA 在将密钥对交付订户保管之前，采取以下有效措施保障其安全性：

- a. 保障签名私钥生成和传输过程的安全；
- b. 审核订户密钥是否符合国家或行业相关安全标准要求，对不符合要求的拒绝颁发证书，包括：RSA 密钥长度小于 2048 位、使用 MD5、SHA-1 等不安全算法。

湖南 CA 订户的签名密钥对由其持有的密码设备（如智能密码钥匙、IC 卡等）产生，加密密钥由密钥管理中心（KMC）产生。

#### 4.5.2 私钥管理服务要求

湖南 CA 为订户提供签名私钥管理服务时，承诺遵守以下要求：

- a. 未经订户书面授权，不得保存或委托他人保存其签名私钥；
- b. 机构证书签名私钥的使用，应设置法定代表人或受托人作为授权主体；
- c. 仅在获得订户明确授权的情况下使用其签名私钥；
- d. 签名私钥应以加密形式存储，且存储条件符合安全标准；

e. 所有涉及签名私钥的操作应有完整、可追溯的记录。

订户使用湖南 CA 的证书时，承诺遵守以下要求：

a. 必须妥善保管和存储与证书相关的私钥，避免遗失、泄露、被篡改或者被盗用；

b. 任何人使用证书都必须检验证书的有效性，证书到期或吊销后，须停止使用该证书及对应的私钥；

c. 在使用与湖南 CA 所签发的证书有关的签名及经过签名的信息时，参与方按本 CPS 的规定享有相应的权利和应尽的义务。任何超出本 CPS 的规定的证书及私钥的使用，湖南 CA 将不承担由此带来的任何后果。

依赖方有义务妥善保管订户的公钥和证书，不将其用于不适合的证书用途，使用前有责任检查证书的真实性和有效性。验证证书的有效性包括三个方面：

a. 用湖南 CA 的证书验证证书中的签名，确认该证书是由湖南 CA 签发的，并且证书的内容没有被篡改；

b. 检验证书的有效期，确认该证书在有效期之内；

c. 查询证书状态，确认该证书没有被注销。

### 4.5.3 安全事件反馈

湖南 CA 建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。反馈渠道：

a. 电话：0731-88590261；

b. 电子邮件：cps@hunca.com.cn；

c. 现场：湖南省长沙市岳麓区潇湘南路一段 368 号中盈广场 C 座 13 楼。

### 4.6 证书续期

证书续期是指在不改变订户主体信息的情况下，在原证书到期前，为订户签发新证书。

#### 4.6.1 证书续期的情形

证书上都有明确的证书有效期，表明该证书的起始日期与截止日期，订户应当在证书有效期到期前，到湖南 CA 指定的办理地点申请对证书进行续期。

#### 4.6.2 申请实体

证书续期的申请人为订户或其受托人。

#### 4.6.3 处理续期请求时的身份查验方式

若自申请人上次完成身份查验之日起至本次续期申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认；否则，需按照 § 3.2 章节的规定重新进行身份查验。

#### 4.6.4 证书签发与接受

证书续期的签发与接受流程需符合 § 4.3 章节与 § 4.4 章节的规定。

### 4.7 证书密钥更新

证书密钥更新是指为订户生成新的密钥对并为其新公钥签发新证书。

#### 4.7.1 证书密钥更新的情形

- a. 当订户证书即将到期或已经到期时；
- b. 当订户证书密钥对已经被泄露、被窃取、被篡改或者其他原因导致的密钥对安全性无法得到保证；
- c. 当订户证实或怀疑其证书密钥不安全时；
- d. 其他可能导致密钥更新的情形。

#### 4.7.2 申请实体

证书密钥更新的申请人为订户或其受托人。

### 4.7.3 处理密钥更新请求的身份确认方式

若自申请人上次完成身份查验之日起至本次更新申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认；否则，需按照 § 3.2 章节的规定重新进行身份查验。

### 4.7.4 证书签发与接受

证书密钥更新的签发与接受流程需符合 § 4.3 章节与 § 4.4 章节的规定。

新证书签发后旧的证书将被注销。湖南 CA 将在 2 小时内在 LDAP 上发布订户的新证书。订户旧证书废止信息在 24 小时内通过 CRL 发布。

## 4.8 证书变更

证书变更是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（如订户名称改变等）。

### 4.8.1 证书变更的情形

证书订户的信息发生了变化，如订户名称改变等。

### 4.8.2 申请实体

证书变更的申请人为订户或其受托人。

### 4.8.3 处理证书变更请求的身份确认方式

按照 3.2 章节的规定查验，若发起方不是证书订户，CA 需取得订户同意。

### 4.8.4 证书签发与接受

证书变更的签发与接受流程需符合 § 4.3 章节与 § 4.4 章节的规定。

## 4.9 证书撤销或冻结

#### 4.9.1 审批流程

湖南 CA 制定证书撤销的审批流程如下：

- a. 申请：请求撤销证书的实体向湖南 CA 提出撤销申请，申请渠道可通过线上热线电话或线下注册中心提交。可请求撤销证书的实体包括且不限于订户、受托人、依赖方或 CA；
- b. 受理：湖南 CA 对申请人的身份与权限进行验证，根据验证结果做出是否受理决定；
- c. 审批：做出受理决定后，由第二人复核是否符合受理要求，执行双人审核制度，复核通过将记录影响证书或私钥安全的事件（如密钥遗失、泄露）；
- d. 执行：通过审批后立即执行证书撤销操作；
- e. 通知：通过电话、邮件、短信等方式通知订户，被吊销的订户证书将在 24 小时内通过 CRL 向外界公布。

湖南 CA 将保留处理证书撤销处理流程的相关信息。

#### 4.9.2 可请求撤销证书的实体

可请求撤销证书的实体包括：

- a. 订户本人；
- b. 持有效书面授权的受托人；
- c. 发现证书被滥用时的依赖方；
- d. 湖南 CA 发现违规或安全问题时主动撤销。

#### 4.9.3 证书撤销的情形

- a. 新的密钥对替代旧的密钥对；
- b. 密钥失密：与证书中的公钥相对应的私有密钥被泄密或订户怀疑自己的密钥失密；
- c. 从属关系改变：与密钥相关的订户的主题信息改变；
- d. 操作中止：由于证书不再需要用于原来的用途；

- e. 订户不能履行电子认证业务规则或其他协议、法律及法规所规定的责任和义务；
- f. 订户申请初始注册时，提供不真实材料；
- g. 证书已被盗用、冒用、伪造或者篡改；
- h. CA 失密：电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因；
- i. 利用数字证书在网上进行违法犯罪活动的；
- j. 其他情况：这些情况可以是因法律或政策的要求湖南 CA 采取的临时撤销措施，也可以是订户申请撤销证书时填写的其他原因。

#### 4.9.4 证书撤销的处理时限

订户一旦发现需要撤销证书，应及时向湖南 CA 提出撤销请求，撤销原因分两类：

- a. 私钥泄露等事件：撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出；
- b. 其他吊销原因：撤销请求必须在 48 小时内提出。

湖南 CA 在接到订户挂失、废除、注销等数字证书撤销申请时，应及时受理。在受理后 24 小时内保证数字证书撤销操作正式生效。在订户办理数字证书吊销相关手续前及湖南 CA 受理订户证书撤销相关申请时起到证书撤销生效时 24 小时内造成的损失，湖南 CA 不承担相关法律责任。

被撤销的订户证书在 24 小时内通过 CRL 向外界公布，订户可通过目录服务器指定的位置查询下载。

#### 4.9.5 CRL 的发布频率

湖南 CA 可采用实时或定期的方式发布 CRL，订户可以访问 CRL 验证证书当前状态。

发布 CRL 的频率根据证书策略确定，通常为 24 小时内定期发布，订户如有特殊要求的，可根据订户申请需求，适当更新 CRL 发布的频率，发布的最大滞后时间为 24 小时。

#### 4.9.6 撤销信息的发布形式

CRL 和 OCSP 作为吊销信息的主要发布形式，湖南 CA 每 24 小时签发一次 CRL。提供 7X24 小时 LDAP 目录查询服务，并提供 OCSP 作为可选的在线状态有偿查询方式。

#### 4.9.7 密钥损害的特别要求

无论是订户还是湖南 CA，在发现其密钥遭受安全威胁时，应及时撤销证书。

#### 4.9.8 证书冻结

湖南 CA 不提供证书冻结业务，订户可直接选择证书撤销业务。

### 4.10 证书状态信息服务

#### 4.10.1 证书状态信息服务方式

湖南 CA 通过多种渠道向依赖方提供证书状态查询与验证服务，以确保其能准确、及时地验证数字证书的有效性。

a. 在线证书状态协议（OCSP）服务：湖南 CA 通过 OCSP 服务为依赖方提供证书吊销状态的实时在线查询能力。OCSP 服务遵循 RFC 6960 规范。

b. 备用查询机制：当在线服务因不可抗力或系统维护等原因暂时不可用时，依赖方可拨打湖南 CA 官方客服热线或发送电子邮件，申请人工协助核实证书状态。

#### 4.10.2 证书状态信息服务响应时间

为保障依赖方能够及时获取准确的证书状态信息，湖南 CA 承诺遵守以下时间标准：

a. OCSP（在线证书状态协议）服务响应：湖南 CA 提供 7×24 小时不间断的 OCSP 在线查询服务。在系统正常运行状态下，对接收到的合法 OCSP 查询请求，湖南 CA 在毫秒级至秒级内完成数据库检索与响应生成，并向请求方返回经数字签名的响应结果，状态包括“正常”、“已撤销”或“未知”。

b. 备用查询机制响应时效：当在线自动化查询服务因不可抗力、系统维护或突发故障导致不可用时，湖南 CA 启动人工备用查询机制。依赖方通过官方客服热线或电子邮件提交证书状态核实请求后，湖南 CA 将及时完成核实并给予明确答复。

