中铁数字证书认证中心
电子认证业务规则
（版本号 2.0.3）

版权声明

中铁数字证书认证中心电子认证业务规则受到完全的版权保护。本文件所涉及的“中铁 CA 电子认证业务规则”、“中铁 CA”等是由中铁数字证书认证中心独立持有的，享有完全的版权和其他知识产权。

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。但上述的版权说明和上段主要内容应标于每个副本开始的显著位置。

未经中铁数字证书认证中心的书面同意，任何个人和团体不得以任何方式、任何途径（电子的、机械的、影印、录制等）进行部分的转载、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站 www.sinorailca.com，或者联系中铁数字证书认证中心。本规则如有改动，除法律法规另有要求，不再针对特定对象另行通知。

地址：北京市西城区马连道南街 2 号院 1 楼二层

电话：010-51892503

电子邮件：srca@sinorail.com

注意

《中铁 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：

《刑法》《民法典》《著作权法》《保守国家秘密法》《商标法》《民事诉讼法》《全国人民代表大会常务委员会关于维护互联网安全的决定》《计算机信息系统安全保护条例》《商用密码管理条例》《电子认证服务密码管理办法》《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违法、违规而影响中铁 CA 证书服务的组织、单位和个人，中铁 CA 将保留依法追诉的权利。

修订表

版本	发布日期	备注
1.0	2009 年 4 月 18 日	根据工业和信息化部《电子认证业务规则规范（试行）》修订
2.0	2019 年 6 月 26 日	根据工业和信息化部《电子认证业务规则规范（试行）》修订
2.0.1	2020 年 12 月 09 日	修改 4.4.1 构成证书接受的行为 增加 4.6.1 证书更新的办理方式
2.0.2	2024 年 12 月 13 日	修改 1.1.2 中铁数字证书认证中心概述，概括性描述了开展跨国（境）电子认证服务的情况、修改 1.1.3 证书类别、1.4.2 注册机构、1.5.2 所颁发证书禁止的证书应用列表或者类型、1.6.1 策略文档管理机构、1.7 定义缩写、2.1 认证信息的发布、2.2 发布的时间或频率、3.1.4 不同名称形式的规则、3.3 密钥更新请求的标识与鉴别、4.3.2 电子认证服务机构和注册机构对订户的通告、4.4.1 构成证书接受的行为、4.5.1 订户私钥和证书的使用、4.9 证书撤销和挂起、4.12.1 密钥生成、备份与恢复的策略与行为、5.1.2 物理访问、5.1.8 异地备份、5.5.1 归档记录的类型、5.6 电子认证服务机构密钥更替、6.1.5 密钥的长度、6.2.2 私钥多人控制、7.1.3 算法对象标识符、7.2.2 CRL 和 CRL 条目扩展项、9.3.1 保密的商业信息、9.9.1 SRCA 赔偿责任、9.12 修订、9.13 争议解决等相关描述内容。

2.0.3	2025 年 9 月 18 日	修改 4.9.9 在线状态查询计费方式、5.3.1 中的入职员工考察期、5.4.2 日志的处理周期、5.4.3 审计日志的保存期限、5.4.6 审计采集系统、5.7 造成损害和灾难恢复情况、8.2 修改内部审计评估人员的选择范围、8.4 审计评估规范、修改文档错误内容。

目　录

目　录 ..... - 5 -

1．概括性描述 ..... - 12 -

1.1 概述 ..... - 12 -

1.1.1 电子认证业务规则 ..... - 12 -

1.1.2 中铁数字证书认证中心 ..... - 13 -

1.1.3 证书类别 ..... - 14 -

1.2 SRCA 标识 ..... - 15 -

1.3 文档说明 ..... - 15 -

1.3.1 名称 ..... - 15 -

1.3.2 版本 ..... - 16 -

1.3.3 发布 ..... - 16 -

1.4 电子认证活动参与者 ..... - 16 -

1.4.1 电子认证服务机构 ..... - 16 -

1.4.2 注册机构（Registration Authority） ..... - 16 -

1.4.3 受理点（Business Terminal） ..... - 17 -

1.4.4 证书垫付商（Sponsor） ..... - 18 -

1.4.5 订户（Subscriber） ..... - 18 -

1.4.6 依赖方（Relying Party） ..... - 18 -

1.4.7 证书应用行业组织 ..... - 19 -

1.4.8 其他参与者（Other Participants） ..... - 19 -

1.5 证书应用 ..... - 19 -

1.5.1 适用的证书应用 ..... - 19 -

1.5.2 所颁发证书禁止的证书应用列表或者类型 ..... - 20 -

1.6 策略管理 ..... - 20 -

1.6.1 策略文档管理机构 ..... - 20 -

1.6.2 联系方式 ..... - 20 -

1.6.3 CPS 批准程序 ..... - 21 -

1.7 定义和缩写 ..... - 21 -

2.信息发布与信息管理 ..... - 23 -

2.1 认证信息的发布 ..... - 23 -

2.2 发布的时间或频率 ..... - 23 -

2.3 信息库访问控制 ..... - 23 -

2.3.1 信息的发布与处理 ..... - 23 -

2.3.2 信息访问控制和安全审计 ..... - 24 -

2.3.3 信息资料权限管理 ..... - 24 -

3.身份标识与鉴别 ..... - 25 -

3.1 命名 ..... - 25 -

3.1.1 名称类型 - 25 -
3.1.2 对名称意义化的要求 - 25 -
3.1.3 订户的匿名或伪名 - 25 -
3.1.4 不同名称形式的规则 - 25 -
3.1.5 名称的唯一性 - 26 -
3.1.6 商标的识别、鉴别和角色 - 27 -
3.2 初始身份确认 - 27 -
3.2.1 证明拥有私钥的方法 - 27 -
3.2.2 组织机构身份的鉴别 - 27 -
3.2.3 个人身份鉴别 - 28 -
3.2.4 域名（或 IP 地址）的确认和鉴别 - 28 -
3.2.5 没有验证的订户信息 - 28 -
3.2.6 授权确认 - 29 -
3.2.7 互操作准则 - 29 -
3.3 密钥更新请求的标识与鉴别 - 29 -
3.3.1 常规密钥更新的标识与鉴别 - 29 -
3.3.2 撤销后密钥更新的标识与鉴别 - 29 -
3.4 撤销请求的标识与鉴别 - 30 -
4.证书生命周期操作要求 - 31 -
4.1 证书申请 - 31 -
4.1.1 证书申请实体 - 31 -
4.1.2 证书申请过程与责任 - 31 -
4.2 证书申请审核 - 34 -
4.2.1 执行识别与鉴别功能 - 34 -
4.2.2 证书申请审核流程 - 34 -
4.2.3 处理证书申请的时间 - 35 -
4.3 证书签发 - 35 -
4.3.1 证书签发中注册机构和电子认证服务机构的行为 - 35 -
4.3.2 电子认证服务机构和注册机构对订户的通告 - 35 -
4.4 证书接受 - 36 -
4.4.1 构成证书接受的行为 - 36 -
4.4.2 电子认证服务机构对证书的发布 - 36 -
4.4.3 电子认证服务机构对其他实体的通告 - 36 -
4.5 密钥对和证书的使用 - 37 -
4.5.1 订户私钥和证书的使用 - 37 -
4.5.2 签名及验证 - 38 -
4.5.3 依赖方公钥和证书的使用 - 39 -
4.6 证书更新 - 40 -
4.6.1 证书更新的办理方式 - 40 -
4.6.2 证书更新的情形 - 40 -
4.6.3 请求证书更新的实体 - 40 -
4.6.4 证书更新请求的处理 - 40 -
4.6.5 证书更新的注意事项 - 41 -
4.6.6 颁发新证书时对订户的通告 - 41 -

4.6.7 构成接受更新证书的行为 - 41 -
4.6.8 电子认证服务机构对更新证书的发布 - 41 -
4.6.9 电子认证服务机构对其他实体的通告 - 41 -
4.7 证书密钥更新 - 42 -
4.7.1 证书密钥更新的情形 - 42 -
4.7.2 请求证书密钥更新的订户实体 - 42 -
4.7.3 证书密钥更新请求的处理 - 42 -
4.7.4 密钥更新的注意事项 - 43 -
4.7.5 颁发新证书时对订户的通告 - 43 -
4.7.6 构成接受密钥更新证书的行为 - 43 -
4.7.7 电子认证服务机构对密钥更新证书的发布 - 43 -
4.7.8 电子认证服务机构对其他实体的通告 - 43 -
4.8 证书变更 - 43 -
4.8.1 证书变更的情形 - 43 -
4.8.2 请求证书变更的订户实体 - 43 -
4.8.3 证书变更请求的处理 - 44 -
4.8.4 证书变更的注意事项 - 44 -
4.8.5 证书变更时对订户的通告 - 44 -
4.8.6 构成接受变更证书的行为 - 44 -
4.8.7 电子认证服务机构对变更证书的发布 - 44 -
4.8.8 电子认证服务机构对其他实体的通告 - 44 -
4.9 证书撤销和挂起 - 44 -
4.9.1 证书撤销的情形 - 45 -
4.9.2 请求证书撤销的实体 - 46 -
4.9.3 撤销请求的流程 - 46 -
4.9.4 撤销请求宽限期 - 46 -
4.9.5 电子认证服务机构处理撤销请求的时限 - 47 -
4.9.6 依赖方检查证书撤销的要求 - 47 -
4.9.7 CRL 发布频率 - 47 -
4.9.8 CRL 发布的最大滞后时间 - 47 -
4.9.9 在线状态查询的可用性 - 47 -
4.9.10 在线状态查询要求 - 48 -
4.9.11 撤销信息的其他发布形式 - 48 -
4.9.12 密钥损害的特别要求 - 48 -
4.9.13 证书挂起的情形 - 48 -
4.9.14 证书挂起的订户实体 - 48 -
4.9.15 证书挂起和解挂的流程 - 48 -
4.9.16 挂起的期限限制 - 49 -
4.10 证书状态服务 - 49 -
4.10.1 操作特征 - 49 -
4.10.2 服务可用性 - 49 -
4.10.3 可选特征 - 50 -
4.11 订购结束 - 50 -
4.12 密钥生成、备份与恢复 - 50 -

4.12.1 密钥生成、备份与恢复的策略与行为 - 51 -
4.12.2 会话密钥的封装与恢复的策略与行为 - 51 -
5.认证机构设施、管理和操作控制 - 52 -
5.1 物理控制 - 52 -
5.1.1 场地位置与建筑 - 52 -
5.1.2 物理访问 - 52 -
5.1.3 电力与空调 - 52 -
5.1.4 水患防治 - 53 -
5.1.5 火灾防护 - 53 -
5.1.6 介质存储 - 53 -
5.1.7 废物处理 - 53 -
5.1.8 异地备份 - 54 -
5.2 操作过程控制 - 54 -
5.2.1 可信角色 - 54 -
5.2.2 每项任务需要的人数 - 54 -
5.2.3 每个角色的识别与鉴别 - 55 -
5.2.4 需要职责分割的角色 - 55 -
5.3 人员控制 - 55 -
5.3.1 资格、经历和无过失要求 - 55 -
5.3.2 背景审查程序 - 56 -
5.3.3 培训要求 - 56 -
5.3.4 再培训周期和要求 - 56 -
5.3.5 工作岗位轮换周期和顺序 - 56 -
5.3.6 未授权行为的处罚 - 57 -
5.3.7 独立合约人的要求 - 57 -
5.3.8 提供给员工的文档 - 57 -
5.4 审计日志程序 - 57 -
5.4.1 记录事件的类型 - 57 -
5.4.2 处理日志的周期 - 58 -
5.4.3 审计日志的保存期限 - 58 -
5.4.4 审计日志的保护 - 58 -
5.4.5 审计日志备份程序 - 58 -
5.4.6 审计收集系统 - 58 -
5.4.7 对导致事件实体的通告 - 59 -
5.4.8 风险评估 - 59 -
5.5 记录归档 - 59 -
5.5.1 归档记录的类型 - 59 -
5.5.2 归档记录的保存期限 - 59 -
5.5.3 归档文件的保护 - 60 -
5.5.4 归档文件的备份程序 - 60 -
5.5.5 记录时间戳要求 - 60 -
5.5.6 归档收集系统 - 61 -
5.5.7 获得和检验归档信息的程序 - 61 -
5.6 电子认证服务机构密钥更替 - 61 -

5.7 损害和灾难恢复 ..... - 61 -
5.7.1 事故和损害处理程序 ..... - 62 -
5.7.2 计算资源、软件和/或数据的损坏 ..... - 62 -
5.7.3 SRCA 证书被作废 ..... - 62 -
5.7.4 实体私钥损害处理程序 ..... - 62 -
5.7.5 灾难后的业务连续性能力 ..... - 62 -
5.8 电子认证服务机构或注册机构终止 ..... - 63 -
5.8.1 电子认证服务机构终止 ..... - 63 -
5.8.2 RA 的终止根据 ..... - 63 -
6. 认证系统技术安全控制 ..... - 64 -
6.1 密钥对的生成和安装 ..... - 64 -
6.1.1 密钥对的生成 ..... - 64 -
6.1.2 私钥的传递 ..... - 64 -
6.1.3 公钥传送给证书签发机构 ..... - 64 -
6.1.4 电子认证服务机构公钥传送给依赖方 ..... - 64 -
6.1.5 密钥的长度 ..... - 64 -
6.1.6 公钥参数的生成和质量检查 ..... - 65 -
6.1.7 密钥使用目的 ..... - 65 -
6.2 私钥保护和密码模块工程控制 ..... - 65 -
6.2.1 密码模块的标准和控制 ..... - 65 -
6.2.2 私钥多人控制 ..... - 65 -
6.2.3 私钥托管 ..... - 65 -
6.2.4 私钥备份 ..... - 66 -
6.2.5 私钥归档 ..... - 66 -
6.2.6 私钥导入、导出密码模块 ..... - 66 -
6.2.7 私钥在密码模块的存储 ..... - 66 -
6.2.8 激活私钥的方法 ..... - 66 -
6.2.9 解除私钥激活状态的方法 ..... - 66 -
6.2.10 销毁私钥的方法 ..... - 67 -
6.2.11 密码模块的评估 ..... - 67 -
6.3 密钥对管理的其他方面 ..... - 67 -
6.3.1 公钥归档 ..... - 67 -
6.3.2 证书操作期和密钥对使用期限 ..... - 67 -
6.4 激活数据 ..... - 67 -
6.4.1 激活数据的产生和安装 ..... - 67 -
6.4.2 激活数据的保护 ..... - 68 -
6.4.3 激活数据的其他方面 ..... - 68 -
6.5 计算机安全控制 ..... - 68 -
6.5.1 特别的计算机安全性要求 ..... - 68 -
6.5.2 计算机安全评估 ..... - 68 -
6.6 生命周期技术控制 ..... - 68 -
6.6.1 系统开发控制 ..... - 68 -
6.6.2 安全管理控制 ..... - 69 -
6.6.3 生命期的安全控制 ..... - 69 -