#### 4.10.3 查询服务连续性与可用性保障

为确保依赖方能够持续、稳定地获取证书状态信息，保障数字信任体系的平稳运行，湖南 CA 提供的 OCSP 在线查询及 CRL 分发服务均为 7×24 小时全年无休运行，承诺年度服务可用率不低于 99%。

#### 4.10.4 提供备用查询机制

当 OCSP 服务因不可抗力、网络攻击、硬件故障等突发原因不可用时，湖南 CA 即时启动备用查询机制：

- a. 人工辅助通道：依赖方可拨打 7×24 小时官方客服热线或发送电子邮件，申请人工核实证书状态；
- b. 公告通报渠道：发生大规模证书撤销或重大服务变更时，湖南 CA 通过官方网站公开渠道及时通报相关证书状态及处置进展。

### 4.11 停止使用认证服务

#### 4.11.1 停止订户服务的情形

- a. 订户主动申请停止服务，包括证书撤销；
- b. 订户违反服务协议或相关法律法规法规；
- c. 订户证书有效期满后，订户未续期订购结束；
- d. 订户主体消亡。

#### 4.11.2 处理停止服务请求的时限和方式

- a. 停止服务后应撤销证书、安全销毁订户签名私钥等按照 § 4.9 章节予以执行；

b. 用户数据的保存、销毁或转移政策按照隐私保护以及相关法律法规要求执行。

#### 4.11.3 停止服务后可能涉及的责任延续条款

订户申请停止使用认证服务之日起，应履行以下义务：

a. 立即停止使用该证书进行电子签名或身份认证，并通知已知依赖方该证书已失效；

b. 妥善保管证书私钥，不得泄露、转让或继续使用；

c. 对停止使用认证服务前使用该证书实施的电子签名行为承担法律责任，不得以证书失效为由否认有效签名；

d. 因订户未及时通知依赖方或继续使用已失效证书导致第三方损失的，由订户自行承担赔偿责任；

e. 配合认证机构完成必要的审计追溯，提供与证书使用相关的证明材料。

停止服务后湖南 CA 延续承担停止服务前已产生的认证相关责任，包括但不限于因服务过程中存在过错导致订户或第三方损失的赔偿责任、用户数据保密责任、证书撤销后的后续告知责任。

#### 4.11.4 完整记录操作过程

湖南 CA 完整记录并保存操作过程。

### 4.12 密钥托管与恢复

#### 4.12.1 密钥托管

湖南 CA 根证书私钥未托管给任何第三方机构或个人，在自身控制的安全环境中保管。

#### 4.12.2 密钥生成、备份与恢复

湖南 CA 建立了根证书密钥备份与恢复策略，对根证书密钥进行安全备份。

## 5. 认证机构设施、管理和操作控制

### 5.1 物理控制

湖南 CA 的物理场地满足以下安全要求并最有效地控制风险：防止物理非法进入 4 层物理结构及完善的安全管理体系保护湖南 CA 的运营设施和信息安全。防止未经授权的物理访问确保未经过授权的人或仅被授权访问有限物理区域的人员不得访问湖南 CA 受到限制的区域。维护 CA 服务的完整性、可用性。针对环境的安全威胁，采用了如 UPS 电源保障、数据线路、门禁系统、监控装置和屏蔽机房建设等措施保障提供 CA 服务的系统、设施不受到破坏，保证认证服务不被中断。

#### 5.1.1 基础设施

a. 地理位置：湖南 CA 主机房位于湖南省长沙市岳麓区，选址避开危险火源区、环境污染区、落雷区，以及强电磁干扰与强振动源（如电气化铁路、高压传输线、机场、火车站等），主体建筑具备抗震、抗洪涝及防风能力；

b. 物理建筑标准：机房室内净高不低于 3 米，地板承重大于  $150\text{kg}/\text{m}^2$ ，铺设防静电活动地板。机房内无易燃易爆物品，给排水管道及消防栓避开核心区，楼板孔洞采用非燃烧材料封堵；

c. 机房环境建设：机房按 GM/T 0034 标准建设，温度维持  $18\text{--}27^{\circ}\text{C}$ ，相对湿度  $40\%\text{--}60\%$ ，静电电压控制在  $1000\text{V}$  以内。配备七氟丙烷气体灭火系统、全覆盖视频监控与生物识别门禁，进出人员须签字刷卡并留存记录，每年至少进行一次屏蔽室检测。

d. 网络通信设施建设标准：核心网络设备（路由器、交换机等）均采用冗余配置，通信线路采取多路接入方式，防止单点故障，确保业务高可用性与数据传输安全。

湖南 CA 的建筑物和机房建设按照下列标准实施：

| 序号 | 标准号 | 标准名称 |
|----|-----|------|
|----|-----|------|

|    |               |                   |
|----|---------------|-------------------|
| 1  | GB 2887-89    | 《计算站场地技术条件》       |
| 2  | GB 50174-93   | 《电子计算机机房设计规范》     |
| 3  | SJ/T30003-93  | 《电子计算机机房施工验收规范》   |
| 4  | GB 50016-2006 | 《建筑设计防火规范》        |
| 5  | GB 50222-95   | 《建筑内部装修设计防火规范》    |
| 6  | GB 9361-88    | 《计算站场地安全要求》       |
| 7  | GB 6650-86    | 《计算机机房用活动地板技术条件》  |
| 8  | GB 50116-2008 | 《火灾自动报警系统设计规范》    |
| 9  | GB 50057-2010 | 《建筑物防雷设计规范》       |
| 10 | GB 5054-2011  | 《低压配电设计规范》        |
| 11 | GBJ19-2003    | 《采暖通风与空气调节设计规范》   |
| 12 | YD\T754-95    | 《通讯机房静电防护通则》      |
| 13 | GB 8702-88    | 《电磁辐射防护规则》        |
| 14 | GB 12190      | 《高性能屏蔽室屏蔽效能的测量方法》 |

### 5.1.2 分区管理与访问控制

为了保证湖南 CA 主机房的安全，采取了一定的隔离、控制、监控手段。机房的所有门都符合相关规定的安全性要求，能防止非法的进入，机房通过设置门禁和监控系统来实现机房物理安全。

### 5.1.2.1 技术设施内部的安全区域划分

湖南 CA 技术设施内部严格实行分层分区防护，划分为公共区、服务区、管理区和核心区四个安全区域，各区域具有明确的功能定位与安全防护要求：

a. 公共区：该区域与内部办公区实行物理隔离，仅允许经授权的接待人员与访客进入，严禁访客跨区域流动；

b. 服务区：主要部署面向外部提供域名解析、Web 服务器、从目录服务器及外部访问接口等系统。该区域通过防火墙等安全设备与管理区和核心区进行严格的逻辑隔离，防范外部网络攻击渗透；

c. 管理区：仅供 CA 内部工作人员及运维人员使用，部署注册审核系统（RA）、日常系统维护及运维管理终端。该区域实行严格的身份鉴别与访问控制，禁止非授权人员进入；

d. 核心区：作为 CA 系统的安全核心，部署核心应用、数据库、密钥管理系统（KMC）及核心密码设备等。该区域实行最高级别的安全防护，采用双人双因素访问控制，确保进入人员的合法性与安全性。

### 5.1.2.2 机房核心区和管理区的物理访问控制策略

针对机房核心区和管理区等敏感安全区域，湖南 CA 实施极为严格的物理访问控制策略：

a. 双人共管与双因素认证：进入核心区和管理区必须严格执行“双人共管”制度，即任何时间进入该区域必须有两名及以上授权可信人员同时在场。同时，强制实施“双因素认证”机制，访问人员需通过“生物识别（如指纹/人脸）+智能门禁卡”等多重身份验证方可通行，有效防止尾随进入及单人违规操作。

b. 访问信息记录与留存：所有进出核心区和管理区的人员均须签字与刷卡，并全程留存详细的物理访问记录。系统自动记录访问人员信息、进出时间及活动区域，非公共区的视频监控记录和门禁访问记录至少保存 6 个月以上。

### 5.1.3 电力保障

为确保湖南 CA 核心业务系统、密码设备等数据的持续稳定运行，防范因电

力中断导致的安全风险与业务停滞，湖南 CA 特制定并严格执行以下电力应急保障方式：

a. 多重冗余供电架构与应急电源配置：湖南 CA 机房采用双路市电引入及 UPS（不间断电源）冗余架构。在电网中断时，UPS 系统将实现零秒级无缝切换，保障核心设备持续供电，保障业务连续性。

b. 核心设备专属不间断供电保障：针对 CA 系统的核心应用服务器、密钥管理系统（KMC）及核心密码机等关键设备，配置专属的在线式 UPS，UPS 提供充足的后备时间，确保核心数据零丢失、密码运算不中断。

c. 应急状态下的业务降级与有序处置：若发生极端情况导致应急电力保障能力无法满足全量需求，机构将立即启动电力应急预案，实施业务降级策略。优先保障 CA 核心签发系统、数据库及机房基础环境（如精密空调、消防安防系统）的用电需求，暂停非关键区域的办公及测试用电，确保核心密码资产与业务的绝对安全。

d. 常态化运维巡检与实战演练：建立严格的电力保障设备运维机制，定期对 UPS 电池组、配电柜及切换开关进行巡检与预防性维护。同时，每年至少组织一次“市电中断”专项电力应急演练，确保应急保障体系随时处于可用状态。