6.7 网络安全控制 ..... - 69 -
6.8 时间戳 ..... - 69 -
7. 证书、证书撤销列表和在线证书状态协议 ..... - 70 -
7.1 证书 ..... - 70 -
7.1.1 版本号 ..... - 70 -
7.1.2 证书扩展项 ..... - 70 -
7.1.3 算法对象标识符 ..... - 70 -
7.1.4 名称形式 ..... - 71 -
7.1.5 名称限制 ..... - 71 -
7.1.6 证书策略对象标识符 ..... - 71 -
7.1.7 策略限制扩展项的用法 ..... - 71 -
7.1.8 策略限定符的语法和语义 ..... - 71 -
7.1.9 关键证书策略扩展项的处理规则 ..... - 71 -
7.2 证书撤销列表 ..... - 71 -
7.2.1 版本号 ..... - 71 -
7.2.2 CRL 和 CRL 条目扩展项 ..... - 72 -
7.3 在线证书状态协议 ..... - 72 -
7.3.1 版本号 ..... - 72 -
7.3.2 OCSP 扩展项 ..... - 72 -
8. 认证机构审计和其他评估 ..... - 72 -
8.1 审计评估的频率或情形 ..... - 72 -
8.1.1 SRCA 的审计 ..... - 72 -
8.1.2 SRCA 对关联单位的审计 ..... - 73 -
8.2 审计评估者的资质 ..... - 73 -
8.3 评估者与被评估者之间的关系 ..... - 74 -
8.3.1 审计评估者与 SRCA 的关系 ..... - 74 -
8.3.2 审计报告与 SRCA 的关系 ..... - 74 -
8.4 审计评估内容 ..... - 74 -
8.5 对问题与不足采取的措施 ..... - 74 -
8.6 审计评估结果的传达与发布 ..... - 75 -
9. 法律责任和其他业务条款 ..... - 76 -
9.1 费用 ..... - 76 -
9.1.1 费用支付 ..... - 76 -
9.1.2 证书费用 ..... - 76 -
9.1.3 证书查询费用 ..... - 76 -
9.1.4 证书撤销或状态信息的查询费用 ..... - 77 -
9.1.5 其它服务费用 ..... - 77 -
9.1.6 退款政策 ..... - 77 -
9.2 财务责任 ..... - 77 -
9.3 商业信息的保密 ..... - 77 -
9.3.1 保密的商业信息 ..... - 77 -
9.3.2 非保密的商业信息 ..... - 78 -

9.4 个人信息的保密 - 78 -
9.4.1 保密的个人信息 - 78 -
9.4.2 非保密的个人信息 - 78 -
9.4.3 客户资料保存 - 79 -
9.5 知识产权 - 79 -
9.6 陈述与担保 - 79 -
9.6.1 电子认证服务机构的陈述与担保 - 79 -
9.6.2 注册机构、受理点的陈述与担保 - 80 -
9.6.3 订户的陈述与担保 - 80 -
9.6.4 依赖方的陈述与担保 - 81 -
9.6.5 其他参与者的陈述与担保 - 81 -
9.7 担保免责 - 81 -
9.8 责任范围 - 82 -
9.8.1 CA 的责任 - 82 -
9.8.2 注册机构的职责 - 82 -
9.8.3 受理点的职责 - 83 -
9.8.4 证书订户的职责 - 83 -
9.9 赔偿 - 83 -
9.9.1 SRCA 赔偿责任 - 83 -
9.9.2 注册机构赔偿责任 - 84 -
9.9.3 受理点赔偿责任 - 84 -
9.9.4 订户的赔偿责任 - 84 -
9.9.5 赔偿额度 - 84 -
9.10 有效期和终止 - 85 -
9.10.1 有效期限 - 85 -
9.10.2 终止 - 85 -
9.10.3 效力的终止与保留 - 85 -
9.11 信任体间的责任关系 - 85 -
9.11.1 信任体和证书订户的赔偿责任 - 85 -
9.11.2 信托关系 - 86 -
9.12 修订 - 86 -
9.13 争议解决 - 86 -
9.14 监管法律 - 86 -
9.15 适用的法律 - 87 -
9.16 其他规定 - 87 -
9.16.1 各种规范的冲突 - 87 -
9.16.2 安全资料的财产权益 - 87 -
9.17 一般条款 - 88 -
9.17.1 完整协议 - 88 -
9.17.2 分割性 - 88 -
9.17.3 强制执行 - 88 -
9.17.4 不可抗力 - 88 -
9.17.5 其他条款 - 88 -

1. 概括性描述

本文件是中铁数字证书认证中心（SRCA）电子认证业务规则（CPS, Certification Practice Statement）。

本 CPS 的结构符合“互联网 X.509 公开密钥基础设施证书策略和认证业务框架”（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网组织“互联网工程工作组”（Internet Engineering Task Force)制定的 RFC3647 标准。RFC3647 框架已经成为 PKI 行业中的一个标准。中铁 CA 尽可能地使 CPS 符合 RFC3647 标准，但它保留在需要的时候采用不同于 RFC3647 结构的权利，如为了提高 CPS 的质量或其对中铁 CA 信任域参与者的适用性。而且 SRCACPS 的结构不一定会与 RFC3647 以后的版本保持一致。

1.1 概述

1.1.1 电子认证业务规则

中铁 CA 电子认证业务规则（CPS）是中铁 CA 对所提供的全部证书服务生命周期中的业务实践（如签发、管理、撤销、更新证书或密钥）所遵循的规范的详细描述和声明，包括责任范围、作业操作规范和信息安全保障措施等内容，是证书管理、证书服务、证书应用、证书分类、证书授权、证书责任等政策规则的集合。中铁 CA CPS 的编制依据《电子认证业务规则规范（试行）》，遵从《中华人民共和国电子签名法》、工业和信息化部《电子认证服务管理办法》及 RFC3647《公钥基础设施证书策略和证书运行框架》，主要由以下几部分组成：

（一）概括性描述

（二）信息发布与信息管理

（三）身份标识与鉴别

（四）证书生命周期操作要求

（五）认证机构设施、管理和操作控制

（六）认证系统技术安全控制

（七）证书、证书撤销列表和在线证书状态协议

（八）认证机构审计和其他评估

（九）法律责任和其他业务条款

中铁 CA 认证体系内的实体以及中铁 CA 数字证书持有者，必须完整地理解和执行中铁 CA 电子认证业务规则所规定的条款，承担相应的责任和业务。

1.1.2 中铁数字证书认证中心

中铁数字证书认证中心(Sinorail Certificate Authority)，缩写为 SRCA，简称中铁 CA。中铁 CA 成立于 2008 年，由中铁信弘远（北京）软件科技有限责任公司运营管理。

SRCA 是由中铁信弘远（北京）软件科技有限责任公司提出、设计、建设并运行的第三方电子认证服务机构，按照《中华人民共和国电子签名法》《电子认证服务密码管理办法》等法律法规，向公众（包括但不限于政府机构、企事业单位、个人）提供身份认证和信任服务。中铁 CA 在 2009 年 4 月通过了国家密码管理委员会办公室组织的建设实施方案专家论证，2009 年 4 月通过了国家密码管理委员会办公室组织的安全性审查，2009 年 4 月通过了国家密码管理局组织的系统安全性审查。SRCA 严格按照工业和信息化部、国家密码管理局的等主管部门的各项要求从事运营服务，获得了国家密码管理局签发的电子认证服务使用密码许可证，所使用密钥由中铁 KMC 提供。

中铁数字证书认证中心是按照国家规范要求建设的、面向全国的信息安全认证机构，承担数字证书的申请、审核、签发、撤销、更新、查询等工作。

中铁数字证书认证中心（中铁 CA）依托铁路广阔的运输信息化应用，面向全国市场应用，提供具有自主特色的电子认证服务。针对不同应用需求，提供以数字证书认证、电子签名等服务为基础的专业化、不同类别、不同级别的全方位服务。

中铁 CA 服务将根据不同的应用和需求，提供分不同类别、不同级别的专业化服务。根据客户应用性质的不同，可分成个人、企业、系统等不同的服务类别，提供有针对性的专业化的定制服务；根据不同应用需求，可分成数字证书认证服务、电子签名服务、系统整体安全保障解决方案等不同服务。

针对铁路市场可分为运输应用服务、经营管理应用、建设运营应用、电子商务应用等不同类别服务，结合应用系统提供专门定制的服务，保证数据交换、信息交换、身份认证、电子签名等安全服务的合法性和有效性。

中铁数字证书认证中心在开展跨国（境）电子认证服务时，需符合我国密码相关法律法规、技术标准和管理要求，根据电子认证跨国（境）业务实际情况，通过电子认证跨境协作协议或合同约定的方式，约定与电子签名认证证书使用的密码算法及证书格式、身份标识与鉴别、证书生命周期操作要求、认证系统技术安全控制及法律责任和其他业务条款等方面的内容。

1.1.3 证书类别

中铁 CA 证书策略根据社会活动中参与的实体不同分为四类证书，根据安全保障级别和证书的适用范围等又进行了细分，用于保障各参与方的权利和义务。

一类证书是个人证书，提供基本的安全保障级别，主要颁发给个人用户，分为个人安全电子邮件证书、个人身份证书、个人代码签名证书。一类证书代表法定公民在中华人民共和国境内从事社会活动的网络身份，只承担由个人行为所引发的责任。一类证书能够应用于数字签名、加密和访问控制，以及中等额度交易中的身份证明。

按照中铁CA证书策略的规定，经过中铁CA或相关注册机构鉴证的一类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其所产生的电子签名符合《中华人名共和国电子签名法》的要求。

二类证书是单位证书，提供高级的安全保障级别，主要颁发给组织机构，分为企业或机构安全电子邮件证书、企业或机构身份证书、法定代表人证书、企业代码签名证书。二类证书用于提供企业或机构的身份证明，代表组织机构在中华人民共和国境内或跨国（境）网络身份，直接或间接(通过委托授权人证书)承担企业网上行为责任。

按照中铁CA证书策略的规定，经过中铁CA或相关注册机构鉴证的二类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其所产生的电子签名符合《中华人名共和国电子签名法》的要求。

三类证书是设备证书，提供高级的安全保障级别，主要分为服务器证书、网关证书、SSL证书、应用系统证书、终端设备证书（移动终端、PC终端等）、物联网设备证书等，保障各类设备的身份。

支持面向移动互联网业务场景下的个人、单位和设备证书进行身份认证与电子签名。订户私钥由订户终端和协同签名服务器协同运算生成，证书请求信息中包含用私钥进行的电子签名，中铁CA使用订户的公钥来验证私钥签名的有效性和申请数据的完整

性。

四类证书是事件型证书，提供基本的安全保障级别，面向事件或活动提供临时身份，主要用于一次性事件型电子签名，签名过后私钥销毁。通过对签名行为业务场景的数据签名，证明数据自签名后未被篡改，保证特定业务场景下数据的完整性和签名行为的不可抵赖性。

按照中铁CA证书策略的规定，经过中铁CA或相关注册机构鉴证的四类证书，在满足《中华人民共和国电子签名法》的其他规定下，由其所产生的电子签名符合《中华人名共和国电子签名法》的要求。

1.2 SRCA 标识

SRCA 是中铁数字证书认证中心（Sinorail Certificate Authority）的缩写。同时，中铁 CA 和中铁 CA 中心也是中铁数字证书认证中心的有效缩写。“SRCA”、“中铁 CA”、“中铁 CA 中心”及其相关的文字、标识、图示等都代表着其所有者——中铁数字证书认证中心的形象，以及在不同场所所代表的利益主体。

中铁数字证书认证中心、“SRCA”、“中铁 CA”、“中铁 CA 中心”的标准图标为：

1.3 文档说明

1.3.1 名称

本文档的名称为 SRCA 电子认证业务规则，是中铁数字证书认证中心对所提供的第三方认证服务及相关业务的全面描述。“中铁 CA 电子认证业务规则”“中铁 CA 中心电子认证业务规则”“SRCA 电子认证业务规则”“中铁 CA CPS”“中铁 CA 中心 CPS”“SRCACPS”

“SRCA 认证业务声明”“中铁 CA 认证业务声明”及其类似表述，无论出现在何种场所，均应被视为是指称本文档或者是对本文档的引用。

1.3.2 版本

本电子认证业务规则（CPS）版本号为 2.0.3。本 CPS 将会根据 SRCA 第三方认证业务的发展更新。电子认证业务规则（CPS）后应注明版本信息（“2.0.3 版本”或“CPS2.0.3”）。

1.3.3 发布

本文档将通过中铁 CA 网站 www.sinorailca.com 面向社会公开发布。如有更新，将在中铁 CA 网站提供更新说明和最新版本。

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

中铁数字证书认证中心是颁发证书的实体，也为证书用户提供电子签名认证服务。中铁 CA 中心和其下属机构统称为 SRCA。

中铁 CA 中心是所有 SRCA 下属机构和实体的根。在十分严密的保密和安全机制控制下，SRCA 根据根证书有效期的策略，自己生成密钥对，自己签发根证书。SRCA 根据授权和协议，签发下一级的证书。SRCA 所签发的证书与每一个证书申领实体的公钥绑定。SRCA 已签发的、在有效期内的证书，将采用证书目录服务器和证书撤销列表 CRL（Certificate Revocation List） 服务公布该证书可以公开的信息和状态。

SRCA 将根据业务需要，与 SRCA 服务框架体系中未涉及的其它 CA 机构建立交叉认证关系，实现互联互通。交叉认证是指两个完全独立的、采用各自 CPS 的认证机构之间建立相互信任关系，从而使双方的证书用户可以实现互相认证。

1.4.2 注册机构（Registration Authority）

注册机构 RA，作为 SRCA 授权委托的下属机构，负责对证书用户信息的审核、整理汇总、统计分析、与上级 CA 进行数据交换、管理和服务下属受理点(BT)等。每个 RA 可

以按照行业、行政地域或其它因素分成 BT，对最终用户提供服务。RA 机构是为最终证书申请者建立注册过程的实体，对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。RA 机构依据相关法律、法规在受理申请证书及相关电子签名业务时，需由证书申请人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，依照相关法律、法规和本 CPS 妥善保存证书用户的数据，不允许将证书用户的数据透露给与证书业务无关的任何单位或个人，不允许用作商业利益方面的用途。RA 必须获得 SRCA 的授权，根据授权从事各类证书服务，并依据授权拓展相应的下级服务机构。

1.4.3 受理点（Business Terminal）

经过 SRCA 及其授权注册机构的审查，SRCA 及其授权注册机构可以授权某特定单位或实体成为受理点，负责办理数字证书的申请、撤销、查询等证书服务。证书有关服务的申请手续、办理过程和受理要求，必须与 SRCA 正在实施的 CP、CPS 以及 SRCA 与之签署的受理点授权协议书相一致。受理点负责向 SRCA 或 RA 提供证书服务申请实体的信息，包括申请实体的名称、可以表明身份的法定标识以及 SRCA 要求的任何合法的证明文件、联系方法（通信地址、电子邮件信箱、电话）等。受理点（BT）根据这些信息为申请实体提供证书申请、证书制作、签名密钥生成、证书查询、证书撤销、证书更新等被授权的服务或根据申请实体的要求，提供申请实体任何其它合乎本 CPS 及 SRCA 公布的服务和技术支持。受理点（BT）对其提供证书服务的受理过程负有相关的法律责任，包括但不限于本 CPS 和授权协议中所规定的有关内容。根据是否承担证书申请者费用的不同情况，受理点可以分为垫付型受理点和非垫付型受理点。除非特别声明，受理点通常指非垫付型受理点。

如果受理点满足和实现了 SRCA 对实行证书垫付服务的要求，并取得了 SRCA 及其授权机构的授权，则把该受理点称为垫付型证书受理点。

如果受理点没有承担证书申请者的费用（与垫付型证书受理点不同），则称该受理点为非垫付型受理点。

1.4.4 证书垫付商（Sponsor）

证书垫付商，是指能够为其所属或所服务的订户或潜在订户群体承担所有证书服务费用的团体或者组织。证书垫付商根据本 CPS 的规定、SRCA 公布的其它规定和法律、政策要求的情况，有权取缔由其支付费用的证书持有者的全部或部分证书服务，包括但不限于对持有者数字证书的取消。垫付商必须根据与 SRCA 签署的协议，事先预订证书数量并预先缴纳所有的证书费用，并可以根据 SRCA 的规定享受一定的优惠政策。垫付商必须承担其代付费用的全部证书持有者的身份真实性的责任。

1.4.5 订户（Subscriber）

订户，即证书持有人、证书用户、证书客户，是指从 SRCA 接受证书的实体。包括已经申请并拥有 SRCA 签发的数字证书的个人、企业、组织、机构、服务器设备、网站等各类主体或实体，以及其他任何具有确定的身份标识，并持有 SRCA 签发的各类证书的对象，包括任何实体或者非实体的人、物和组织等。

订户分为两类：

（1）被垫付的证书持有者，其证书费用由证书垫付商承担；

（2）自支付的证书持有者，自行承担证书费用。

订户在申请证书之前，已被建议接受适当的电子认证技术使用方面的培训。订户可以从 SRCA 得到有关电子签名、证书、PKI 等相关的文件和学习资料，SRCA 会根据实际情况，通过网站、培训活动、宣传材料等提供。SRCA 提供不同类型的证书，订户应决定何种证书适合于自己的需要。订户同意如遇危及私钥安全的状况时及时通知发证机构。

1.4.6 依赖方（Relying Party）

对于依赖方，SRCA 承诺，除了未经验证的订户信息外,证书中的所有信息都是准确的。依赖方应合理的信任证书以及相关的数字签名。如果信任数字签名时需要额外保证，依赖方必须在得到这些保证后才能合理的信任该数字签名。

作为 SRCA 证书订户的依赖方，享有 SRCA CPS 规定的各种相应的权利，包括 SRCA 可能提供的证书保障，以及本 CPS 中涉及的权益。非 SRCA 订户的依赖方，SRCA 除了担保其所信任的并且由 SRCA 签发的证书和相关签名信息的真实性以外，不承担其它义务和责任。

1.4.7 证书应用行业组织

证书应用行业组织是 SRCA 电子认证服务重要的参与者。SRCA 数字证书在行业的应用，得益于证书应用行业组织的许可。证书应用行业组织对 SRCA 的基础证书用户是否具有在本行业的具体应用中的使用权限具有决定权。为便于证书在各行业的拓展，并保持基础证书的通用性，SRCA 在证书中定义证书订户在行业应用中的权限，采用证书扩展域定义证书用户在行业应用中的需要的关键信息。

1.4.8 其他参与者（Other Participants）

SRCA 电子认证活动的其他参与者包括以上未提及的，属于 SRCA 认证体系的，与电子认证服务相关的其他各类实体。例如 SRCA 选定的 PKI 应用技术服务提供者、目录服务提供者等。

1.5 证书应用

1.5.1 适用的证书应用

SRCA 签发的证书，从功能上可以满足下列安全需要，除非被要求，否则 SRCA 通常并不承担下列安全需要的实现：身份认证—保证采用 SRCA 信任服务的证书持有者身份的真实性；验证信息完整性—保证采用 SRCA 证书和数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收的信息是否完整一致；验证数字签名—对信任体交易不可抵赖性的依据即数字签名进行验证。必须指出，对于任何电子通信或交易，不可抵赖性应根据法律和争议解决办法裁定。SRCA 证书支持机密性。机密性保证传送方和接收方信息的机密，不会泄露给其它未合法被授权方。但 SRCA 对机密性事件，没有承担相应责任的义务。对于机密性用途而引发的所有直接或间接的破坏和损失，SRCA 不承担责任。SRCA 目前支持两种不同信任等级的用户证书，正式证书和测试证书。正式证书的申请者必须通过规定的实体身份认证和 SRCA 需要的鉴别程序，有效期一般为 1 年。测试证书有效期一般不超过 3 个月。SRCA 一般不接受证书订户对证书有效期的特殊要求，除非证书垫付商、证书应用行业组织和 SRCA 商议并形成关于证书有效期的专门协议。涉及证书签发、申请、受理、操作、管理、使用的单位和个人，应熟悉本 CPS 中的术语、条件、需求、建议以及权益等内容。

SRCA 证书可以在电子商务、企业信息化、网上信息传递、网上公共服务等多个领域应用，为建设网络信任环境提供了基础性的信任服务。详细信息请参阅中铁 CA 网站 www.sinorailca.com。证书申请者、订户和依赖方等各类主体可以根据实际需要，自主判断和决定采用相应合适的证书类型，以及了解证书的应用类型、应用范围，选择自己的应用方式。

除非在本 CPS 中特别声明,SRCA 没有义务承担因任何使用证书而产生的额外的经济赔偿责任。

1.5.2 所颁发证书禁止的证书应用列表或者类型

SRCA 证书禁止在任何违反国家法律、法规或破坏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。

SRCA 所颁发的数字证书主要在铁路行业身份认证、数据完整性、数据机密性、不可否认性等应用场景中实现人员、机构和设备的实体信息关联绑定，在铁路行业以外使用造成的法律后果由订户自己承担。

1.6 策略管理

1.6.1 策略文档管理机构

根据《中华人民共和国电子签名法》《电子认证服务管理办法》及其它法律法规的要求，中铁 CA 制定本 CPS。

中铁 CA 安全策略委员会，是 SRCA 电子认证业务规则的最高管理机构，由安全策略委员会主任召集管理人员、技术人员、客服人员等组成，负责审核并批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

1.6.2 联系方式

SRCA 对电子认证业务规则进行严格的版本控制，并由中铁 CA 负责解释。

电话： 010-51892503

地址： 北京市西城区马连道南街 2 号院 1 楼二层

邮编： 100055

电子邮件：srca@sinorail.com

1.6.3 CPS 批准程序

SRCA 的 CPS 由中铁 CA 安全策略委员会指定的专人或编写组起草拟定后，提交中铁 CA 安全策略委员会审核。如需进行变更，由指定的专人或编写组提交变更报告及进行修改，中铁 CA 安全策略委员会将对提供的变动建议进行研究分析，并征询法律顾问有关意见后，形成最终决议。SRCA 将在决议形成后，在网站公布变更后的《电子认证业务规则》正式文档。

1.7 定义和缩写

公钥基础设施（PKI）：即 Public Key Infrastructure,是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛地用于 CA 认证、数字签名和密钥交换等领域。

电子认证服务机构（CA）：即 Certificate Authority，是指颁发用以创建数字签名和公/私密钥对的电子签名认证证书的可信第三方组织或者公司。本规则指中铁数字证书认证中心（SRCA）。

注册机构（RA）：Registration Authority，证书的注册机构，负责证书的申请业务。本规则指中铁数字认证中心注册机构。

密钥管理中心（KMC）：Key Management Center,负责管理和维护密钥的全过程，包括生成、存储、备份、恢复等。本规则指中铁 KMC。

电子认证业务规则（CPS）：Certification Practice Statement，是关于电子认证服务机构在全部证书服务生命周期中的业务实践（如签发、管理、撤销、更新证书或密钥等）所遵循的规则的详细描述和声明，提供其它业务、法律和技术方面的细节。SRCA CPS，是 SRCA 证书相关业务和系统的运行规则。

证书策略（CP）:Certificate Policy,是关于电子认证服务机构制订的一个指定的规则集合，表明证书对于具有普通安全需求的一个特定团体和(或)具体应用类的适用性。

证书撤销列表（CRL）：Certificate revocation list，由电子认证服务机构(CA)签发并发布的被撤销证书的列表。证书撤销可能由于证书过期、私钥失窃或者其他原因产生。又称证书吊销列表、证书黑名单。

CA 注销列表（ARL）：Certificate authority revocation list，是标记已经被注销的 CA 的公钥证书的列表,表示这些证书已经无效。

在线证书状态查询协议（OCSP）：Online Certificate Status Protocol，X.509 公钥基础设施的一部分，在不请求 CRL 的情况下判断证书状态的协议。

电子签名认证证书（证书）：Certificate，是经一个权威的、可信赖的、公正的第三方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据电文或者其他电子记录。认证机构可以签发自己的证书，这种自签名的证书称为该 CA 的根证书并用来签署下级证书。

电子签名人：是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的实体。

电子签名依赖方：是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的实体。

私钥（电子签名制作数据）：Private key，是非对称算法产生的两个密钥中的一个，由最终订户唯一持有，用于制作电子签名。

公钥（电子签名验证数据）：Public key,是非对称算法产生的两个密钥中的一个，绑定在电子签名认证证书中，通过 SRCA 在公网上发布，用于验证电子签名信息的有效性。

在电子签名认证证书中，通过 SRCA 在公网上发布，用于验证电子签名信息的有效性。

2.信息发布与信息管理

2.1 认证信息的发布

SRCA 通过网站 www.sinorailca.com 提供信息服务包括但不限于以下内容:电子认证业务规则（CPS）、证书策略（CP）、证书、证书撤销列表（CRL）查询服务、在线证书状态查询服务（OCSP）和 SRCA 不定期发布的信息。SRCA 证书订户都可以通过 SRCA 网站 www.sinorailca.com 查询有关信息。

SRCA 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 SRCA 的目录服务器获取证书的信息。SRCA 存储用户的身份认证公开信息和证书相关信息，不包含任何交易数据，数据信息以数据库方式存放。SRCA 系统成功签发证书后，同时将订户证书和 CRL 发布到目录服务器，供订户在线查询证书。SRCA 证书订户可以通过 LDAP 查询、下载并验证订户证书。

2.2 发布的时间或频率

证书通过目录服务器发布时，SRCA 将在成功签发证书的同时进行发布。发证机构在挂起或撤销证书后，必须在 24 小时内，在 SRCA 信息库中发出挂起和撤销的公告，更新证书撤销列表和在线证书状态查询服务。根据需要，也可以人工发布最新 CRL。

除非另有规定，SRCA 保证每 24 小时一次发布各类证书的撤销表（CRL），提供在线证书状态查询服务（OCSP）。在紧急情况下，SRCA 可自行决定缩短公布证书撤销列表的时间。网站的公告、SRCA CPS 公布、证书应用情况、学习资料等信息不定期进行更新，无固定的发布时间或频率。

2.3 信息库访问控制

2.3.1 信息的发布与处理

SRCA 将及时在网站上发布新的各类信息（如公告、学习资料、证书应用情况等）。只有 SRCA 授权的工作人员有权对 SRCA 网站上的信息进行处理。

SRCA 对外公布证书信息和 CRL 信息，任何 SRCA 订户或非订户均可使用 LDAP 查询证书，获取当前证书状态信息。

2.3.2 信息访问控制和安全审计

SRCA 设置了信息访问控制和安全审计措施，保证只有经过授权的 SRCA 工作人员才能编写和修改 SRCA 网站的公告或发布信息。SRCA 网站在物理上与 SRCA 系统无关。

2.3.3 信息资料权限管理

SRCA 在必要时可自主选择是否实行信息的权限管理，以确保只有经过授权的人员或机构才有权阅读受 SRCA 控制的信息资料，确保 SRCA 相关实体的实际权益。

3.身份标识与鉴别

3.1 命名

3.1.1 名称类型

认证机构依照特定的签发程序，保存与证书注册过程有关的特定记录，对特定对象的身份进行鉴别，以区别于其他的申请者。SRCA 生成或签发的证书的主要识别名称（SubjectName),采用 X.501 Distinguished Name(DN)的方式。每个证书订户按照 X.509 的规定，将对应一个可分辨的名称。作为可信第三方的认证机构负责确认公钥与已命名实体之间的联系。这种确认关系通过证书明白无误地表示出来。命名可以由 SRCA 和申请者协商解决，也可以由申请者独立完成。

3.1.2 对名称意义化的要求

SRCA 标识名称所采用的用户识别信息一般具有明确的、可追溯的、肯定的代表意义，订户应该使用真实名称，个人订户应使用身份证件所标示的名称；单位订户应使用工商营业执照、企事业单位组织机构代码证等所标示的名称；设备证书应使用能标识该设备的名称。特殊情况允许匿名或者伪名等出现。

3.1.3 订户的匿名或伪名

SRCA 中心允许订户使用匿名或假名，但只限于党政部门存在特殊要求证书的申请。订户必须在申请时明确申明其所用匿名或假名申请证书的目的以及使用范围,SRCA 会对其进行严格审核同时要求订户保证其证书使用范围的控制并签定协议，如超出范围使用而造成的一切后果由订户自行承担。其名称将使用抽象通用名称，如：zf1401020012、bb140000007602 等。SRCA 中心会将使用部门提出的特殊要求申请存档。