#### 5.1.4 门禁与监控

为保障技术设施的安全，防止未授权访问与物理破坏，湖南 CA 在技术设施内部署了严密的综合安防系统，并对安防记录实行严格的全生命周期管理。

##### 5.1.4.1 机房安防系统部署

a. 门禁系统：在技术设施各安全区域部署生物识别与智能卡结合的门禁系统，实行严格的权限划分与访问控制；

b. 入侵检测系统：部署红外探测、震动传感器等入侵检测设备，对非公共区域的非法闯入行为进行实时监测与报警；

c. 视频监控系统：实现技术设施内无死角视频监控覆盖，对人员进出、设备操作等关键活动进行全天候实时录像与行为分析。

#### 5.1.4.2 安防记录保存期限

针对非公共区域（包括服务区、管理区、核心区），湖南 CA 严格执行安防记录的留存标准：

- a. 视频监控记录：非公共区域的视频监控录像保存时间不少于 6 个月；
- b. 门禁访问记录：非公共区域门禁系统访问记录（含人员信息、进出时间等）保存时间不少于 6 个月；
- c. 为确保安防数据的合规性与可追溯性，上述视频监控记录和门禁访问记录在达到保存期限、必须履行以下程序：
  - i. 专项安全审计：由独立于日常运维的安全审计人员或审计团队，对即将销毁的安防记录进行全面审查；
  - ii. 审计报告存档：审计完成后，必须形成正式的审计报告。该报告需详细记录审计时间、审计人员、审计范围及审计结论，并作为重要安全档案长期存档备查，确保安防记录销毁过程的合规性与安全性。

#### 5.1.5 灾备

为有效应对地震、火灾、洪涝等区域性灾难，保障核心密码资产与业务数据安全，湖南 CA 在距主机房 20 公里外的长沙市望城区设立异地备份中心。关键数据（包括系统配置、审计日志及证书数据库）通过专线加密同步至备份中心的 HSM 或加密存储设备，备份介质享有与主机房同等的物理安全保护，形成完整的异地灾备体系：

- a. 核心数据异地备份策略：针对 CA 系统的重要数据（包括但不限于核心业务数据、数据库文件、系统配置文件及密钥数据等），湖南 CA 严格执行异地备份机制，并通过安全专线或加密网络通道进行传输，确保数据在传输与存储过程中的机密性与完整性；
- b. 异地备份位置及距离声明：为确保在本地发生极端灾难时，备份数据不受波及且具备快速恢复能力，湖南 CA 异地灾备中心选址严格遵循地理隔离原则；
- c. 地理位置：异地灾备中心部署于与生产中心位于同城市的不同的区域，有效规避了区域性自然灾害的连带风险；

d. 安全距离：异地灾备中心与生产中心的直线物理距离大约 20 公里，满足国家相关标准对重要数据异地灾备的地理安全要求。

### 5.1.6 环境保障措施

为确保湖南 CA 核心密码设备与数据服务器的安全、稳定运行，防止因环境异常导致设备故障或数据损毁，湖南 CA 机房配备了专业、完善的环境保障系统，具体保障措施如下：

a. 温湿度精密控制：湖南 CA 机房内部署了精密空调系统和除湿机设备，对机房环境进行全天候精准调控。系统实时监测并自动调节机房环境，确保机房温度严格保持在 18℃-28℃ 范围内，相对湿度稳定维持在 40%至 60%之间；

b. 防水防潮安全防护：针对机房可能面临的水患风险，机房选址避开了用水设备的下层或隔壁，并对屋顶、墙壁进行了严格的防水处理。同时，在机房内（特别是精密空调区域）部署了漏水检测报警装置，一旦发生渗漏，系统将立即触发告警并短信通知到机房运维人员，确保设备免受水浸损害。

### 5.1.7 消防措施

为全面保障湖南 CA 机房核心设备与密码资产的安全，防范火灾风险，湖南 CA 在机房内配备了消防预警与灭火系统，并建立了严格的日常维保与人员防护机制：

a. 智能火灾自动报警系统：机房内部署了高灵敏度的火灾自动报警系统，该系统具备温度和烟雾双重检测功能。通过智能感烟探测器与感温探测器的组合联动，能够实现对机房内火灾隐患的极早期精准探测与实时预警，确保在火情发生初期即可触发声光报警并联动相关设备；

b. 自动灭火系统：机房核心区域配备了与火灾自动报警系统联动的依爱 JB-QB-EIN70 消防报警主机系统。当确认火情时，系统可在保障人员安全撤离的前提下，自动切断非必要电源并精准释放灭火气体，实现全淹没式高效灭火，且不对精密电子设备造成二次损害；

c. 定期消防安全检测：为确保消防系统始终处于良好运行状态，由专业维保团队每年进行一次对火灾报警系统、气体灭火系统、灭火器及消防通道等进

行全面巡检与功能测试，及时排查并消除安全隐患，确保消防设施完好有效；

d. 专用呼吸防护装备配备：鉴于机房采用了气体灭火系统，为应对突发火情及保障人员在气体喷放后的安全，湖南 CA 在机房指定安全区域专门配备了过滤式消防自救呼吸器，机房运维人员每年定期检查呼吸器的有效期与密封性，确保在紧急状况下可正常使用。

### 5.1.8 设备管理

湖南 CA 建立并维护完整的设备台账，涵盖所有密码设备、服务器、网络及存储等关键资产。设备台账记录每台设备的责任人、当前使用状态及报废标准。为确保湖南 CA 基础设施与密码设备的稳定运行，实现资产全生命周期的精细化、规范化管控，湖南 CA 建立了严密的设备管理体系。

#### 5.1.8.1 建立标准化设备台账

湖南 CA 对所有基础设施、网络设备、密码设备及服务器等实行“一台一档”的台账化管理。设备台账信息详细且动态更新，核心字段必须包含：

- a. 责任人：明确每台设备的唯一归属人与日常运维负责人，落实管理责任。
- b. 使用状态：实时记录设备的运行状态（如正常运行、维护中、停用、待报废等），确保资产底数清晰。
- c. 报废标准：明确各类设备的报废条件（如达到使用年限、性能无法达标、维修成本过高等），规范资产退出机制。

#### 5.1.8.2 定期盘点与账实核对

为防止资产流失及台账信息滞后，湖南 CA 严格执行定期盘点制度：

- a. 常态化盘点：由设备管理部门牵头，采购、财务和机房运维部门一起配合每年定期对机房及办公区域的实体设备进行实地盘点。对于盘盈、盘亏或状态变更的设备，及时更新台账并说明原因，保证台账的准确性、完整性和可追溯性；
- b. 账实核对：将现场设备的实际物理状态、存放位置与设备台账进行逐一比对，确保“账、卡、物”完全相符。

### 5.1.9 存储媒体管理

为保障湖南 CA 核心密码资产与业务数据的绝对安全，防止因存储媒体管理不当导致敏感信息泄露，湖南 CA 针对各类存储媒体（包括但不限于移动硬盘、U 盘、光盘、服务器硬盘等）制定了严格的全生命周期管理规范：

#### 5.1.9.1 存储媒体使用与权限管理

a. 权限分配：实行严格的“专人专用”与“最小权限”原则。根据岗位职责和业务需求，由信息安全管理部门统一分配存储媒体的使用权限。严禁未经授权或跨密级使用存储媒体，严禁在未经授权的存储媒体上存储 CA 核心密钥及敏感业务数据；

b. 安全操作：存储涉密或核心数据的媒体必须采取强密码保护或硬件加密措施。严禁将内部存储媒体接入非涉密计算机、互联网终端或外部私人设备，防范“摆渡攻击”与数据交叉感染。

#### 5.1.9.2 存储媒体报废标准

当存储媒体出现以下情形时，必须纳入报废与销毁流程：

- a. 达到规定的使用年限或保管期限；
- b. 发生物理损坏、老化，且经评估无法修复或数据无法安全清除；
- c. 因业务调整、设备更新等原因不再使用；
- d. 存储的数据已按合规要求完成迁移，且不再需要保留。

#### 5.1.9.3 销毁方法与审批流程

a. 审批流程：存储媒体报废须由使用部门填写申请表，经部门负责人审核、信息安全管理部门评估后，报分管领导审批；

b. 销毁方法：存储核心密钥或绝密级数据的磁介质/半导体介质，须采用消磁、物理粉碎等不可逆方式销毁；普通数据经多次覆写擦除并验证。严禁将涉密存储媒体作为普通垃圾丢弃或出售。

#### 5.1.9.4 全生命周期记录与追溯

- a. 台账管理：建立完善的存储媒体管理台账，对存储媒体的采购、入库、领用、归还、变更及报废等全生命周期环节进行完整记录；
- b. 流转登记：领用与归还时必须办理严格的签字交接手续，确保账物相符；
- c. 销毁归档：在实施销毁时，必须由至少两名授权人员共同监督执行。销毁过程需全程录像，并详细填写《存储媒体销毁登记表》。所有相关记录与审计报告至少保存 3 年以上，确存储媒体管理全过程可追溯、可审计。

### 5.2 操作过程控制

#### 5.2.1 可信角色

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任，任职要求详见 § 5.3.1 章节。所有湖南 CA 的在职人员，按照所担任角色的不同进行身份鉴别；进入机房需要使用门禁卡或指纹识别；进入系统需要使用数字证书进行身份鉴别。湖南 CA 将独立完整地记录其所有的操作行为，湖南 CA 可信角色包括：

| 角色     | 主要职责                        | 人员配置 |
|--------|-----------------------------|------|
| 系统管理员  | 负责系统策略配置、用户与权限管理等           | 2 人  |
| 技术运维员  | 负责物理环境、网络、服务器及系统软件的日常监控与维护等 | 3 人  |
| 数据库管理员 | 负责数据库进行日常运维、性能优化及数据备份等      | 2 人  |
| 系统审计员  | 负责系统和网络日志的审计、管理、审计报告生成等     | 3 人  |

|         |                          |     |
|---------|--------------------------|-----|
| 密钥管理员   | 负责根证书密钥材料管理、根证书密钥生存周期管理等 | 5 人 |
| 业务操作员   | 负责证书申请的受理、审核，订户的身份与意愿鉴证  | 3 人 |
| 客户档案管理员 | 负责客户证书相关档案资料的归档与保密等      | 1 人 |
| 运营审计员   | 负责对客户签发、客户服务等核心业务进行独立审计等 | 3 人 |
| 其他人员    | 对公司运营有重要影响的其他管理人员        | 1 人 |