3.1.4 不同名称形式的规则

SRCA 签发的证书其甄别名 DN 的内容格式都符合 X.501 Distinguished Name（DN）的命名方式，中铁 CA 的用户证书甄别名称中包含下表所列出的组成部分：

识别名称（DN）	说　明	内　容（示范性）
Country(C)	所在国家名称	C=CN
Organization(O)	证书颁发机构	O= Sinorail Certification Authority
Organization Unit（OU）	单位或部门名称	OU=CA中心 可以不填写。可以作为应用预留字段，具体定义结合证书应用完成。一张证书可以包含多个 OU 属性。
Common Name（CN）	证书持有者的一般通用名称	CN=张三 必须填写。

通用名称 CN 包含于每张证书的主题中，各类证书命名方式不同，但是所有证书订户通用名称都需要严格审查。一般命名方式如下：

1	个人证书	个人姓名（与身份证件上标明的一致）。
2	单位证书	单位名称或单位下属的某一部门（与单位的营业执照、组织机构代码证等有效证件上标明的一致）。
3	设备证书	能标识该设备的名称（如域名或者 IP 地址）。
4	事件型证书	根据业务及场景要求确定标识名称。

3.1.5 名称的唯一性

SRCA 的所有证书持有者，甄别名必须都是唯一的。SRCA 根据该名称有效地鉴别证书持有者。当出现相同的名称时，以先申请者优先使用，SRCA 没有权利和义务处理因此产生的相关纠纷，相关用户可以向有关主管部门申请解决。

当订户或者申请者的名称，经有关主管部门的合法文件证明为其他订户或者申请者所有时，SRCA 将即刻撤销先前用户对该名称的使用权，该用户必须承担因此产生的法律责任。

3.1.6 商标的识别、鉴别和角色

使用商标作为标识符，应向 SRCA 提供商标注册方所有权的文件证明。SRCA 尊重任何订户名称中的注册商标权，禁止任何证书申请者对他人知识产权的侵犯。但 SRCA 对证书申请者在其证书申请中提供的标识符是否具有知识产权不做验证和认可，并且不保证这种权利的唯一性。对于因商标、服务标志等的归属问题造成的纠纷，SRCA 不负有仲裁或调停等责任，这不在 SRCA 的业务职责范围之内。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

发证机构必须验证申请者拥有私钥的合法性和正确性。至少通过以下任何一种方法验证申请者的私钥：

（1）通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。在 SRCA 电子认证服务体系中，私钥在用户端生成，证书请求信息中包含用私钥进行的数字签名，SRCA 用其对应的公钥来验证这个签名。

（2）SRCA 为证书申请者提供完成证书申请所需要的初始化信息。证书申请者在申请证书或证书的某些操作中必须使用这些初始化信息，向 SRCA 确保其是私钥的合法所有者。

SRCA 要求证书申请人妥善保管自己的私钥，因此，证书申请人被视作其私钥的唯一持有者。

3.2.2 组织机构身份的鉴别

在组织机构申请者身份的鉴别流程中，SRCA 将按照每种证书的要求进行不同的验证。证书申请表上需要组织机构所授权代表（经办人）的签字，经办人应持身份证件供鉴别身份。SRCA 或其授权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 SRCA 提供单位或服务器确实存在的有效证明，包括但不限于工商营业执照、税务登记证、企事业单位组织机构代码证等，申请法定代表人证书还需提供法定代表人的身份证件；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。SRCA

在进行法律规定的有限审查后，不承担对申请者身份证明文件（如身份证等）进行合法性甄别的义务。

SRCA 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、主管部门的要求决定。

3.2.3 个人身份鉴别

在个人申请者身份的鉴别流程中，可以使用以下有效的身份证件：身份证、护照、军官证、警官证、士兵证、士官证和文职干部证等。证书申请表上有申请者本人或被充分授权的证书申请者代表的签字。SRCA 主要通过面对面鉴定方式进行个人的身份鉴别。SRCA 将申请者本人和两份身份证明（原件和复印件）进行比较。身份证明文件必须是有效的身份证件。如果 SRCA 或受理点已经明确确认申请者个人的身份，那么 SRCA 或受理点可以信任现有的证明。

申请者必须承担材料的真实性的责任，SRCA 在进行法律规定的有限审查后，不承担对申请者身份证明文件（如身份证等）进行合法性甄别的义务。SRCA 和其授权注册机构、受理点在规定期限内保存申请者的全部申请材料，这个规定期限由法律、政策、主管部门的要求决定。

3.2.4 域名（或 IP 地址）的确认和鉴别

如果证书的名称为域名（或 IP 地址），除了在对申请者递交的书面材料进行审核外，SRCA 需要申请者提供额外的域名（或 IP 地址）使用权证明材料，申请者必须承担材料的真实性的责任，SRCA 在进行法律规定的有限审查后，不承担对该证明材料进行合法性甄别的义务。

3.2.5 没有验证的订户信息

订户证书中所包含信息以外的信息为没有验证的订户信息。

3.2.6 授权确认

为确保经办人具有特定的许可，能够代表组织机构获取数字证书，需要组织机构对其授权。组织机构在 SRCA 的数字证书申请表上加盖单位公章后，则证明本组织对经办人的授权确认。

3.2.7 互操作准则

对于其他电子认证服务机构，如果双方之间有协议，那么 SRCA 将依据协议的内容，接受该机构鉴别过的信息，并为之签发相应的证书。如果双方之间没有任何的协议，SRCA 会根据业务需要，决定是否接受这些被其他机构鉴别审核过的资料进行受理。

如果国家法律法规对此有规定，SRCA 将严格予以执行。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

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。SRCA 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”。

订户使用当前私钥对密钥更新请求进行签名，订户的身份验证一是使用订户持有的公钥验证确认签名以识别，二是使用与初始身份验证相同的流程进行标识与鉴别。

对于 SRCA 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、主题名和证书用途的证书。除非先将证书撤销，否则在证书有效期到期前，不能通过申请新证书的方法获得有相同签发者、主体名、身份标识和证书用途的证书。

事件型证书不涉及密钥更新。

3.3.2 撤销后密钥更新的标识与鉴别

SRCA 不为被撤销后的证书提供密钥更新，撤销的证书订户必须重新进行身份鉴别和注册，向 SRCA 申请重新签发证书。订户在申请重新签发证书时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件。

3.4 撤销请求的标识与鉴别

订户撤销证书的标识和鉴别，通过以下方法中的一种来进行：

（1）到 SRCA 或其授权的证书服务机构，递交撤销申请并进行身份鉴别。

（2）如果由于条件的限制无法进行现场审核时，SRCA 将首先采取证书挂起的方式让证书暂时失效，直到完成身份鉴别以后，再对证书进行撤销处理。订户本人撤销时的身份标识和鉴别使用原始身份验证相同的流程，详见 3.2.2 组织机构身份的鉴别和 3.2.3 个人身份的鉴别。

如果 SRCA 或其授权的证书服务机构已经明确确认申请者的身份，那么 SRCA 或其授权的证书服务机构可以信任现有的证明。

如果是因为订户没有履行本 CPS 所规定的义务，由受理点申请撤销订户的证书时，不需要对订户身份进行标识和鉴别。

SRCA 保证对于撤销请求的鉴别，予以合理的进行。

4.证书生命周期操作要求

本章节描述的证书包括CA证书、管理员证书、普通订户证书。本章节主要以普通订户证书为例，描述证书业务规则。

4.1 证书申请

4.1.1 证书申请实体

在证书申请的过程中，参与整个申请过程的实体主要包括：

（1）证书申请者，包含个人、政府机构以及企业单位、事业单位、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。

（2）注册服务受理机构，包括 RA、BT、证书垫付商，以及相应的系统、管理员、操作员等。

（3）电子认证服务机构，本CPS中指SRCA。

（4）订户，从SRCA接受证书的实体，详见1.4.5 的内容。

（5）主管部门，包括《中华人民共和国电子签名法》《电子认证服务管理办法》《电子认证服务密码管理办法》等规定的各类主管部门。

4.1.2 证书申请过程与责任

一、证书申请过程

1、证书申请者通过中铁CA网站www.sinorailca.com或者是到SRCA授权受理点领取数字证书申请表（一式三份），根据申请表上的注意事项认真、如实、完整地填写申请表内容，并签名（个人）或盖章（单位）。

2、证书申请者携带申请表和身份证明材料到SRCA授权受理点进行身份审核。

3、受理点核对证书申请者和相关身份资料。如果身份鉴别未通过，受理机构将拒绝为用户发放证书，并将未通过的信息存档。

4、如果身份鉴别通过，受理机构录入信息、审核证书申请信息，提交CA处理。受理机构可以提前录入证书申请者信息。

5、CA 根据证书请求签发证书。

6、受理机构下载证书后，将其递交给申请者。

二、各参与方的责任

1、电子认证服务机构的责任

保证电子认证服务机构本身的签名私钥在 SRCA 内部得到安全的存放和保护，SRCA 建立和执行的安全机制符合国家相关政策的规定。

电子认证服务机构对其授权的注册机构、受理点进行审计和管理，保证整个申请过程的安全可靠。

电子认证服务机构保证整个 CA 系统安全可靠的运行。SRCA 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赔偿责任。这些事件包括罢工或其他劳动纠纷、暴力、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其他灾难等。

由于技术的进步与发展，电子认证服务机构会要求证书订户及时更新证书以保证证书的可靠性。

2、注册机构 RA 的责任

电子认证服务机构根据本 CPS 和授权协议对 RA 进行管理。注册机构 RA 按照程序取得 SRCA 的授权，遵循本 CPS 和 SRCA 的授权运作协议和其他 SRCA 公布的标准和流程，接受并处理证书服务申请者的证书服务请求，并依据授权设置和管理下级证书服务受理机构 BT。RA 必须遵循 SRCA 制订的服务受理规范、系统运营规范和管理规范，确定下属受理点的管理方式。根据本 CPS 规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理措施。SRCA 将不断的完善并及时发布有关的规范和标准内容。

3、受理点（BT）的责任

受理点 BT 按照程序取得 SRCA 和其上级 RA 的授权，遵循本 CPS 和相关的授权运作协议和其它 SRCA 公布的标准和流程，接受并处理证书服务申请者的证书服务请求。受理点必须遵循 SRCA 和其上级 RA 制订的服务受理规范、系统运作规范和管理规范，SRCA 和其上级 RA 将不断的完善并及时发布有关的规范和标准内容。根据本 CPS、SRCA 和其上级 RA 公布的规范，受理点有权决定是否给申请者提供相应的证书服务。受理点依据本 CPS 的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理措施。SRCA 和其上级 RA 根据本 CPS 和授权协议对受理点进行管理，包括进行服务资质审核和

规范执行检查。SRCA 具有对所有证书服务申请者服务请求的最终处理权。SRCA 有权对申请者的资料进行复查。

受理点 BT 对所有证书服务申请者身份资料的信息核对负有责任，无论这种申请是否被决定受理与否。由于 BT 对申请者的资格审核不严而导致的所有损失，由受理点承担。

4、垫付商的责任

垫付商必须承担其所有垫付的证书费用，并按 SRCA 规定的方式付清。垫付商的垫付行为，就表明其愿意并且能够承担本 CPS 以及 SRCA 相关协议的规定，对证书服务申请者的身份真实性提供担保的责任。

5、证书申请者的责任

证书申请者必须严格遵守与证书申请以及私钥的所有权和安全保存相关的规范。证书申请者承诺，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，可供发证机构检查和核实；证书申请者应承担任何因提供虚假信息、伪造信息等行为引起的法律责任。由于证书申请者自身原因导致发证机构无法正确为其签发证书的，由申请者自行承担有关损失和责任。

证书申请者必须仔细阅读和理解本 CPS 的内容或者由 SRCA 推荐或使用的安全措施，以充分了解私钥保存的重要性，确保私钥的安全。证书申请者在申请、接受证书及其相关服务前，需要熟悉本 CPS 的条例和与证书相关的政策、法规等，SRCA 在接到证书申请者的任何服务申请前，都认为该持有人已经了解本 CPS 的内容，并承诺遵守证书持有者证书使用方面的有关限制。

SRCA 一旦通过证书申请者的申请并为其签发证书，无论是否已经获得证书，该证书申请者自然成为证书订户。

订户必须保证私钥的安全。SRCA 只是告知，但并不要求证书申请者一定遵从 SRCA 提出的安全措施；订户可以选择任何自己认为可以保密的所有措施；同时，SRCA 声明，SRCA 并不承担因订户的私钥保存出现问题而带来的所有责任,除非订户能够合法的证明这种问题产生的主要责任在 SRCA。

6、证书应用行业组织的责任

（1）证书应用行业组织承担证书订户对所在行业是否具有应用权限的审定,并承担相应的责任；

（2）根据具体应用的不同,证书应用行业组织可以根据协议对行业订户身份的真实性进行审查,并承担相应的责任；

（3）证书应用行业组织不承担要求行业用户接受 SRCA 证书成为 SRCA 证书订户的责任。

7、依赖方的责任

依赖方在信赖任何 SRCA 签发的证书时，必须保证遵守和实施以下条款：

（1）依赖方熟悉本 CPS 的条款以及和证书相关的政策、法律，了解证书的使用目的和使用限制；

（2）依赖方在信赖 SRCA 签发的证书前，必须对其进行合理的审查，包括但不限于：查看证书是否在有效期内；检查 SRCA 公布的有效 CRL，以获得该证书的状态。SRCA 认为，依赖方一直是遵循了此条款的。一旦依赖方因为疏忽或者其他原因违背了此条款，所带来的损失由其自身承担。如给 SRCA 带来损失时，SRCA 保留采取相应法律行为的权利；

（3）所有依赖方必须承认，他们对证书的信赖行为就表明他们承认、了解本 CPS 的有关条例，包括有关免责、拒绝和限制义务的条款。

4.2 证书申请审核

4.2.1 执行识别与鉴别功能

SRCA 在办理证书申请注册手续时，将严格执行用户身份识别和鉴别。具体的鉴别流程详见 3.2.2 组织机构身份的鉴别和 3.2.3 个人身份的鉴别。SRCA 将严格核对用户提供的各类证件，在确认无误后进行业务处理，并将妥善保存用户提供的各类证明材料和用户证书申请表。