### 5.2.2 职责分离

为保证系统安全，遵循可信角色分离的原则，即湖南 CA 的可信角色由不同的人担任。湖南 CA 遵循职责分离原则，所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色实现双人操作或复核机制；涉及业务连续性相关操作（运维、鉴证、审计等）的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，具体情况如下：

- a. 系统管理员、技术运维员、数据库管理员、系统审计员之间由不同的人担任；
- b. 同一证书业务的录入与审核环节，由不同的业务操作员完成；
- c. 业务操作员、用户档案管理员、运营审计员之间由不同的人担任；
- d. 密钥管理员、系统管理员、技术运维员之间由不同的人担任；
- e. 密钥管理员不宜与除策略管理机构成员外的其他可信角色兼任。

## 5.3 人员控制

### 5.3.1 可信人员资格要求

湖南 CA 对本公司可信人员进行从业经历调查，公司所有可信人员和即将调入的可信人员都必须同意对其进行从业经历调查。从业经历调查分为：基本调查和全面调查；基本调查包括对工作经历，教育，最高学历证书、社会关系方面的调查；全面调查指除基本调查外还包括对犯罪记录和社会安全方面的调查。湖南 CA 要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响湖南 CA 运行的其它兼职工作、无同行业重大错误记录、无犯罪记录等。

湖南 CA 与公司所有可信人员签署劳动合同。还需与可信人员签署具有法律约束力的保密协议，并承诺不得私自保存、复制或泄露电子认证服务的所有秘密或敏感信息。对于充当可信角色的人员，必须具备履行岗位职责所必需的专业技能要求。

### 5.3.2 可信人员培训要求

湖南 CA 对所有可信人员按照其岗位和角色安排不同的培训，所有可信人员上岗前须完成不少于 20 学时的培训并通过考核；同时每年至少接受一次培训，每人每年培训时长不少于 20 学时并通过考核。当认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

湖南 CA 对运营人员按照其岗位和角色安排不同的培训。对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由湖南 CA 组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。培训内容包括但不限于：

- a. 电子认证服务相关法律法规与标准；
- b. 岗位通用职责要求及各角色特定的工作要求；
- c. 内部管理政策、制度及流程等；
- d. PKI 和密码技术基础知识；
- e. 湖南 CA 电子认证业务规则；

- f. 安全管理策略和机制；
- g. 订户身份查验和审核策略和流程；
- h. 电子认证服务运营体系构成；
- i. 电子认证服务技术体系构成；
- j. 灾难恢复和业务连续性管理

### 5.3.3 工作轮换的周期和顺序

对于可替换角色，湖南 CA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

### 5.3.4 未授权行为的处罚

当湖南 CA 员工进行了未授权或越权操作，湖南 CA 在确认后立即作废或终止该人员的安全令牌和相关证书，中止该员工进入湖南 CA 证书服务体系。根据情节严重程度，实施包括辞退或提请司法机关处理等措施。因未授权或越权操作给湖南 CA 中心或订户造成损失的，当事人负有赔偿责任。

### 5.3.5 提供给员工的文档

为使得系统正常运行，湖南 CA 向其员工提供完成其工作所必须的文档。

## 5.4 审计日志程序

### 5.4.1 审计日志的记录范围

湖南 CA 持续、完整地记录关键操作与事件，包括：

- a. 根证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；
- b. 系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；
- c. 系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系

统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；

d. 网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；

e. 证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；

f. 机房门禁控制等物理环境事件：包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

#### 5.4.2 审计日志的记录内容

审计日志无论其载体是纸张还是电子文档的形式，包含事件的时间、类型、内容、操作人、作用对象及结果；系统的关键操作由操作人员进行电子签名。

#### 5.4.3 审计日志的保存期限

湖南 CA 系统审计日志至少保存至相关证书失效后五年，湖南 CA 授权的人员才能对审查日志进行相应操作，日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作。

#### 5.4.4 日志审计内容

湖南 CA 对系统和操作人员在系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件进行合规性审计。

#### 5.4.5 审计周期

湖南 CA 每季度对系统日志进行一次审计，形成审计报告，并基于审计结果采取改进措施。

### 5.5 记录归档

### 5.5.1 归档范围

- a. 证书申请材料与订户意愿记录：订户身份证明材料、授权委托书、证书申请表、已签署的订户协议，以及通过视频、面签或公证等方式获取的订户意愿表达证据；
- b. 审计日志：RA/CA/KMC 系统产生的管理员操作审计、用户访问审计及权限变更审计等全部日志；
- c. 密码设备全生存周期记录：HSM、密码卡等设备从采购、入库、初始化、密钥灌装、领用、使用、维修至报废销毁的全过程档案；
- d. 密码设备的日常操作与使用记录：设备启停、密钥生成/备份/恢复、状态检查、异常报警处理及日常运维操作记录；
- e. 根证书密钥管理记录：根密钥生成、存储、备份、使用、更新、废止、销毁、恢复等全生命周期操作记录（含多人分持、双人操作相关记录）；
- f. 证书认证系统运行日志：操作系统、数据库、应用服务、证书签发/吊销、OCSP/CRL 服务等日志；
- g. 安全事件处置记录：入侵尝试、病毒/木马告警、非法访问、配置篡改、DDoS 攻击、系统异常崩溃等事件的发现、分析、遏制、恢复、溯源及整改报告；
- h. 证书认证系统关键操作日志：系统启停、策略变更、权限分配、防火墙规则变更、数据库结构变更及 CA 证书更新等高关键操作记录；
- i. 其他重要服务记录：关键投诉处理记录、系统升级记录、第三方安全评估报告及合规自查报告等。

### 5.5.2 保存期限

- a. 订户相关档案：订户申请材料、意愿记录、订户身份证明材料、授权委托书、证书申请表、订户协议、意愿确认记录等档案，自相关证书失效之日起至少保存五年。
- b. 系统日志和审计记录：系统运行日志、审计日志、安全日志及关键操作日志，自记录产生之日起至少保存至相关证书失效后五年。

### 5.5.3 保护措施

对电子归档记录采取技术手段保障其完整性，并存储在安全的物理与数字环境中，建立备份机制。

### 5.5.4 管理机构

#### 5.5.4.1 机构设置

**档案管理中心：**由用户服务中心、运维服务中心等部门以及安全策略委员会抽调相关人员组成档案管理中心。

配置专职用户档案管理员作为用户办理业务以及相关资料专门的档案管理岗位，并明确 A/B 角备岗制度。配置专职机房档案管理员作为机房以及相关技术资料的档案管理岗位，并明确 A/B 角备岗制度。管理职责统管责任：制定档案管理制度、监督各部门归档执行、管理档案访问权限、组织档案鉴定与销毁。

**接收与登记：**接收来自技术部门、运营部、客服部等的归档材料，核对完整性后登记入档。

**保管与保护：**执行所列《保护措施》章节，定期检查存储介质与备份有效性。

**利用与借阅：**仅授权人员可查阅档案，所有查阅行为留痕（时间、人员、理由、查阅内容）。

**到期销毁：**保存期满后，按国家秘密（如涉及）和商业秘密要求，经审批后双人监督销毁。

#### 5.5.4.2 操作规范

**归档流程：**各部门在事件结束后 5 个工作日内提交归档材料→档案管理员核对→生成完整性校验值→导入档案系统→更新归档清单。

**访问控制：**采用“最小必要+审批”原则，查询普通档案需部门领导审批；查询敏感档案（含订户隐私或密钥材料）需合规负责人及技术负责人双签。

### 5.5.4.3 安全要求

用户资料管理员独立于证书签发、系统运维等操作岗位；机房档案管理员不得兼任系统管理员或密钥管理员；所有档案管理员每年接受至少一次档案安全与数据保护培训。

## 5.6 电子认证服务机构根证书密钥更替

### 5.6.1 密钥更替程序

湖南 CA 密钥更替方式如下：

- a. 密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，具体见 6.2 节；
- b. 根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；
- c. 旧密钥处理：在完成签名密钥更替后，由国家密码管理主管部门授权的机构销毁旧私钥及其备份，并保留相关操作记录。

### 5.6.2 密钥更替的时间

湖南 CA 根证书有效期为 20 年。在湖南 CA 根证书到期前二年，湖南 CA 将按照《湖南 CA 密钥管理策略及流程》对 CA 密钥进行更替，生成新的 CA 证书；若发现密钥泄露或存在安全隐患，立即启动密钥更替程序。

## 5.7 损害和灾难恢复

湖南 CA 已制定完整的电子认证服务连续性计划与灾难恢复应急预案，明确了相应的事故与损害处理程序。

### 5.7.1 灾难恢复目标

恢复时间目标（RTO）：核心系统不超过 8 小时，一般业务系统不超过 12 小时

恢复点目标（RPO）：24 小时

### 5.7.2 恢复流程及应急预案

具体应急预案与流程，包括：

a. 证书库恢复流程: 包括重建安全运行环境的流程，生成受影响并被撤销的证书列表，对订户密钥的处理方式，以及重新向订户提供实体公钥证书的要求和流程；生成受影响并被撤销的证书列表：从备份的签发日志和数据库中提取灾难发生前已确认受影响的所有证书，生成撤销证书列表（CRL）并发布；

b. 根密钥损害恢复过程: 包括重建安全环境的流程，为订户重新签发公钥证书，向订户提供新的公钥证书的流程；

c. 其他关键资产恢复方案: 物理设施、计算资源、网络环境、软件或数据，以及其他密钥数据的恢复方案。

### 5.7.3 根私钥应急处理

湖南 CA 的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的嫌疑时，湖南 CA 应该：

a. 立即向电子认证服务管理办公室和其他政府主管部门汇报，并立即吊销所有已经被签发的证书，更新 CRL 信息，供证书订户和依赖方查询。同时湖南 CA 立即生成新的密钥对，并自签发新的根证书，告知订户及依赖方；

b. 新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发下级证书和湖南 CA 下级操作子 CA 证书；

c. 湖南 CA 新的根证书签发以后，将会立即通过目录服务器、HTTP 等方式进行发布。

### 5.7.4 事件报告

同 § 5.9 节。

### 5.7.5 定期验证

a. 根私钥应急处理流程每年进行一次应急演练；

b. 湖南 CA 定期验证备份的设备、数据可用性，包括备份恢复测试和功能

验证，每年至少进行一次灾难恢复演练。

## 5.8 电子认证服务机构终止

因各种原因，湖南 CA 需要终止运营时，将按照相关法律法规规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