在证书签发后，SRCA 除非被通知该证书发生了本 CPS 所述的安全损害情况，SRCA 不负有监控和调查证书中信息准确性的责任。

4.2.2 证书申请审核流程

SRCA 收到申请者的申请后，对申请信息及身份资料进行审核，准确无误后批准。如申请者未能成功通过鉴别，SRCA 将拒绝证书申请，并通知申请者鉴别失败。对于鉴别失

败的原因，SRCA 有权拒绝解释，并且不需要通知申请者，法律法规对此有明确要求的除外。如果是由于第三方信息而导致身份鉴别失败，SRCA 将向申请者提供第三方的联系方式，以便申请者查询。SRCA 采用合理的方式来通知证书申请者其证书申请失败。

SRCA 可以根据其独立判断，拒绝为某一申请者签发证书，不需要为此做出解释，并且不对因此而导致的任何损失或费用承担责任和义务。除非证书申请者提交了欺骗性的或伪造的信息，在拒绝签发证书后，SRCA 将归还证书申请者所付的证书购买费用，证书申请者支付的邮递费、材料费等事先发生的费用除外。被拒绝的证书申请者可随后再次提出申请。

4.2.3 处理证书申请的时间

SRCA 将在接受用户申请 5 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。

受理点能否在上述时间期限内更快地处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了 SRCA 的管理要求。

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

证书申请者一旦提交了申请，尽管事实上还没有获得证书，仍被视为该订户已同意 SRCA 签发其证书。

注册机构下属的受理点 BT 对证书申请者身份审核通过以后，通过安全方式将用户证书 DN 信息以及公钥发送到 SRCA 证书签发系统。

证书签发系统对 RA 提交的用户 DN 信息以及公钥按 X.509 证书格式标准组织并签发数字证书，然后发送到 RA 处。所签发的证书通过 LDAP 方式发布。证书的发布意味着 SRCA 最终完全正式地批准了证书申请。RA 将签发成功的数字证书在规定时间内发放给用户。

4.3.2 电子认证服务机构和注册机构对订户的通告

SRCA 数字证书由中铁 CA 中心统一申请、发放，并且存储于证书载体 UKEY 中或根据证书申请者的要求存储于其它安全存储介质，由证书申请者填写或监督 SRCA 工作人员

填写申请信息，证书签发成功后将公钥证书存储到证书载体 UKEY 或其它安全存储介质中，并根据与证书申请者约定的方式交付。

SRCA 不提供上门为订户安装证书的服务。如果证书申请者需要，SRCA 可以上门安装，但需要收取相应的服务费用。SRCA 和其授权的证书服务机构提供热线支持服务。联系方式由 SRCA 及其授权的证书服务机构的网站公布。

4.4 证书接受

4.4.1 构成证书接受的行为

证书申请者在向 SRCA 成功提交证书申请后，从证书签发起就被视为已同意接受证书。

证书存储于证书载体 UKEY 中的，采取当面交付或顺丰、EMS 快递实名寄送的交付方式。

证书存储于其它安全存储介质中的，如移动终端、PC 终端，根据与证书申请者约定的方式交付。

SRCA 证书订户在获得证书后，请详细查看证书主体项信息及其它标识内容，绑定相应的铁路行业信息系统，如有问题可以在 5 个工作日之内与 SRCA 联系解决。订户接受数字证书后，应妥善保存与其证书对应的私钥。

4.4.2 电子认证服务机构对证书的发布

SRCA 将在其信息库、目录服务中发布证书的副本。SRCA 可以决定在其它信息库里发布证书的副本。订户也可以在其它场所公布他们的证书。订户、依赖方可以通过证书目录服务方式下载自己或他人的证书。

4.4.3 电子认证服务机构对其他实体的通告

订户接受证书后，SRCA 将不专门对注册机构、受理点、主管部门等实体进行专门的通告，这些实体可以通过目录服务或者查询 SRCA 信息库来获得订户的证书及相关信息。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户使用证书时，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。任何人使用证书时都必须检验证书的有效性。包括该证书是否被撤销、是否还在有效期内、是否是 SRCA 签发等。

在使用与 SRCA 所签发的证书有关的签名及经过签名的信息时，参与方（SRCA、证书订户和依赖方等）按本 CPS 的规定享有相应的权利和应尽的义务。

参与方均视为已被通知并同意遵守本 CPS 以及 SRCA 与各方签署的协议、规范中的条款。拒绝任何超出本 CPS 的规定的证书及私钥的使用。

SRCA 签发的各类证书，仅用于 SRCA 证书策略中规定的应用范围内使用私钥和证书，否则，其应用是不受相关法律和 SRCA 证书策略保障的。

SRCA 签发的证书中可以明确证书的使用范围和用途，例如证书策略对象标识符(OID)，这个标识符可以决定在一个特定应用中是否可以信任某一个证书，那么该证书将在也只被允许在这一范围内使用。

证书的应用范围：

证书类型	应用范围类型	订户私钥与证书的用途
个人证书	个人安全电子邮件证书	个人安全电子邮件安全证书中包含订户的电子邮件地址、公钥及SRCA的签名。使用安全电子邮件证书的订户可以收发加密和数字签名邮件。
	个人身份证书	个人身份安全证书中包含证书持有者的个人身份信息、公钥及SRCA的签名，在网络通讯中标识证书持有者的个人身份，可以用于个人在网上进行合同签定、定单、支付等各类活动中标明身份。
	个人代码签名证书	个人代码签名证书是CA中心签发给独立软件编写人员的数字证书，包含软件提供者的身份信息、公钥及SRCA的签名。
单位证书	企业或机构安全电子邮件证书	单位电子邮件安全证书中包含订户的电子邮件地址、公钥及SRCA的签名。使用安全电子邮件证书的订户可以收发加密和数字签名邮件。

	企业或机构身份证书	单位身份安全证书中包含单位信息、公钥及SRCA的签名，在网络通讯中标识证书持有单位的身份。
	法定代表人证书	法定代表人证书是用来表明证书持有者是单位的法定代表人，在网络通讯中标识单位法定代表人的身份，包含证书持有者的身份信息、公钥及SRCA的签名。
	企业或机构代码签名证书	企业代码签名证书是CA中心签发给软件提供商的数字证书，包含软件提供商的身份信息、公钥及SRCA的签名。
设备证书	服务器证书	服务器证书中包含服务器信息、公钥及SRCA的签名，在网络通讯中标识和验证服务器的身份。在网络应用系统中，服务器软件利用证书机制保证与其他服务器或客户端通信的安全性。
	网关证书	支付网关、VPN网关证书中包含网关信息、公钥及SRCA的签名，在网络通讯中标识网关服务器的身份。
	SSL证书	SSL证书中包含域名、IP信息公钥及SRCA的签名。
	应用系统证书	应用系统证书包含应用系统名称及其它标识信息、公钥及SRCA的签名。
	终端设备证书（移动终端、PC终端等）	终端设备证书中包含该终端的主体标识信息、公钥及SRCA的签名。
	物联网设备证书	物联网设备证书中包含该设备的主体标识信息、公钥及SRCA的签名。
事件型证书	事件型证书	事件型证书中包含业务场景的相关数据信息、公钥及SRCA的签名。

4.5.2 签名及验证

签名只限于满足以下的条件才能被创建：

（1）在证书的使用有效期内被创建；

（2）该签名能通过对证书链的确认来正确验证；

（3）依赖方没有发现或注意到签名者违背本 CPS 要求的行为；

（4）签名方和依赖方遵守本 CPS 的所有规定；

证书的使用并不表示订户一方可以按任何个人的利益而行事或者有采取任何特殊行为的权利。

进行签名的验证是为了确认签名是用签名者证书中所列的公钥相对应的私钥创建的，以及该签名创建后被签名的信息没有被更改过。验证证书的有效性包括三个方面的内容：

（1）用 SRCA 的证书验证证书中的签名，确认该证书是 SRCA 签发的，并且证书的内容没有被篡改。

（2）检验证书的有效期，确认该证书在有效期之内。

（3）查询证书状态，确认该证书没有进入 CRL(证书黑名单)。

在验证电子签名时，依赖方应准确知道什么数据已被签名，在公钥密码标准中，标准的签名信息格式能够准确表示签名过的数据。

4.5.3 依赖方公钥和证书的使用

在信任证书和签名前，依赖方要独立地做出应有的努力和合理的判断。除非本 CPS 另有规定，证书并不是来自发证机构的对任何权利或特权的承诺。依赖方在本 CPS 规定的范围内信赖证书和证书中包含的密钥，并对此做出决定。

SRCA 签发的证书中可以在某些字段明确证书的使用范围和用途,这些应用在 SRCA 的证书策略中规定，那么该证书将在也只被允许在这一范围内进行使用。当依赖方接受到经数字签名的信息后，应该，

① 获得数字签名对应的证书及信任链。

② 确认该签名对应的证书是依赖方信任的证书，并验证其证书的有效性。

③ 证书的用途适用于对应的签名。

④ 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。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。依赖方应将加密证书连同加密信息一起发送给接受方。

4.6 证书更新

证书更新指 SRCA 在不改变证书中订户的公钥或其他任何信息的情况下，为证书订户签发一张新证书。遵从国家相关法律、法规和管理规定，原则上订户证书更新应按照密钥更新的办理方式完成证书更新。

4.6.1 证书更新的办理方式

SRCA 提供现场更新和在线更新两种办理证书更新的方式：

4.6.1.1 现场更新

在证书有效期到期前到 SRCA 受理点现场提交纸质更新申请材料并办理证书更新。

4.6.1.2 在线更新

在 SRCA 数字证书在线证书受理网站提交证书更新申请并同时邮寄纸质更新申请材料至 SRCA 受理点进行线下审核，根据审核通过后用户方可在线自行下载更新后的数字证书（网址详见中铁 CA 网站 www.sinorailca.com,“自助在线更新服务”）。

4.6.2 证书更新的情形

当证书持有者的证书有效期到期前，SRCA 将作出合理的努力，在证书有效期满之前向证书订户或者证书垫付商发送证书更新提示。合理的努力包括但不限于网站提示、系统提示、书面提示、电子邮件通知或者其它方式，SRCA 采取了上述任意一项提示或者通知方式，均可被视作进行了合理的努力。一般地，证书订户应在证书到期前一个月内提出更新申请。特殊情况下，在证书到期后的一个月内提出申请并补交当月的服务费用方可进行更新。

4.6.3 请求证书更新的实体

任何合法持有有效期限未到的 SRCA 证书的订户均可向 SRCA 申请更新持有的证书。

4.6.4 证书更新请求的处理

订户在申请更新证书时，由 SRCA 所属受理点根据申请更新的证书种类，发放相应的“数字证书申请（更新）表”，订户填写完毕依据申请表缴纳相应的费用；受理点根

据申请表进行证书更新具体工作；订户凭申请表“用户联”、交费单据领取更新后的证书。

订户在申请办理更新证书时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件，并按时缴纳相应费用。

4.6.5 证书更新的注意事项

请订户在进行证书更新之前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）。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，SRCA 概不负责。

4.6.6 颁发新证书时对订户的通告

SRCA 会在订户提交证书更新申请时告知其领取新证书的时间和地点。在订户获得更新证书时自动通知或面对面告知新证书已颁发。

4.6.7 构成接受更新证书的行为

需要证书更新的订户在向 SRCA 成功提交证书申请后，新证书被签发意味着订户已经接受了证书。订户凭证书更新申请表、交费单据领取更新后的证书，订户领取数字证书后，请详细查看证书及其内容，如有问题可以在 5 个工作日之内与 SRCA 联系解决。

4.6.8 电子认证服务机构对更新证书的发布

一旦订户接受更新证书，SRCA 将在其信息库、目录服务中发布证书的副本。SRCA 可以决定在其它信息库里发布证书的副本。订户也可以在其它场所公布他们的更新证书。

4.6.9 电子认证服务机构对其他实体的通告

订户接受更新证书后，SRCA 将不专门对注册机构、受理点、主管部门等实体进行通告，这些实体可以通过目录服务或者查询 SRCA 信息库来获得订户的更新证书及相关信息。

4.7 证书密钥更新

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。由于技术的不断更新，为了加密的安全性，SRCA 可以要求订户更新证书的密钥。

最终订户的私钥有效期一般均与其证书的有效期一致。但对于 CA 的签名密钥而言，私钥的有效期都应比其证书有效期短。其原因是为了防止电子认证服务机构签发的证书出现刚签发不久即失效的情况。

4.7.1 证书密钥更新的情形

如果出现下列情形，订户必须进行证书密钥更新:

（1）证书到期并且密钥对的使用期也到期；

（2）证书密钥对已经或怀疑被泄露、被窃取、被篡改或者其它原因导致的密钥对安全性无法得到保证；

（3）证书被撤销后需要重新获得证书；

（4）凡是在 SRCA 内部使用的证书，包括 RA、服务操作人员等的证书，到期时，必须进行证书密钥更新。

4.7.2 请求证书密钥更新的订户实体

任何合法持有有效期限未到的SRCA证书的订户均可向SRCA申请更新持有的证书密钥。

4.7.3 证书密钥更新请求的处理

订户在申请证书密钥更新时，由 SRCA 所属受理点根据申请密钥更新的证书种类，发放相应的“数字证书申请（更新）表”，订户填写完毕依据申请表缴纳相应的费用；受理点根据申请表进行证书密钥更新具体工作；订户凭申请表“用户联”、交费单据领取密钥更新后的证书。订户在申请办理证书密钥更新时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件，并按时缴纳相应费用。

4.7.4 密钥更新的注意事项

请订户在进行密钥更新之前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）。以上操作完成后才能进行密钥的更新。 如订户未解密文件而进行证书更新，由此造成的可能损失，SRCA 概不负责。

4.7.5 颁发新证书时对订户的通告

SRCA 在颁发新证书时对订户的通告同 4.6.6。

4.7.6 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同 4.6.7。

4.7.7 电子认证服务机构对密钥更新证书的发布

SRCA 对密钥更新证书的发布同 4.6.8。

4.7.8 电子认证服务机构对其他实体的通告

SRCA 对其他实体的通告同 4.6.9。

4.8 证书变更

在证书有效期内，当订户信息发生变化时，订户应进行证书变更，申请签发新的证书。SRCA 在对申请者递交的资料进行鉴别确认后，将为其重新签发证书。

4.8.1 证书变更的情形

证书变更指改变证书中订户信息而签发新证书的情形。当订户实体身份信息发生改变，而影响证书项内容时，证书订户有义务向 SRCA 报告并申请证书变更，将证书撤销后重新签发证书。