湖南 CA 在终止服务九十日前，就业务承接及其他有关事项通知各方，包括但不限于证书订户、依赖方等相关实体。

在终止服务六十日前向中华人民共和国工业和信息化部报告，同时按照相关法律法规的要求办理注销登记手续和业务移交手续。

在 CA 终止期间，采用以下措施终止业务：

- a. 起草 CA 终止声明；
- b. 通知与 CA 业务停止相关的实体和主管部门；
- c. 和具有电子认证服务资质的业务承接单位签署承接协议，明确约定承接机构的工作范围与责任；
- d. 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
- e. 停止证书状态服务并归档相关数据；
- f. 停止其他电子认证相关服务并归档相关数据；
- g. 停止密码设备并归档相关密钥数据；
- h. 撤销业务管理员和业务操作员的操作权限；
- i. 对所有存档文件记录进行整理和封存；
- j. 对所有敏感文档和数据进行安全处理和封存；
- k. 清除主机和密码硬件设备中的敏感数据；
- l. 停止涉及 CA 运营的数据、密钥安全的操作；
- m. 停止与电子签名认证证书外部合作机构的服务，并清除相关敏感数据；

## 5.9 重大事项报告

### 5.9.1 重大事项范围

a. 证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变。符合以下任意之一：

- i. 机房迁移，或机房内服务区、管理区或核心区划设范围改变；
- ii. 变更电子签名认证证书签发逻辑；
- iii. 新增远程证书注册子系统；
- iv. 新增、更改或者删除用于签发电子签名认证证书的证书链；
- v. 其他对电子认证服务安全、用户资料安全有影响的改变。

b. 重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：

- i. 证书签发及验证服务连续停机时间超过 24h；
- ii. 发生根证书密钥等关键数据泄露；
- iii. 持续或较大范围未经授权的私钥访问记录或其他异常活动；
- iv. 系统日志持续或较大范围显示异常操作（如非授权时间或网络地址访问敏感功能）

c. 订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：

- i. 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；
- ii. 数据丢失导致无法恢复证书状态信息

d. 合规性事件：包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：

- i. 涉及电子认证服务的司法判定；
- ii. 收到行政部门违规通知或处罚决定

e. 人力资源类事件：包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：

- i. 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；
- ii. 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确  
认由 CA 承担法律责任。

### 5.9.2 重大事项报告程序

所有重大事项执行三级同步上报机制：内部公司管理层上报、上级机构和  
主管部门上报，严禁迟报、漏报、瞒报、谎报。

### 5.9.3 重大事项报告时限

| 报告主体  | 时限     |
|-------|--------|
| 公司管理层 | 1 小时内  |
| 上级机构  | 48 小时内 |
| 主管部门  | 72 小时内 |

### 5.9.4 重大事项报告内容

- a. 事件完整全过程复盘；
- b. 事件原因分析：技术漏洞、管理疏漏、人为操作、外部攻击、合规管控  
缺失等；
- c. 影响统计：受影响证书数量、受影响订户人数、服务停机时长、舆情及  
投诉情况、监管关联风险；
- d. 全部应急处置动作及后续计划。

## 6. 认证系统技术安全控制

### 6.1 技术安全管理制度要求

湖南 CA 已建立并实施覆盖密钥管理、系统开发、网络防护等领域的技术安

全管理制度，并定期接受安全策略委员会的评审，频率不低于每年一次。

## 6.2 密钥对的生成和安装

### 6.2.1 根证书密钥对的生成和安装

湖南 CA 根证书密钥对的生成与安装要求：

- a. 根证书密钥对应在物理隔离的安全环境中，采用通过国家密码管理部门认可的硬件密码设备生成；
- b. 生成、备份、恢复、销毁过程应实施 5 选 3 多人控制机制，操作应在安全策略委员会授权下进行，并通过录音录像方式全程记录，保存期限不少于操作完成后十年。

### 6.2.2 订户密钥对的生成和交付

订户签名密钥对的生成、交付及控制方式，符合以下要求之一：

- a. 由订户持有的符合国家安全标准的密码模块产生和存储；
- b. 由 CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权；
- c. 采用经主管部门认可的其他创新性保护方案。

湖南 CA 完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期限不少于证书失效后五年。

## 6.3 私钥保护和密码模块工程控制

### 6.3.1 CA 私钥保护和密码模块工程控制

湖南 CA 根证书私钥保护符合的要求：

- a. 根证书私钥保护使用通过国家密码主管部门认可的密码产品，符合 GB/T 37092-2018 第 5 章的要求；
- b. 根证书私钥实施严格的分割保护机制，实现单人无法获取完整私钥；
- c. 根证书私钥备份由密钥管理员分别保存在有防盗措施的安全场所。

### 6.3.2 订户私钥保护和密码模块工程控制

湖南 CA 订户签名私钥保护符合下列要求：

#### a. 通用介质证书

通用介质证书的订户签名密钥对由订户持有的符合国家安全标准的密码模块（如智能密码钥匙）产生，加密密钥对由密钥管理中心产生，订户密钥对均安全存储在智能密码钥匙中，受 PIN 码保护，订户签名私钥由订户持有。湖南 CA 将与订户签订协议，并在协议中要求证书订户要妥善保管自己的介质，PIN 码保密不告知他人并定期修改 PIN 码，确保签名私钥的安全，防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用。

#### b. 云签协同证书

云签协同证书的订户私钥可由订户终端和云签平台协同运算生成，也可由订户委托在云签平台生成，订户通过安全授权认证来独占控制私钥，确保签名私钥的安全，防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用。

具体如下：

- i. 采用的电子签名模式为协同签名模式或代理签名模式；
- ii. 采用不限于口令、短信验证码、生物特征或数字证书等安全控制措施，并每年定期对安全控制措施进行安全评估；
- iii. 每次签名私钥调用必须获得订户的明确授权，授权记录完整保存；
- iv. 将会向订户提供关于签名私钥及激活数据安全使用的指导与建议；
- v. 电子签名模式和控制措施符合相关标准或经主管部门认可的其他方式。

## 6.4 密钥对管理的其他方面

### 6.4.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由湖南 CA 和密钥管理中心定期归档，归档间隔不超过 1 年。

## 6.4.2 证书操作期和密钥对使用期限

- a. 无论订户证书还是 CA 证书，证书到期后，签名私钥不可用于电子签名；
- b. 密钥对使用期限：

| 密钥类型    | 最长有效期 |
|---------|-------|
| 根证书密钥对  | 20 年  |
| 订户证书密钥对 | 10 年  |
| 加密密钥对   | 10 年  |
| 签名密钥对   | 10 年  |
| 会话密钥    | 单次会话  |

## 6.5 激活数据

### 6.5.1 激活数据的产生和安装

- a. 激活数据用于保护订户的私钥。
- b. 通用介质证书存储介质（如：智能密码钥匙）出厂时设置了缺省的 PIN 值，证书制作时更改此 PIN 值并通过安全的方式告知订户，订户可以自行设置或更改。
- c. 云签协同证书应通过安全授权认证（包括但不限于通过口令、短信验证码、生物识别信息、数字证书等）方可激活私钥。

### 6.5.2 激活数据的保护

订户需要采取妥善的方式保护激活数据，当发现激活数据失密，应告知湖南 CA 并申请证书吊销。

### 6.5.3 激活数据的其他方面

- a. 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。
- b. 云签协同证书应通过安全授权认证（包括但不限于通过口令、短信验证码、生物识别信息、数字证书等）才能调用订户私钥。

## 6.6 计算机安全控制

### 6.6.1 系统补丁检查与评审

#### 6.6.1.1 检查频率

安全管理员每半年组织一次全面的系统升级补丁检查，针对“高危”或“紧急”漏洞，不受此时间限制，按应急流程进行变更。

#### 6.6.1.2 检查内容

- a. 操作系统安全更新
- b. 数据库及中间件版本漏洞
- c. 应用系统开发框架及第三方依赖库漏洞。

#### 6.6.1.3 审批与实施

所有补丁升级须遵循“申请—测试—审批—实施—验证”流程并留存完整记录：运维人员发起申请单并附漏洞详情、影响范围及回退预案，在仿真环境中完成兼容性 & 业务回归测试，经主管批准后，在变更窗口内实施并详细记录操作过程，最后通过漏洞扫描工具验证补丁生效情况。

### 6.6.2 无官方支持系统更替与管控

针对已停止技术支持的操作系统及软件，湖南 CA 实施强隔离与限期替换；过渡期内采取网络微隔离（禁止外联、限制端口）、功能裁剪（卸载非核心组件、禁用 USB/PowerShell/匿名共享）及部署入侵防御工具等加强防护措施。

### 6.6.3 杀毒软件安装

所有物理服务器、虚拟机及操作终端安装经公安部认证的防病毒软件。

### 6.6.4 病毒库更新

互联网连接环境：病毒库更新间隔不超过 24 小时，配置为“自动更新”，确保第一时间获取最新特征库。

物理隔离/涉密网络：由管理员通过内部专用分发服务器进行更新，更新间隔不超过 48 小时。

### 6.6.5 病毒扫描周期与策略

执行定时查杀任务，每月至少一次全盘扫描，病毒查杀记录至少保留 180 天。

## 6.7 生存周期安全控制

### 6.7.1 证书认证中心运行管理安全控制

湖南 CA 严格遵循 GB/T 25056-2018 第 10 章要求，建立 CA 系统运行监控机制，实时监测系统状态、证书签发队列、CRL/OCSP 发布情况等。定期备份系统数据与配置信息，确保在发生故障时可快速恢复。所有运维操作（如系统配置变更、证书策略更新）均须经过审批、授权，并记录完整的操作日志。