4.8.2 请求证书变更的订户实体

请求证书变更的订户实体同 4.6.3。

4.8.3 证书变更请求的处理

订户在申请证书变更时，由 SRCA 所属受理点根据申请更新的证书种类，发放相应的“数字证书申请（更新）表”，订户填写完毕依据申请表缴纳相应的费用；受理点根据申请表进行证书变更具体工作；订户凭申请表“用户联”、交费单据领取变更后的证书。

订户在申请办理证书变更时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件，并按时缴纳相应费用。

4.8.4 证书变更的注意事项

证书变更后，证书的有效期并没有改变，仍然为原证书有效期。其他注意事项同 4.6.4。

4.8.5 证书变更时对订户的通告

SRCA 在颁发新证书时对订户的通告同 4.6.6。

4.8.6 构成接受变更证书的行为

正式接受变更证书的行为同 4.6.7。

4.8.7 电子认证服务机构对变更证书的发布

SRCA 对变更证书的发布同 4.6.8。

4.8.8 电子认证服务机构对其他实体的通告

SRCA 对其他实体的通告同 4.6.9。

4.9 证书撤销和挂起

订户、电子认证服务机构、国家法律部门或者政府公共权力部门等可以要求将证书撤销或者挂起。

4.9.1 证书撤销的情形

证书撤销分为主动撤销和被动撤销，主动撤销是指订户主动申请撤销其数字证书，受理点审核申请后撤销其证书。被动撤销是指电子认证服务机构确认用户违反 CPS 规则内容申请使用证书、证书主体消亡、私钥泄漏或遗失 UKEY 等风险情况的发生，则撤销数字证书。

一、证书有效期内，如果出现下列情况（包括但不限于下列情况），SRCA 可以直接将证书予以撤销：

1、由于证书管理系统的不适用或者证书系统的整合需要；

2、由于证书订户未能履行与各参与方之间的协议（如未缴纳费用等）而被这些有权力主张撤销的实体提出；

3、由于证书的不当使用而违反国家的法律法规及本 CPS 规定的主要和重要义务；

4、政府公共权力部门或者国家法律部门依照正式合法的程序提出申请；

5、订户申请证书服务时，提供不真实或者欺骗性材料的；

6、发现并证实其证书没有根据本 CPS 要求的程序而签发的；

7、电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因的；

8、证书的私钥丢失、被盗、被篡改、被未经授权泄露或被损坏；

9、由于不可抗力、自然灾害、计算机或通信故障、法律法规的修改、政府行为（包括但不限于出口控制管理部门的限制行为）或其它超出人力合理控制的原因，拖延或阻止了订户责任的执行。

二、证书在有效期内，如果出现下列情况，订户必须提出撤销请求：

1、与证书中的公钥相对应的私钥被泄密、被窃取、被篡改或者其它原因产生对私钥的安全性顾虑；

2、证书中的订户相关信息发生变更而申请证书变更时；

3、由于证书不再需要用于原来的用途而要求终止；

4、证书中的相关内容和申请时提交申请材料不一致；

5、证书持有者已经不能履行或违反了本 CPS 或其它协议、法规及法律所规定的责任和义务。

三、其它 SRCA 认为可以进行撤销的原因。

四、SRCA 没有义务一定要公开某一张证书被撤销的原因。

4.9.2 请求证书撤销的实体

能够要求撤销证书的实体包括：

1、自己支付证书费用的证书订户；

2、垫付商或垫付商型证书服务机构；

3、经证书持有者合法授权的代表；

4、电子认证服务体系内的各个机构；

5、国家法律部门、政府主管部门及其他公共权力部门。

4.9.3 撤销请求的流程

SRCA 在主动发现订户证书符合强制撤销条件，则提出申请及书面证明材料，并进行归档，在签署强制撤销命令后 24 小时内撤销订户证书。强制撤销订户证书前，SRCA 没有必要通知订户，但在强制撤销后，应在 5 个工作日内以电话、传真、网站公告或电子邮件等形式之一通知订户。

政府公共权力部门也可以提出撤销证书请求，必须按照规定出具书面证明材料，填写撤销申请表并签字盖章。SRCA 在审核材料通过后 24 小时内撤销证书，在 5 个工作日内以电话、传真、网站公告或电子邮件等形式之一通知订户。

主动撤销的流程如下：

1、证书订户（或者其授权的委托代理人）书面填写申请表并签字盖章，向 SRCA 进行撤销申请，同时提交合法的证明材料。

2、SRCA 收到撤销申请后，验证申请者的身份、权限和撤销理由的正当性，并对审核资料进行书面归档，验证确定无误后作出撤销决定并及时处理。

3、SRCA 在 24 小时内将证书撤销信息发布到信息库和目录服务，以供查询。

4.9.4 撤销请求宽限期

一旦发现需要撤销证书，订户应该实时提出撤销请求，如果确实因为客观原因导致延迟的，这个时间也不得超过 8 个小时。

SRCA 在应该撤销证书的情况下强制撤销订户证书，强制撤销立即生效，订户不能请求宽限。

4.9.5 电子认证服务机构处理撤销请求的时限

SRCA 从接受完整的撤销请求资料到完成审核,作出撤销决定并将撤销证书发布到目录服务器，应当在 24 小时内完成。

4.9.6 依赖方检查证书撤销的要求

证书撤销列表 CRL 作为公开的信息，没有读取权限的安全设置，依赖方可以自由的根据需要进行查询。依赖方在信赖证书前，应根据 SRCA 最新公布的 CRL，主动检查该证书的状态。同时，还需要验证 CRL 的可靠性和完整性，确保它是经过 SRCA 发布、包含 SRCA 的数字签名的。

4.9.7 CRL 发布频率

CRL 是 SRCA 提供的证书发布服务之一，订户可以访问 CRL 验证证书当前状态。为了保证至少 24 小时内发布 CRL 一次，SRCA 的 CRL 采用每 8 小时更新一次的策略。根据情况，SRCA 可以自主决定缩短产生和更新 CRL 的时间。

4.9.8 CRL 发布的最大滞后时间

CRL 一般在批准撤销请求后 24 小时内生效。特殊紧急情况下可以立即生效（不考虑网络传输条件的影响，因为网络因素造成的时效差异是被允许的）。生效表示 SRCA 将在 CRL 中公布被撤销的证书。

SRCA 承诺，在证书撤销后，最晚也将在撤销行为发生的 24 小时内发布证书撤销列表。

4.9.9 在线状态查询的可用性

SRCA 提供 7X24 小时 LDAP 目录查询服务。并提供了 OCSP 作为可选的在线状态无偿查询方式。

4.9.10 在线状态查询要求

在线状态查询可以通过证书序列号、证书主题等信息对证书的实时状态进行查询。

4.9.11 撤销信息的其他发布形式

OCSP 作为可选的无偿的撤销信息发布形式。

4.9.12 密钥损害的特别要求

当 SRCA 的根密钥损害发生时，SRCA 将主动地即时撤销证书，并实时把证书发布到 CRL。SRCA 承担因密钥损害给订户造成的损失，并及时为其签发新的证书。

4.9.13 证书挂起的情形

当证书仍处于有效期，为了保留订户的证书使用权利，而不申请撤销该证书，当出现下列情况时，可以进行证书挂起：

1、证书订户要求暂停使用该证书一段时间；

2、订户未能履行与 SRCA 签订的协议中应尽的义务，但向 SRCA 提出申请并获得批准后；

3、除证书订户（或者其授权的委托代理人）外的其它实体，如电子认证服务机构及其授权的服务机构、国家法律部门、政府主管部门及其他公共权力部门。向 SRCA 提出挂起证书请求并获得批准。

4.9.14 证书挂起的订户实体

只有证书订户实体或者其授权的委托代理人，以及电子认证服务机构及其授权的服务机构、国家法律部门、政府主管部门及其他公共权力部门等，才有权力提出证书挂起的请求。

4.9.15 证书挂起和解挂的流程

订户在申请证书挂起和解挂时，由 SRCA 所属注册机构、受理点根据申请变更的证书种类，发放相应的申请表，订户填写完后依据申请表缴纳相应的费用；注册机构根据申请表进行证书挂起或解挂等制作工作。订户在申请办理证书挂起或解挂时，有责任在

证书申请中提供准确有效的信息，提供相关的证明文件，并按时缴纳相应费用。除证书订户以外的其它实体，如 SRCA 的授权机构、国家法律部门、政府公共权力部门等，提出证书挂起请求，也需按规定填写申请表并提交证明材料。

SRCA 审核通过挂起请求后，应在 24 小时内办理挂起操作。强制挂起的订户证书，需在 5 个工作日内通过电子邮件、电话、传真或网站公告等方式通知订户。如订户需解挂，需按相关法律法规提交证明材料，证明该证书的合法性等原始状态，SRCA 才能按照规定程序办理解挂手续。

4.9.16 挂起的期限限制

证书挂起后，如订户没有在规定时间内申请解挂、撤销或恢复等其他证书相关业务，SRCA 将对该证书做解挂处理，请订户注意及时撤销、恢复或解挂证书。

如订户没有及时处理，由此造成的可能损失，SRCA 概不负责。证书挂起的最长时间是 6 个月，如果没有接到合法的撤销通知，该证书将被解挂。如证书挂起时间内到达有效期，SRCA 将废除该证书。

4.10 证书状态服务

4.10.1 操作特征

SRCA 证书和 CRL 发布于支持 LDAP 协议标准的目录服务器中，为订户提供证书状态服务。证书和 CRL 的查询通过 LDAP 协议实现。证书由签发服务器发布到系统的主目录服务器上，并通过目录服务器的自动映射功能，将证书映射到从目录服务器中，供用户查询和下载。用户需要将 CRL 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。

4.10.2 服务可用性

SRCA 提供 7X24 小时的证书状态查询服务。

若由于不可预测原因造成通过目录服务无法进行查询，则 SRCA 将在 48 小时之内，通过查询 CA 数据库中证书状态信息发布到 SRCA 网站上。

4.10.3 可选特征

根据订户的要求，在请求者支付相关费用后，可以由 SRCA 查询 CA 数据库中证书订户的状态并将之通知订户。也可以在指定的证书被撤销时，为请求者提供付费的通知服务。

4.11 订购结束

证书已经到期，在用户不声明继续使用认证服务的情况下，视为用户终止订购，SRCA 或授权受理点可撤销该用户证书。

证书未到期，用户声明不继续使用 SRCA 认证服务，SRCA 授权受理点将根据用户要求撤销或挂起该用户数字证书。用户申请撤销或挂起证书时，填写申请表（一式三份），SRCA 授权受理点按照 4.9.3 的撤销流程或 4.9.15 的挂起流程进行批准或拒绝的操作，证书在有效期内被撤销后，即订购结束。

证书未到期，政府公共权力部门提出撤销证书要求，按照规定出具书面证明材料，填写撤销申请表并签字盖章。SRCA 在审核材料通过后 24 小时内撤销证书，证书在有效期内被撤销后，即订购结束，SRCA 在 5 个工作日内以电话、传真、网站公告或电子邮件等形式之一通知订户。

4.12 密钥生成、备份与恢复

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，确保密钥对的生成、传送、安装等具备保密性、完整性和不可否认性。证书用户的加密密钥对是由中铁 KMC 负责生成的，其生成、备份和恢复策略由该机构自行决定。

签名密钥对由客户端生成，证书申请者使用国家密码管理局认可的 SRCA 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，保证签名密钥对无法复制。

4.12.1 密钥生成、备份与恢复的策略与行为

订户的签名密钥对在订户持有或指定的证书载体中产生,证书载体包括但不限于智能密码钥匙 UKEY、密码设备、密码模块。订户加密证书密钥由中铁 CA 密钥管理中心（以下简称中铁 KMC）系统集中安全产生和保存。

事件型证书的签名密钥由签名设备生成密钥并执行签名后，即时销毁。

密钥恢复是指订户加密密钥对的恢复,密钥管理中心不负责签名密钥对的恢复。密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

1）证书持有人提出申请；

2）注册机构 RA 提出申请，并有充分的理由；

3）国家执法、司法机构因执法、司法的需要；

4）国家其他管理部门管理需要。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

密钥恢复分为两类：用户密钥恢复和司法密钥恢复。

用户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在注册机构申请，提交有关文件及材料且审核通过后，CA 向密钥管理中心请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并存储于订户证书载体中。

司法密钥恢复：司法取证人员在密钥管理中心申请，提交有关文件及材料且审核通过后，由密钥恢复模块恢复所需的密钥并记录于指定的载体中。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，中铁 CA 不对其进行保存和恢复。

5.认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

SRCA 的建筑物和机房建设按照下列标准实施：

（1）GB 50174—93《电子计算机机房设计规范》

（2）GB 2887—89《计算站地技术条件》

（3）GB 9361—88《计算站场地安全要求》

（4）GB 6650—1986《计算机机房用活动地板技术条件》

（5）GB 50034—1992《工业企业照明设计标准》

（6）GB 5054—95《低匹配电装置及线路设计规范》

（7）GBJ 19—87《采暖通风与空气调节设计规范》

（8）GB 157《建筑防雷设计规范》

（9）GBJ 79—85《工业企业通信接地设计规范》

SRCA 机房位于北京市西城区马连道南街 2 号院 1 号楼 2 层。实行分区访问的安全管理，SRCA 的功能区域划分为制证室、办公区、机房区域。

5.1.2 物理访问

通过门禁控制系统为人员分配相应的权限，决定人员出入是否被准许。运维人员进入机房履行登记手续后通过刷门禁卡进入机房，进入核心区人员应通过门禁和生物识别双人双因素方式进入。非运维人员进入机房时，履行登记手续，由机房场地管理人员陪同进入，机房各区域配有 24 小时视频监控设备。

5.1.3 电力与空调

机房供电按照负荷要求，选用相应线径的供电电缆和不同容量的电源滤波器。多处采用低泄漏电流的电源滤波器，达到插入衰减能力与屏蔽室综合效能一致的效果。

采取三相供电方式供电。机房采用一台在线式 UPS，UPS 接有备用电池组，当市电断电后由电池组给 UPS 供电，市电供电与电池组供电为零秒切换，确保在电源切换过程计算机不丢失数据。

机房空调采用高效能、高灵敏度的空调系统，辅助以通风、加湿等措施，控制运营设施中的温度和湿度，保证了系统正常运行。

5.1.4 水患防治

机房在建设中已采取相应措施，防止漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

5.1.5 火灾防护

SRCA 消防报警系统设计依据 GBJ116-88《火灾自动报警系统设计》进行设计。系统通过设置在机房的温感、烟感探头采集消防数据，提供系统实时处理火灾自动报警终端的报警数据和系统运行状态数据。系统管理分手动模式和自动模式两种。