### 6.7.2 密钥管理中心运行管理安全控制

湖南 CA 严格遵循 GB/T 25056-2018 第 11 章要求，建立密钥管理系统运行监控机制，实时监测密钥生成服务状态、密钥库（备用库、在用库、历史库）运行情况、密钥恢复与归档操作请求等。定期备份密钥数据与系统配置信息，确保在发生故障时可快速恢复。所有运维操作（如密钥生成、密钥备份、密钥恢复、密钥归档等）均须经过审批、授权，并记录完整的操作日志，操作人员须对关键操作进行数字签名。

### 6.7.3 证书操作流程安全控制

湖南 CA 依据 GB/T 25056-2018 第 12 章要求，规范证书的全生命周期操作流程，包括证书申请、审核、签发、延期、撤销及历史归档。建立严格的 CP 与证书操作规范（CPS），确保每一项证书操作均有据可依、流程透明。对 CRL 和 OCSP 响应器进行定期或实时更新与发布，保证证书状态信息的准确性和时效性。

## 6.8 网络安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库的安全运行。湖南 CA 已按照 GB/T 25056-2018 中 5.3.8 的要求，建立并实施网络安全控制体系，具体如下：

### 6.8.1 网络结构设计

湖南 CA 系统网络结构依据 GB/T 25056-2018 附录 A.1 证书认证系统网络结构图设计。核心网络划分为服务区、管理区、核心区等独立安全区域，各区域间通过路由访问控制列表（ACL）或防火墙策略实现逻辑隔离，满足标准对网络架构的安全要求。

### 6.8.2 安全防护

在各区域网络部署下一代防火墙、Web 应用防火墙、入侵检测系统，基于访问控制、防病毒、入侵检测、内容过滤等构建了完整精细的网络安全防护体系。服务器及访问终端均部署企业杀毒软件，实现端到服务器的安全访问。

### 6.8.3 网络拓扑图维护

建立并持续维护完整的网络拓扑图，涵盖所有网络设备（交换机、防火墙、负载均衡器等）。拓扑图由网络管理员负责更新，当设备变更、链路调整或策略修改时，于变更完成后 48 小时内同步更新图纸，确保与机房实际部署情况严格一致。

#### 6.8.4 网络访问控制

严格执行精细化的白名单访问控制机制，采用“IP+端口”方式授权：

a. 证书签发子系统及数据库：仅允许证书注册子系统内的必要功能模块及指定的管理设备访问。签发子系统管理端口仅对特定管理终端开放，数据库仅允许签发子系统及指定数据库管理主机连接；

b. 证书注册子系统及数据库：证书注册子系统的 Web 端口及管理接口仅对最终用户、RA 管理员及运维监控系统的白名单 IP 开放；其关联数据库仅允许注册子系统应用服务器及授权备份/审计主机访问，其他来源连接一律拒绝。

#### 6.8.5 网络监控

建立常态化网络监控，实时监控系统及网络状态并预警。同时建立常态化日志分析机制，定期分析防火墙、负载均衡、交换机、操作系统、应用服务等日志，分析内容涵盖：系统及网络异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

### 6.9 时间戳

#### 6.9.1 使用范围

电子签名服务，对签名时间进行固化，为电子签名提供可信时间证明。电子取证服务，电子数据固定与保全时的时间证明

#### 6.9.2 使用方式

时间戳系统提供的时间戳服务在技术实现上采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

#### 6.9.3 保障机制

- a. 通过国家密码主管部门认可的硬件密码设备；
- b. 7X24 小时不间断服务；
- c. 服务可用率不低于 99%。

#### 6.9.4 相关技术标准

时间戳服务符合 GM/T 0033-2023 时间戳接口规范、遵循国际标准时间戳协议（RFC3161）标准要求。

### 7. 证书、证书撤销列表和在线证书状态协议

#### 7.1 证书

湖南 CA 电子签名认证证书的格式符合 GB/T 20518-2018 的要求。

##### 7.1.1 版本号

证书格式版本号：X.509 V3

##### 7.1.2 证书标准项

湖南 CA 电子签名认证证书包含以下标准项：

- a. 支持的数字证书格式版本号：X.509 V3；
- b. 密码算法对象标识符：符合国家密码主管部门批准的算法对象标识符；
- c. CA 和订户的名称：见 § 3.7 章节；
- d. 证书策略对象标识符：必须包含主管部门制定的相应等级证书策略 OID（2.16.156.339.2.1.1.1/2.1.1.2/2.1.2.1/2.1.2.2），可包含湖南 CA 制定或遵循的证书策略 OID（1.2.156.115291）；
- e. 证书序列号：唯一标识该证书的一组字符；
- f. 证书有效期：根据协议规定定义；
- g. 订户的电子签名验证数据（公钥）；
- h. CA 的电子签名。

#### 7.2 证书撤销列表

湖南 CA 证书撤销列表(CRL)的格式符合 GB/T20518 — 2018 中 5.3 的要求。

### 7.3 在线证书状态协议

OCSP 为湖南 CA 签发的数字证书提供实时的状态查询服务。依赖方可通过 OCSP 协议，在不下载完整证书撤销列表（CRL）的情况下，实时获取单个或多个证书的吊销状态信息。湖南 CA 在线证书状态服务符合 GB/T 19713-2025《网络安全技术公钥基础设施在线证书状态协议》第 7 章的要求。

## 8. 认证机构审计及相关评估

### 8.1 审计评估制度

#### 8.1.1 审计评估的类型

审计的定义与目的：审计是为检查、确认湖南 CA 是否依据《电子认证业务规则》及相关业务规范、管理制度和安全策略开展业务，并发现潜在风险。审计评估的类型如下：

认证业务审计：审计人员由湖南 CA 内部人员组织实施，其结果用于湖南 CA 自身改进和完善业务，且无需公开内部，又称内部审计。

全面符合性评估：由湖南 CA 内部人员组织实施或者委托第三方审计机构进行，对 CA 的业务安全策略、《电子认证业务规则》、业务规范、管理制度以及国家或行业相关标准进行符合性评估。

#### 8.1.2 审计评估的频率

湖南 CA 认证业务的认证业务审计每季度至少一次，全面符合性评估每年至少一次。

#### 8.1.3 评估者的资质

a. 湖南 CA 无条件接收上级主管部门的评估。对湖南 CA 实施评估的评估者所具有的资质和经验，由主管部门决定。

b. 由湖南 CA 安全策略委员会负责组织实施审计，审计评估人员至少具备认证机构、信息安全审计的相关知识，熟悉本 CPS 的规范，以及具备计算机、

网络、信息安全等方面的知识和实际工作经验。内部审计人员选择范围：CA 的安全负责人及安全管理人员、CA 业务负责人、认证系统及信息系统负责人、人事负责人，以及其他根据实际需要确定的相关人员。

c. 如果湖南 CA 认为有必要聘请外部的审计者实施全面符合性评估，那么该审计者应该具备以下的资质：

- i. 必须是经许可的、有营业执照的评估机构，在业界享有良好的声誉；
- ii. 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和规范；
- iii. 具备检查系统运行安全和可靠性的专业技术和工具；
- iv. 熟悉认证机构的管理和运营模式以及相关法律法规。

#### 8.1.4 审计评估的主题

审计所涵盖的主题包括以下几个方面：

- a. 人事审查：对相关人员的任职资格、职责履行等人事相关事项进行审查。
- b. 物理环境建设及安全运营管理规范审查：针对物理环境的建设情况以及安全运营管理规范的执行情况展开审查。
- c. 系统结构及其运行审查：涉及对系统的结构设计和实际运行状况的审查。
- d. 密钥管理审查：对密钥的生成、存储、使用、更新等管理过程进行审查。
- e. 客户服务及证书处理流程审查：围绕客户服务质量和证书处理的流程合规性进行审查。

### 8.2 认证业务审计

#### 8.2.1 审计周期

湖南 CA 认证业务审计每季度至少一次。

#### 8.2.2 审计内容

围绕客户服务质量和证书处理的流程合规性进行审查。审计内容包括但不限于证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份

查验、意愿记录、协议签署、资料保存的合规性；

### 8.2.3 审计方式

审计采用抽样审计方式，抽样率不低于 30%。

### 8.2.4 对问题与不足采取的措施

对于审计发现的问题，通知相关部门和人员及时整改，并跟踪整改落实情况。

## 8.3 全面符合性评估

### 8.3.1 评估周期

湖南 CA 全面符合性评估可采用内部人员或外部第三方评估机构，评估周期不少于每年一次。

### 8.3.2 评估内容

湖南 CA 全面符合性评估的评估内容包括但不限于年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等。

### 8.3.3 审计方式

同 § 8.2.3 节。

### 8.3.4 对问题与不足采取的措施

同 § 8.2.4 节。

### 8.3.5 评估结果的报送与发布

- a. 湖南 CA 在每年 1 月底前将上一年度符合性评估报告报送主管部门；
- b. 除非法律明确要求，湖南 CA 一般不公开评估结果；
- c. 对 CA 关联方，湖南 CA 将依据签署的协议来公布评估结果。

## 9. 法律责任和其他业务条款

### 9.1 费用

湖南 CA 开展了服务成本核算，制定价格策略，各项目的价格详见湖南 CA 的官方网站（[www.hunca.com.cn](http://www.hunca.com.cn)）