5.1.6 介质存储

SRCA 介质存储符合国家有关管理部门的规定和要求,存有密钥的密码设备放置在有高度物理安全保护和进出安保控制的场地内。接触密钥系统的人员必需经过严谨的背景审查以确保其是可信人员。

5.1.7 废物处理

当 SRCA 电子认证服务系统使用的硬件设备、存储设备、密码设备等废弃不用时，履行设备报废手续后，将按国家的有关规定进行报废处理，其中所涉及敏感性、机密性信息都将被安全、彻底的消除，保证其信息无法被恢复与读取。

当电子认证服务机构保存的相关资料数据已不再需要或存档的期限已满时，SRCA 将在上级部门的组织下统一销毁。

所有处理行为将由至少 2 名人员同时进行，相互监督，处理行为记录在案，并签字确认，以供审查的需要。

5.1.8 异地备份

SRCA 采用异地备份的方式备份至中国铁路总公司主数据中心。

5.2 操作过程控制

5.2.1 可信角色

SRCA 可信角色的定义是“可信角色是指那些已经接受和通过广泛的背景调查，并且调查表明他们有能力维持进行相应职能岗位的 CA 体系关键操作的人员，这些人员包括，但不局限于：客户服务、运行维护和安全管理岗位相关人员”。可信角色策略是人员安全系统的基础。鉴于电子认证服务体系建设的特殊性，必须指定可信的雇员来履行电子认证服务体系相关的安全操作，也就是说，所有有权访问敏感操作的工作人员必须是值得信任的人员。

一般来说，可信雇员包含但不限于下述人员：

（1）有权访问电子认证服务系统；

（2）有权访问保险柜的组合和/或保险箱的密钥；

（3）有权访问安全敏感材料；

（4）鉴定和批准证书请求以及发布证书；

（5）授予物理和/或逻辑访问权力。

除此以外，那些被分配到高级行政级别的相关人员也应该属于可信人员。SRCA 根据本 CPS 和授权协议，制订其授权的证书服务机构（RA、BT 等）的管理规范，规范管理人员、操作人员的操作。在与此相关的软件设计中，充分考虑安全的牵制和约束。SRCA 对其授权的证书服务机构的责任进行合理划分，并在系统和技术实现以及管理的责任义务上进行保证。

5.2.2 每项任务需要的人数

SRCA 确保单人不能接触、导出、恢复、更新、废止 SRCA 存储的根证书对应的私钥。至少三人，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 CA 密钥生成、恢复的操作。

SRCA 对与运行和操作相关的职能有明确的分工，贯彻互相牵制、互相监督的安全机制。

5.2.3 每个角色的识别与鉴别

所有 SRCA 的在职人员，必须通过认证后，根据作业性质和职位权限的情况，发放需要的系统操作卡、门禁卡、登录密码、操作证书、作业帐号等安全令牌。对于使用安全令牌的员工，SRCA 系统将独立完整地记录其所有的操作行为，所有 SRCA 关键职位人员必须确保：

（1）发放的安全令牌只直接属于个人或组织所有；

（2）发放的安全令牌不允许共享；

（3）SRCA 的系统和程序通过识别不同的令牌，对操作者进行权限控制。

5.2.4 需要职责分割的角色

对于证书服务的受理，必须通过录入员、审核员两个角色同时进行才能完成。对于根密钥的操作，必须有三名根密钥管理员同时到场，才能进行有关的操作。SRCA 在系统遇到紧急情况需要联合抢修时，必须报安全策略委员会，经同意后，应至少有一名安全策略委员会指定人员在场，抢修人员在该人员的陪同监督下执行许可的操作，所有操作、修改都保留记录。

非 SRCA 员工因物理修理、消防、强电故障等情况，需要进入 SRCA 数据中心实施修理时，必须报安全策略委员会，经同意后，首先认证修理者的身份，然后由一名安全策略委员会指定人员始终陪同和监护，完成约定部位的修理。

5.3 人员控制

5.3.1 资格、经历和无过失要求

SRCA 员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工。

新入职员工通过考察期后，根据考察的结果进行相应的工作安排。SRCA 根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。SRCA 会对其关键岗位的员工进行严格的背景调查。注册机构、受理点操作员的审查可以参照 SRCA 对可信任员

工的考察方式。注册机构、受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背 SRCA 证书受理的规程和 SRCA CPS。

5.3.2 背景审查程序

对所有需要成为可信角色的人员，需要对其进行调查，背景调查包括对先前就业的核实；对所获得的最高学位的核实；犯罪记录调查(当地、省，以及全国)。

所有员工与 SRCA 签定保密协议，受到合同和章程的约束，不得泄露 SRCA 证书服务体系的敏感信息。

SRCA 根据需要，可与有关的政府部门和调查机构合作，完成对 SRCA 可信任员工的背景调查。

5.3.3 培训要求

SRCA 对员工进行以下内容的综合性培训：

（1）SRCA 安全策略；

（2）SRCA 使用的软件介绍；

（3）SRCA 操作的系统和网络；

（4）SRCA 岗位职责；

（5）SRCA 政策、标准和程序；

（6）相关法律、仲裁规则、管理办法等。

5.3.4 再培训周期和要求

根据 SRCA 策略调整、系统更新等情况，SRCA 将对员工进行继续培训，以适应新的变化。每年至少进行一次相关技能和知识培训。

5.3.5 工作岗位轮换周期和顺序

在 SRCA 负责系统运行和负责 CA 系统设计、开发、维护的员工承担不同的职责，双方的岗位互相分离。

为了配合认证系统的运营需要和岗位适应性的需要，SRCA 可能会选派适当的人选，在不同的岗位进行轮换。这种轮换不得和前面的岗位分离原则相违背。

5.3.6 未授权行为的处罚

当 SRCA 员工进行了未授权或越权操作时，SRCA 在确认后立即中止该员工进入电子认证服务体系。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，SRCA 立即作废或终止该人员的安全令牌和对应的权限。

5.3.7 独立合约人的要求

SRCA 因为人力资源不足或者特殊需要，聘请专业外包人员参与系统运作，除了必须就工作内容签署保密协议以外，该独立合约人的权利和职责与内部可信员工的相同。同时还必须对其进行职务上的技能知识培训和规范培训，使其能够严格遵守 SRCA 的规范体系的要求。

5.3.8 提供给员工的文档

SRCA 的员工可以查看 CA 系统的相关硬件、软件以及应用程序的技术手册，同时员工也可以查看 SRCA 的业务流程介绍和证书策略。

5.4 审计日志程序

安全审计服务是 SRCA 系统服务的重要组成部分，它为及时发现认证服务系统自身安全隐患和非法操作，事后的漏洞弥补、系统加固、系统运营状况审查、事故调查取证等提供一个可靠的服务平台。

5.4.1 记录事件的类型

SRCA 架构内的证书服务机构，必须记录与 CA 和 RA、受理点运行系统相关的事件。这些记录应包含事件内容、事件发生的时间和事件相关实体。

（1）证书订户服务流程中产生的信息数据和资料，如申请表、协议、身份资料等；

（2）认证系统日常运作产生的日志记录文件；

（3）进出敏感区域的工作记录；

（4）认证机构、注册机构和受理点之间的协议、规范和相关工作记录；

（5）其它按规定需要记录的内容。

5.4.2 处理日志的周期

对于认证系统日常运作产生的日志记录文件，SRCA 采用日志审计系统实时收集并定期归档，统计跟踪观察的结果，如有异常现象形成报告文档报送相关技术部门记录处理。

SRCA 按照内部管理规定，由内部审计人员定期对其他记录，进行核查，并对核查过程中发现的任何异常或警告进行深入调查。核查过程及结果需完整记录。

5.4.3 审计日志的保存期限

SRCA 审计日志每年形成新的归档文件，交由相关部门保存归档，认证系统日常运作产生的日志至少保存到证书信息失效后保存五年。

5.4.4 审计日志的保护

SRCA 执行严格的管理，确保只有 SRCA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

SRCA 保证所有的审计记录和审计检查都按照 SRCA 备份标准和程序进行备份。根据记录的性质和要求，有实时、每天、每周、每月和每年等多种形式的备份，采用在线和离线的各种备份工具。

5.4.6 审计收集系统

SRCA 系统中所有管理操作在各子服务日志数据库中。由于各子服务日志数据库的维护是主动且独立的，不与其他任何模块或子系统发生联系，因此可以保证该日志库的权威性和独立性。

SRCA 审计采集系统由日志审计系统自动采集，涉及：

（1）证书注册管理系统；

（2）证书签发管理系统；

（3）证书目录服务系统；

（4）证书密钥管理系统；

（5）其他 SRCA 认为有必要审查的系统。

5.4.7 对导致事件实体的通告

在认证系统的运行出现影响安全控制措施的事件的时候，必须通知安全策略委员会，并采取有关的应对措施。

SRCA 对审计中发现的违反服务受理规范、系统运营规范、管理规范的操作事件，根据情节轻重，安全策略委员会决定对导致事件实体采取单独通告、会议通告、警告、处分、开除等措施。

SRCA 对审计中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权力。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。SRCA 有权决定是否通知在审查中发现的攻击者或肇事者。

5.4.8 风险评估

SRCA 对审计过程中发现的一些事件记录为系统的弱点，将对这种事件进行检查后执行安全风险评估。风险评估基于实时的自动记录数据而且根据安全和审计的需求每年对系统进行评估。根据评估结果，随时调整和系统运行密切相关的安全控制措施，以便将系统运作的风险降到最低。

5.5 记录归档

5.5.1 归档记录的类型

SRCA 会对电子认证服务的相关资料定期归档保存，归档的内容包括：

（1）证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议、证书等；

（2）系统运行和认证服务的审计数据；

（3）其他认为有必要归档保存的信息。

5.5.2 归档记录的保存期限

除了法律法规和证书主管机构提出的保存期限以外，SRCA 制订的第三方电子认证服务运营信息的归档保存期限至少应该如下:

（1）电子认证业务规则，用户申请信息表格和相关协议，订户申请、更新、撤销、挂起的证书和过期证书，至少保存到证书有效期结束后 5 年；

（2）证书用户申请、查询、撤销证书的服务记录，至少保存到证书有效期结束后 5 年；

（3）订户证书和密钥的相关变动信息，留存至电子签名认证证书失效后五年；

（4）与法律政策的规定不一致的，选择两者中较长的期限予以保存。

此外，在不违反法律法规和主管部门规定的前提下，SRCA 可以自主决定信息的存档期限，并且不需要对此做出说明和解释。

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接触。SRCA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力的破坏。对于认为必要的资料，SRCA 会采取异地备份的方式予以保存。

SRCA 保存的申请者和订户基本情况资料和身份鉴别资料，除非经过国家法律部、政府主管机构门或其它公共权力部门经过合法的途径予以申请，任意无关的第三方均无法获知。

5.5.4 归档文件的备份程序

存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。SRCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。当认证系统因为异常情况导致无法正常运营时，按照 SRCA 的恢复策略，利用这些归档保存的数据进行系统的恢复。

5.5.5 记录时间戳要求

本 CPS5.5.1 所述的全部存档内容，都有时间标识，比如系统自动记录的时间，或者由操作人员手工标注的时间。

如果有必要，SRCA 会为相关记录加上时间戳服务。

5.5.6 归档收集系统

电子认证服务系统的相关运营信息，全部由 SRCA 内部的工作人员或者具备安全控制措施的内部系统，依照人工和自动操作两部分进行产生和收集。并且由具备相关权限的人进行管理。

5.5.7 获得和检验归档信息的程序

SRCA 每年会按照规定验证存档信息的完整性。归档信息采用在线和离线的两种方式保留两个备份，为了保证归档信息的准确。

5.6 电子认证服务机构密钥更替

SRCA 根证书有效期不超过 20 年。在 SRCA 证书到期之前，SRCA 将对根私钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换过程中起着过渡的作用，旧的 SRCA 证书到期后，SRCA 将用新的 CA 密钥对签发证书。SRCA 密钥更替方式如下:

1）SRCA 根证书到期时间小于订户有效期之前，停止签发新的订户证书；

2)产生新密钥对，签发新的根证书;

3)在旧根证书停止签发之后，将采用新的根密钥签发订户证书;

SRCA 将继续使用旧的根私钥签发的 CRL,直到由旧 CA 根私钥签发的证书到期为止。

5.7 损害和灾难恢复

为了在出现异常或灾难情况时，能够在最短的时间内重新恢复认证系统的运行，SRCA 制订了可靠的损害和灾难恢复计划，以应对突发事故导致的系统问题。

可能造成损害和灾难恢复情况如下：

（1）SRCA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难；

（2）SRCA 根证书被作废；

（3）根私钥被攻破的灾难；

（4）自然灾难或其他灾难。

发生以上损害或灾难，将 SRCA 将按照业务连续性计划实施恢复。

5.7.1 事故和损害处理程序

SRCA 将针对可能出现的事故制定灾难应急计划，事故发生后将依据计划进行处理。灾难应急计划由 SRCA 每年进行风险评估后进行修改与完善。

5.7.2 计算资源、软件和/或数据的损坏

当认证系统运营使用的软件、数据或者其他信息出现异常损毁时，可以依照 SRCA 的系统备份与恢复操作手册，根据系统内部备份的资料，或者异地备份的资料，执行系统恢复操作，使认证系统能够重新正常运行。

当认证系统使用的硬件设备出现损毁时，可以依照 SRCA 的系统备份与恢复操作手册，启动备份硬件设备以及相关的备份操作系统和认证系统，重新恢复系统运行。

5.7.3 SRCA 证书被作废

当 SRCA 证书被作废时，SRCA 应根据本 CPS 相关规定通知证书持有者，证书将被作废。

5.7.4 实体私钥损害处理程序

SRCA 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疑虑时，SRCA 应该：

（1）立即向工业和信息化部和其他政府主管部门汇报，并立即撤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 SRCA 立即生成新的密钥对，并自签发新的根证书；

（2）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；

（3）SRCA 新的根证书签发以后，将会立即通过目录服务器、网站等方式进行发布。

5.7.5 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，SRCA 有能力在灾难发生后的 48 小时内至少恢复以下操作：证书的签发、证书的撤销、发布证书撤销信息、提供密钥恢复信息。