#### 9.1.1 证书颁发或更新费用

湖南 CA 对数字证书的收费标准参照市场执行。根据证书实际应用需要，湖南 CA 在不高于收费标准的前提下可以对证书价格进行适当调整。

#### 9.1.2 证书访问费用

在证书有效期内，对该证书信息进行查询，湖南 CA 不收取查询费用。

#### 9.1.3 撤销证书的费用

证书撤销暂不收取费用。

#### 9.1.4 状态信息访问费用

查询证书是否撤销，湖南 CA 不收取信息访问费。对于 OCSP 服务和其他定制的证书状态查询服务，湖南 CA 根据与客户的服务协议要求进行收费。

#### 9.1.5 电子签名的费用

按各项目服务协议和定价标准执行。

#### 9.1.6 签名验证的费用

签名验证暂不收取费用。

#### 9.1.7 签名验证报告的费用

按服务协议和定价标准执行。

### 9.1.8 其他服务的费用

湖南 CA 保留收取其他服务费的权利。

### 9.1.9 收费标准的公布方式

在湖南 CA 公司网站（[www.hunca.com.cn](http://www.hunca.com.cn)）公布。

### 9.1.10 退款策略

在实施证书操作和签发证书的过程中，湖南 CA 遵守并保持严格的操作程序策略。一旦订户接受数字证书，湖南 CA 将不办理退证、退款手续。订户在接受数字证书之前，湖南 CA 接收用户的退款申请，并按照相关退款制度进行退还。如果订户在证书服务期内退出数字证书服务体系，湖南 CA 将不退还剩余时间的服务费用。

### 9.1.11 通用退款办理要求与流程

订户未接收数字证书，湖南 CA 接收用户的退款申请。具体退款资料和流程详见湖南 CA 网站。

## 9.2 财务责任

湖南 CA 保证具有维持、运作和履行其责任的财务能力。湖南 CA 有能力承担对订户、依赖方等造成的责任风险，并依据本电子认证业务规则规定的方式进行赔偿。

湖南 CA 设立赔付专项备用资金作为资金保障方式，资金保障额度不低于上一年度营业收入的 1.5%。资金来源为公司自有资金，管理方式为由公司财务部专户存储、专款专用，每年经审计后向安全策略委员会报告。

## 9.3 业务信息保密

湖南 CA 根据《信息安全技术个人信息安全规范》明确了保密信息和非保密信息的范围。

### 9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

- a. 在双方披露时标明为保密（或有类似标记）的；
- b. 在保密情况下由双方披露的或知悉的；
- c. 双方根据合理的商业判断应理解为保密数据和信息的；
- d. 以其他书面或有形形式确认为保密信息的；
- e. 从上述信息中衍生出的信息。

对于湖南 CA 来说，保密信息包括但不限于以下方面：

- a. 最终订户的私人签名密钥；
- b. 保存在审计记录中的信息；
- c. 年度审计结果。

除非法律有要求，由湖南 CA 掌握的，除作为证书、CRL、认证规则等被明确发布之外的所有个人和公司的信息均需要保密。

湖南 CA 不保存任何证书应用系统的业务信息或交易信息。除非法律明文规定，湖南 CA 没有义务公布或透露订户数字证书以外的信息。

### 9.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、证书使用操作指南等资料中公布的信息是可以公开的。而且湖南 CA 在处理申请业务时可利用这些信息，包括发布上述信息给第三方。

湖南 CA 在目录服务器中公布的证书信息及其状态信息，不属于保密信息。

当湖南 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电子认证业务规则中具有保密性质的信息时，湖南 CA 可以按照法律、法规或规章条款以及法院的判定要求，向执法部门提供相关的保密信息。这种信息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

湖南 CA 与证书持有者之间的协议、往来函和商务协定等，除非法律明确规定，一般不能在未经另一方许可的前提下擅自公开。

对湖南 CA 审计结果等相关信息是保密信息，除了湖南 CA 授权和信任的员工，不能泄露给其他任何人。这些信息除了用于审查目的或法律规定的目的外，不能用于其他用途。

有关湖南 CA 电子认证服务机构运作的信息只能在严格指定的情况下，才能传授给湖南 CA 授权的员工。

控制发证机构软硬件操作的安全措施和管理证书服务及注册服务的安全措施。

除非法律明文规定，湖南 CA 没有义务公布或透露证书持有者证书以外的信息。

湖南 CA 的每个员工都要接受信息保密方面的培训。

## 9.4 个人隐私保护

依据相关法律、法规，湖南 CA 在受理客户申请证书及相关电子签名业务时，需由证书申请人及/或经办人提供相关个人信息。其中个人信息包括：姓名、联系方式、身份证号、地址和身份证（原件及/或任何形式的复本）等个人隐私信息。本《电子认证业务规则》有关用户个人信息保护条款的完整内容见数字认证公司网站公布的《个人信息保护政策》。湖南 CA 针对用户隐私信息提供如下保障措施。

### 9.4.1 隐私保密方案

在数字证书生命周期中，湖南 CA 应在用户个人隐私信息的收集、使用、存储环节中，采取有效手段，保护个人隐私信息。

湖南 CA 应保护证书申请人所提供的、证明其身份的资料。湖南 CA 应采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

湖南 CA 将实施信息安全管理制度以及行业通行的安全技术和程序来确保用

户的个人信息的个人信息不被丢失、泄露、篡改、毁损或滥用。

#### 9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

#### 9.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料，通常不认为是隐私信息，法律或行政法规另有规定的除外。

#### 9.4.4 用户个人信息的收集

根据《电子签名法》第二十条规定，湖南 CA 作为合法的第三方电子认证企业，在受理用户（含自然人个人以及公司法人与非法人组织）申请数字证书时有权对用户的身份进行核实。湖南 CA 要求用户即证书申请人申请证书时通过纸质申请表、电子申请表、证书服务系统等方式提供其能够证明其真实身份的证明材料。湖南 CA 在《证书申请表》等相关协议中已明确告知用户湖南 CA 对用户包含但不限于用户个人的姓名、性别、年龄、身份证号码、家庭住址、联系方式等信息进行收集。

湖南 CA 不会以非公司名义或授权员工个人收集用户个人信息；亦不会对与电子认证业务无关及非必要的个人信息进行收集。

#### 9.4.5 个人信息的存储

湖南 CA 采取严格的技术手段对存储的数据信息进行加密处理，确保用户个人信息不被窃取、泄露，但该等措施并不排除在湖南 CA 的数据信息存储系统受到恶意黑客入侵等特殊情况及地震、洪水等不可抗力的自然因素而可能发生数据信息泄露的风险。

#### 9.4.6 用户个人信息的使用

湖南 CA 不会在与用户自身使用证书服务及应用无关的系统或场合使用证书用户个人信息。发生下列情形之一的，湖南 CA 将依法提供用户个人相关信息：

- a. 基于国家法律、行政法规、规章的规定而提供的；
- b. 经过用户本人书面授权或同意提供的。

除上述情形外，湖南 CA 不会向任何第三方提供用户的个人信息，不会将用户个人信息用于其他用途。

#### 9.4.7 用户个人信息的共享

湖南 CA 不会以商业目的或未取得用户自身同意或授权的情况下与其他组织或个人共享证书用户的个人信息。

#### 9.4.8 CA 对于用户个人信息的管理

湖南 CA 通过以下措施规范用户个人信息的内部管理：

- a. 湖南 CA 遵循法律法规的要求及行业规范要求采取对个人信息安全保护措施；
- b. 湖南 CA 内部建立严格的用户个人信息收集、查阅、使用、处理等管理制度；
- c. 湖南 CA 通过加强内部员工关于个人信息保护的培训，要求员工参加学习培训后签署用户个人信息保护的承诺书。

#### 9.4.9 个人信息的查阅

用户如需查阅及浏览自身的个人信息，请用户按湖南 CA 官方网站公布的联系方式联系湖南 CA 查询。

#### 9.4.10 个人信息的删除和更改

- a. 个人信息的删除：按照法律法规要求或与用户证书服务协议的约定，湖南 CA 有权对证书用户个人信息进行删除。
- b. 个人信息的更改：用户在使用 CA 证书服务过程中，个人信息发生变更的，应当自个人信息变更之日起 2 日内通过湖南 CA 官方网站公布的联系方式提出；由于用户自身原因未及时将变更信息通知湖南 CA 的，由此发生的风险由用户自身承担。

## 9.5 知识产权

除非额外声明，湖南 CA 享有并保留对湖南 CA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。湖南 CA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。按本 CPS 的规定，所有与湖南 CA 发行的证书和湖南 CA 提供的软件相关的一切版权、商标和其他知识产权均属于湖南 CA 的产权，这些知识产权包括所有相关的文件和使用手册。

## 9.6 陈述和担保

除非湖南 CA 做出特别约定，若本电子认证业务规则的规定与湖南 CA 制定的其他相关规定、指导方针相互抵触，以本电子认证业务规则为准。在湖南 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。

### 9.6.1 电子认证服务机构的陈述与担保

湖南 CA 在提供电子认证服务活动过程中的承诺如下：

- a. 湖南 CA 遵守《中华人民共和国电子签名法》及相关法律法规的规定，接受国家工业和信息化部业务监督和指导，对所签发的数字证书承担相应的法律责任；
- b. 湖南 CA 保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定；
- c. 除非已通过湖南 CA 证书库发出了湖南 CA 的私钥被破坏或被盗的通知，湖南 CA 保证其私钥是安全的；
- d. 湖南 CA 签发给订户的证书符合湖南 CA CPS 规定的所有实质性要求；
- e. 湖南 CA 将向证书订户通报任何已知的、将在本质上影响证书的有效性和可靠性事件；

- f. 湖南 CA 将及时吊销证书，并发布到 CRL 上供订户查询；
- g. 证书公开发布后，湖南 CA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

### 9.6.2 注册机构的陈述与担保

湖南 CA 的注册机构在参与电子认证服务过程中的承诺如下：

- a. 提供给证书订户的注册过程完全符合湖南 CA CPS 的所有实质性要求。
- b. 在湖南 CA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致。
- c. 注册机构将按本 CPS 的规定，及时向湖南 CA 提交证书申请、吊销、更新等服务请求。

### 9.6.3 订户的陈述与担保

订户一旦接受湖南 CA 签发的证书，就被视为向湖南 CA、注册机构及信赖证书的有关当事人作出以下承诺：

- a. 订户已阅读并知悉本《电子认证业务规则》的所有条款以及与其证书相关的证书使用政策，并同意承担证书持有人有关证书的相关责任和义务；
- b. 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，并可供湖南 CA 或注册机构检查和核实；
- c. 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生；
- d. 订户对使用私钥的行为负责；
- e. 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、泄密以及其他情况，订户应立刻通知湖南 CA 和注册机构，及时申请采取证书吊销等处理；
- f. 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知湖南 CA 吊销其证书。

#### 9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书只用于申请时预定的目的。

依赖方在信赖其他订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

证书依赖方对证书的信赖行为就表明他们已阅读并知悉本《电子认证业务规则》的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

#### 9.6.5 其他参与者的陈述与担保

从事电子认证活动的其他参与者应遵守本 CPS 的所有规定，并对其在电子认证活动中的行为承担相应责任。

#### 9.7 担保免责

有下列情况之一的，应当免除湖南 CA 之责任。

a. 订户在申请和使用湖南 CA 数字证书时，有违反如下义务之一的：

i. 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息。如已提供的关键材料或信息有变更，可能影响证书使用的，订户应当及时通知湖南 CA。如因材料或信息变更未及时通知湖南 CA，给订户本人或第三方造成的损失，湖南 CA 不承担责任；

ii. 订户应当妥善保管湖南 CA 所签发的数字证书载体、私钥、保护密码 PIN 及云端协同证书身份凭证的安全，不得泄漏或随意交付他人；

iii. 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

iv. 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，应当及时告知湖南 CA 及相关各方，并终止使用该电子签名制作数据；

v. 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得将数字证书用于湖南 CA 规定使用范围外的其他任何用途使用；

vi. 订户必须在证书有效期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被吊销的数字证书；

vii. 订户有义务根据规定按时向湖南 CA 交纳服务费用。

b. 由于下列依赖方的原因造成的损失，湖南 CA 不承担任何赔偿责任，由依赖方自行承担：

i. 依赖方未经检验证书的状态即决定信赖证书的；

ii. 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的。

c. 由于客观意外或其他不可抗力事件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。关于不可抗力的描述参见 § 9.16.4 章节。

d. 因湖南 CA 的设备或网络故障等技术故障而导致数字证书签发延迟、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“技术故障”引起原因包括但不限于：

i. 不可抗力；

ii. 关联单位如电力、电信、通讯部门而致；

iii. 黑客攻击；

iv. 设备或网络故障。

e. 如果湖南 CA 能够证明其提供的服务是符合法律、行政法规相关规定实施的，湖南 CA 将不对订户或依赖方承担任何赔偿或补偿责任。

## 9.8 偿付责任规则

### 9.8.1 偿付责任范围

如出现下述情形，湖南 CA 承担相应有限赔偿责任：含有错误信息，导致订户或依赖方由此遭受损失；

a. 在订户提交信息或资料真实、完整、准确的情况下，湖南 CA 签发的证

书；

b. 由于湖南 CA 原因致使证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失；

c. 对于订户申请吊销的证书，湖南 CA 未能及时吊销证书由此导致依赖方遭受损失。

湖南 CA 只在证书有效期限内承担损失赔偿责任。在证书有效期内产生的损失，订户或依赖方应在证书有效期内向湖南 CA 书面提出索赔。

### 9.8.2 赔付计算方式

湖南 CA 对所有当事实体（包括但不限于订户、依赖方）的合计责任不超过该特定证书适用的赔偿责任上限。对于一份证书产生的所有数字签名和交易处理，湖南 CA 对于任何实体有关该特定证书赔偿的合计责任应该限制在一个不超过下述赔偿责任上限的范围内。湖南 CA 所颁发数字证书的赔偿责任上限如下：高等级证书不超过证书年服务费用价格的三倍，其他证书不超过证书年服务费用价格的两倍。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有上限而不考虑电子签名和交易处理等有关的其他索赔的数量。当超过责任上限时，可用的责任上限将首先分配给最早得到索赔解决的一方。湖南 CA 没有责任为每份证书支付高出责任上限的赔偿，而不管责任上限的总量在索赔提出者之间如何分配的。

### 9.8.3 有限责任

a. 湖南 CA 所有的赔偿义务不得高于本 CPS § 9.8.2 章节规定的赔偿上限。

b. 湖南 CA 根据判决或裁定应当承担赔偿或补偿责任的，湖南 CA 将按照法院的判决、仲裁机构的裁定承担相应的赔偿或补偿责任。

c. 无论本 CPS 是否有相反或不同规定，就以下损失或损害，湖南 CA 不承担任何赔偿和/或补偿责任：

i. 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉

或商誉损害、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

- ii. 由上述第（1）项所述的损失相应生成或附带引起的损失或损害；
- iii. 非湖南 CA 的行为而导致的损失；
- iv. 因不可抗力而导致的损失，如罢工、战争、灾害、恶意代码病毒等。

## 9.9 赔偿

湖南 CA 申请赔偿流程如下：

a. 申请与受理：受损方向通过书面形式，提交《赔偿申请书》，需包含：受损方信息、时间地点、受损情况说明、诉求金额及依据、证明材料清单。湖南 CA 收到书面申请 7-15 个工作日内完成形式审查决定是否受理，不符合受理条件的，出具《不予受理通知书》。

b. 审核与定损：用户服务中心、运维中心、办公室在 15-30 个工作日内完成核查，出具《事故调查报告》，明确责任归属，如涉及大额或复杂案件，法务/外聘律师需在 20 个工作日内出具法律意见。

c. 执行与支付：若受损方接受《事故调查报告》，签署《赔偿协议书》。财务凭生效的《事故调查报告》及《赔偿协议书》，在 5-10 个工作日内完成支付。

## 9.10 有效期和终止

### 9.10.1 有效期限

湖南 CA 的电子认证业务规则自发布之日起正式生效，文档中将详细注明版本号及发布日期，最新版本请访问湖南 CA 网站，对具体订户不做另行通知。

### 9.10.2 终止

当新版本的《湖南 CA 电子认证业务规则》正式发布生效时，旧版本将自动终止。

### 9.10.3 效力的终止与保留

《湖南 CA 电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，终止后各参与方应返还保密信息给其拥有者。

### 9.11 对参与者的个别通告与沟通

湖南 CA 及其注册机构在必要的情况下，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

### 9.12 修订和发布

当本《电子认证业务规则》不适用时，由湖南 CA 安全策略委员会组织 CPS 起草小组进行修订。修订完成后，湖南 CA 安全策略委员会进行审批，审批通过后将在湖南 CA 的网站([www.hunca.com.cn](http://www.hunca.com.cn))上发布新的《电子认证业务规则》。

《电子认证业务规则》将进行严格的版本控制。

#### 9.12.1 修订程序

- a. 湖南 CA 发现 CPS 中所列条款不能适应运营的实际需求，或与现行法律相抵触；
- b. 将现存问题反馈给 CPS 起草小组；
- c. 经过 CPS 起草小组讨论后，提出具体的修改意见；
- d. 修改意见提交安全策略委员会讨论；
- e. 安全策略委员会审查修改意见，如果不通过则提出意见反馈给 CPS 起草小组；
- f. CPS 起草小组根据反馈意见进一步完善。修改意见经安全策略委员会审查通过后，发布更新。
- g. 更新后的 CPS 自公布之日起 30 日内向工业和信息化部备案。

### 9.12.2 通告机制和期限

本电子认证业务规则在湖南 CA 的网站上发布。版本更新时，最新版本的《湖南 CA 电子认证业务规则》会在湖南 CA 的网站及时公布，对具体个人和单位订户不做另行通知。

### 9.12.3 必须修改业务规则的情形

当管辖法律、法规、适用标准及操作规范等有重大改变时，必须修改本电子认证业务规则。

## 9.13 争议处理与举证

与 CP/CPS、电子认证服务相关的争议解决机制：

#### a. 争议解决机制

i. 受理范围：与 CPS、CP、电子认证服务相关的争议；

ii. 处理流程：当事人首先通知湖南 CA，根据本 CPS 中的规定，明确责任方；由湖南 CA 相关部门负责与当事人协调；若协调失败，可以通过仲裁或司法途径解决；

iii. 协商时限：协商解决争议的时限为 30 日；

iv. 调解规则：可通过湖南 CA 安全策略委员会进行调解；

v. 法定争议解决方式：任何因与湖南 CA 就本 CPS 所产生的任何争议而提起诉讼的，受湖南 CA 所在地的人民法院管辖或长沙市仲裁委员会仲裁。

#### b. 举证制度和能力体系覆盖证书全生存周期，包括但不限于：

i. 证书签发环节：身份验证记录、材料审查记录、告知记录、意愿确认记录等；

ii. 签名环节：签名请求验证、签名操作日志、时间戳记录等；

iii. 验证签名环节：验证请求记录、验证结果记录、异常情况处理记录等；

iv. 提供举证材料的时间承诺：湖南 CA 在收到举证请求后按照法律规定提供相关证据。

## 9.14 管辖法律

本电子认证业务规则在各方面服从中国法律和法规的管辖和解释，包括《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

## 9.15 与适用法律的符合性

无论在任何情况下，本电子认证业务规则的执行、解释、翻译和有效性均应遵守和适应中华人民共和国的相关法律法规。中华人民共和国境内适用的法律法规包括但不限于《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》。

## 9.16 一般条款

### 9.16.1 完整规定

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

### 9.16.2 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

### 9.16.3 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

### 9.16.4 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如

合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，湖南 CA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

## 9.17 其他条款

湖南 CA 对本《电子认证业务规则》拥有最终解释权。