SRCA 计划在异地建立灾难恢复场所，这将进一步提高 SRCA 的灾难后的业务存续能力。

5.8 电子认证服务机构或注册机构终止

5.8.1 电子认证服务机构终止

如果 SRCA 因故计划终止经营，SRCA 会按照相关的法律规定，向工业和信息化部报告，并按照法定程序进行操作，包括：

（1）在法律法规规定的期限前，向工业和信息化部、证书持有者和其他所有相关实体进行通告；

（2）安排业务承接；

（3）保存所有的认证服务相关运营资料，包括证书、用户信息、系统文件、CPS、规范和协议等；

（4）停止有关运营服务；

（5）清除系统根密钥。

5.8.2 RA 的终止根据

当 SRCA 授权的注册机构因故终止服务时，根据 SRCA 与 RA 签订的协议终止 RA（包括其下的受理点 BT）的业务。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

加密密钥对：由中华人民共和国国家密码管理局（以下简称国密局）许可的、SRCA 证书签发系统支持的密码设备生成。中铁 KMC 对密钥生成进行控制管理。

签名密钥对：证书申请者应使用国密局认可的、SRCA 证书签发系统支持的介质生成签名密钥对。签名私钥存储在介质中不可导出，保证无法复制。SRCA 并不承诺接受所有类型的密码产生设备。

服务器证书的密钥对：由订户自己产生，订户应妥善保管。

SRCA 在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 私钥的传递

证书订户的加密私钥是在中铁 KMC 产生的，该私钥只保存在中铁 KMC 和订户介质。在加密私钥从中铁 KMC 到订户的传递过程中采用国密局许可的算法加密,保证了证书订户的密钥安全。

6.1.3 公钥传送给证书签发机构

SRCA 从中铁 KMC 取得订户公钥后为其签发证书,在此过程中也采用国密局许可的算法加密，保证传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

SRCA 的根公钥包含在 SRCA 自签的根证书中。证书订户可以从中铁 CA 网站 www.sinorailca.com 下载 SRCA 根证书。

6.1.5 密钥的长度

密钥算法和长度符合国家密码管理部门的规定。

6.1.6 公钥参数的生成和质量检查

公钥参数的生成和参数质量的检查由国密局鉴证许可、SRCA 证书签发系统支持的硬件进行，这些设备内置的协议、算法等均符合国家密码管理部门的要求。

6.1.7 密钥使用目的

在 SRCA 电子认证服务体系中的密钥用途和证书类型紧密相关。

SRCA 的签名私钥用于签发自身证书、下级证书和所有已签发证书的证书撤销列表（CRL），SRCA 的公钥用于验证 SRCA 私钥的签名。

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；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。签名密钥和加密密钥配合使用，可以实现身份认证、授权管理和责任认定等安全机制。

如果 SRCA 在其签发证书的标准扩展项内指明了证书的用途，证书订户必须按照该指明的用途使用密钥。

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

SRCA 使用国密局许可的产品，密码模块的标准、使用和控制均符合国家密码管理部门的要求。

6.2.2 私钥多人控制

SRCA 的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 张管理员卡中，只有其中三个及以上管理员在场并许可的情况下，才能对私钥进行上述操作。

6.2.3 私钥托管

SRCA 不把根私钥托付给任何第三方组织。

SRCA 订户的签名证书对应的私钥由自己保管，中铁 KMC、SRCA 不进行托管，以保证其不可否认性。中铁 KMC 严格保证用户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

6.2.4 私钥备份

证书订户的签名私钥中铁 KMC 和 SRCA 都不备份。中铁 KMC 备份加密私钥，备份数据以密文形式保存。

6.2.5 私钥归档

中铁 KMC 提供过期的加密私钥的归档服务。

6.2.6 私钥导入、导出密码模块

在 SRCA 电子认证服务体系中，使用 SRCA 的软件可以把订户加密证书的私钥导入密码模块中。私钥无法从硬件及软件密码模块中导出。必须通过口令验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

6.2.7 私钥在密码模块的存储

证书的持有者可以将私钥保存在硬件密码模块中，也可以保存在软件密码模块中。SRCA 的签名私钥必须保存在硬件密码模块中。

6.2.8 激活私钥的方法

SRCA 默认，只有在通过保护密码验证后，订户方可激活其私钥，除非订户自己进行变更，并愿意承担变更后的责任。

6.2.9 解除私钥激活状态的方法

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

订户解除私钥激活状态的方式由其自行决定，例如退出、切断电源、移开令牌/钥匙，自动冻结等。订户必须自行承担其解除私钥激活状态操作的风险和责任。

6.2.10 销毁私钥的方法

用户签名证书的私钥由用户自己根据需要进行管理和销毁。用户加密证书的密钥对由电子认证服务机构的密钥管理中心产生，在用户密钥对、证书失效后，电子认证服务机构应以加密的方式归档保留；所有归档密钥对，应至少在证书失效 5 年后方可销毁，销毁方式应确保彻底地销毁密钥信息。

6.2.11 密码模块的评估

SRCA 密钥存储所用的密码模块均经过国密局的许可，同时 SRCA 会按照安全评估标准定期对密码模块的工作状态以及相关安全参数进行安全性评估。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

订户证书中的公钥由中铁 KMC 和 SRCA 定期归档。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

6.4 激活数据

6.4.1 激活数据的产生和安装

SRCA 产生的激活数据——用于下载证书的口令，是在安全可靠的环境下，由硬件设备随机产生。

这些激活数据，都通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。

对于非一次性使用的激活数据，SRCA 建议用户自行进行修改。

6.4.2 激活数据的保护

订户的激活数据必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果有书面保留的需求时，必须进行安全可靠的保存。同时，为了配合业务系统的安全需要，应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

（1）订户用于申请、下载证书的口令，下载成功后失效。

（2）用于保护私钥或者 IC 卡、USB Key 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后一定要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全性要求

SRCA 的证书签发系统的数据文件和设备由管理员维护，未经管理员授权，其它人员不能操作和控制系统；其它普通订户无系统账号和密码。SRCA 系统部署在多级不同厂家的防火墙之内，确保系统网络安全。SRCA 系统密码有最小密码长度要求，而且必须符合复杂度要求，SRCA 系统管理员定期更改系统密码。

6.5.2 计算机安全评估

SRCA 的认证业务系统，通过了国家密码管理局等部门的有关评估、审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

SRCA 系统的开发由满足国家相关安全和密码标准的可靠软件开发商完成，同时与该开发商建立安全保密约定以保证系统的权威性与可靠性。

6.6.2 安全管理控制

SRCA 的系统配置以及任何修改和升级都会记录在案并进行控制，并且 SRCA 采取有效的安全管理控制机制来控制和监视系统的配置，以防止未授权的修改。

6.6.3 生命期的安全控制

SRCA 和相关产品开发商以及标准机构共同合作，根据国际安全标准和发展动态，在不影响正常提供服务的前提下，积极采用国内外先进的技术和设备，及时进行技术更新。SRCA 对系统的任何修改和升级都会记录在案并进行控制。

6.7 网络安全控制

SRCA 有多级防火墙以及其他访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的 SRCA 员工才能够进入签发管理系统、注册管理系统、目录服务器、密钥管理系统等设备或系统。SRCA 只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

6.8 时间戳

目前 SRCA 根据相关信息系统要求提供时间戳服务。

根据对系统安全管理和控制的需要，SRCA 会决定是否使用时间戳。根据不同数据对时间的敏感性、严密性和逻辑关系的要求，SRCA 将确定时间戳服务的有关规范和策略。

7. 证书、证书撤销列表和在线证书状态协议

7.1 证书

SRCA 签发的证书均符合 X.509 V3 证书格式。遵循 RFC5280 标准。

7.1.1 版本号

SRCA 所签发证书的版本信息存放在证书版本属性栏内。

7.1.2 证书扩展项

X.509 V3 证书的扩展项主要包括：

（1）Authority Key Identifier: 颁发机构密钥标识符；

（2）Subject Key Identifier: 主题密钥标识符；

（3）Key Usage:密钥用法；

（4）Subject Alternative Name：主题备用名；

（5）CRL Distribution Points: CRL 分布点。

针对特别的用户，SRCA 签发的证书有可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。

①密钥用法（Key Usage）

②证书策略扩展项（Certificate Policies）

③主题备用名（Subject Alt Name）

④基本限制扩展项（Basic Constraints）

⑤CRL 的分发点（CRL Distribution Points）

⑥签发CA密钥标识符

⑦主题密钥标识符

⑧名称限制

7.1.3 算法对象标识符

符合国家密码管理部门批准的算法对象标识符。

7.1.4 名称形式

SRCA 签发证书的甄别名符合 X500 关于甄别名的规定。对于证书主体甄别名，O 代表证书持有者所在的组织机构，OU 代表证书持有者所在的部门，甄别名可以包含不止一个的 OU 用于存放其他信息。

对于证书签发者甄别名，O 代表证书签发机构， OU 代表证书签发机构的部门。

7.1.5 名称限制

SRCA 签发的证书中的通用名不能使用假名、伪名。

7.1.6 证书策略对象标识符

SRCA 的每类证书（一类、二类、三类、四类）对应一个证书策略对象标识符（OID）。当使用证书策略扩展项时，SRCA 签发证书中包含证书策略对象标识符，该对象标识符与相应的证书类别对应。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

与 ITU X.509 和 RFC5280 规定一致。

7.2 证书撤销列表

7.2.1 版本号

SRCA 定期签发 CRL（证书撤销列表），其所签发的 CRL 遵循 RFC 5280 标准。采用 X.509 V2 格式。

7.2.2 CRL 和 CRL 条目扩展项

（1）颁发者

CN=SRCA

O=Sinorail Certification Authority

C=CN

（2）CRL 发布

SRCA 至少每隔 24 小时自动发布最新的 CRL。

（3）签名算法

SRCA 采用 sha256/RSA2048 、SM3/SM2 签名算法。

7.3 在线证书状态协议

SRCA 为证书订户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。SRCA OCSP 服务遵循 RFC256 标准。

7.3.1 版本号

SRCA 使用 OCSP 版本 1。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8. 认证机构审计和其他评估

8.1 审计评估的频率或情形

8.1.1 SRCA 的审计

由中铁 CA 或法律主管部门指定审计者。中铁 CA 需要对 SRCA 的关联单位（包含 SRCA 授权的注册机构、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 CPS 和相应的证书政策的规定，其频率可由 SRCA 决定或由法律制定的监管机构决定。审计分为内部审计和外部审计。

内部审计是由CA机构资质组织内部人员进行的审计,审计的结果可供CA机构改进、完善业务、内部审计结果不需要公开。

外部审计由CA机构委托第三方审计机构来承担，审计单依据包括CA所有与业务有关的安全策略、《电子认证业务规则》、业务规范、管理指导，以及国家或行业的相关标准。

8.1.2 SRCA 对关联单位的审计

SRCA 对其关联单位实行定期审计（一般为 1 年），审计人员由 SRCA 指派。审计人员必须熟悉 SRCA 的规则和信任服务的相关知识，了解保证安全的基本知识，按照 SRCA 的规范、协议、履行责任业务等情况，独立、公正地对关联单位作出合格或不合格的结论。

SRCA 可以根据协议对下属的关联机构和单位进行安全审计,有权根据上级的审计结果和自己的审计结果，取消对下属单位的授权或重新授权。

SRCA 的关联单位，一年被审计的次数一般情况下为 1 次，特殊情况也不得超过 2 次。上级机构和单位，不得对下属单位和机构重复审计和重复收费。审计结果根据有关规定而决定是否公布。

8.2 审计评估者的资质

内部审计评估，由中铁CA内部审计评估小组执行，人员的选择一般包括：

CA机构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；

内部审计员与审计管理员；

人事负责人；

其他需要的人员。

外部审计的审计人员的资质由第三方确定。

8.3 评估者与被评估者之间的关系

8.3.1 审计评估者与 SRCA 的关系

对 SRCA 进行审计的审计者必须是一个独立于 SRCA 的实体。SRCA 内部评估者与被评估对象之间，也应是相对独立关系，不影响评估的客观性。

SRCA 可以根据需要，选择专业、公正、客观的专业审计评估机构，协助进行内部评估。

8.3.2 审计报告与 SRCA 的关系

对 SRCA 进行审计会产生审计报告，SRCA 不是这些审计报告的作者，所以对其内容不负任何责任，同时 SRCA 也不对这些审计报告发表任何观点，也不会对由于信任审计报告中有关 SRCA 的内容而导致的任何损失负责。

8.4 审计评估内容

对 SRCA 的规范审计、评估应包括：

1） 运营工作流程和制度是否得到严格遵守；

2） 是否严格按 CPS、业务规范和安全要求开展认证业务；

3） 各种日志、记录完整性，是否存在问题；

4） 是否存在其他可能存在的安全风险。

8.5 对问题与不足采取的措施

如果在审计、评估过程中发现执行规范有不足之处，SRCA 将根据审计报告的内容制定纠正、预防措施，明确对此采取的相应行动。SRCA 将根据普遍认可的国际惯例或监管法律迅速解决问题。

8.6 审计评估结果的传达与发布

除非法律明确要求，SRCA 一般不公开审计结果。在必要的情况下，向 SRCA 关联单位（例如垫付商、注册机构、受理点）通知审计结果的具体规定将在 SRCA 和关联单位的协议中写明。

9. 法律责任和其他业务条款

9.1 费用

9.1.1 费用支付

SRCA 对证书订户和所有关联单位（例如垫付商、注册机构、受理点）收取服务费用。证书订户和 SRCA 关联单位有义务根据 SRCA 的价目表支付给 SRCA 费用。

9.1.2 证书费用

证书相关费用依据物价管理部门的批文制定，在中铁 CA 网站上公布。价目表按 SRCA 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七天后生效。SRCA 也可以通过其他方法通知证书订户或其他各方费用变化。根据证书实际应用的需要，SRCA 在不高于物价部门认可价格的前提下可以对证书价格进行适当调整。

序号	产品名称	单位	价格 （单位：元）	备注
1	单位数字证书	张/年	500	更新需缴纳同样费用
2	个人数字证书	张/年	100	更新需缴纳同样费用
3	设备字证书	张/年	2600	更新需缴纳同样费用
4	移动端数字证书	张/年	300	更新需缴纳同样费用
5	事件型证书	张	5	/
6	智能 UKey	枚	120	质保期 1 年

9.1.3 证书查询费用

在证书有效期内，对该证书信息进行查询，SRCA 不收取查询费用。SRCA 保留对占用大量资源的证书查询操作进行收费的权利。

9.1.4 证书撤销或状态信息的查询费用

对证书撤销列表查询，SRCA 不收取信息访问费用。对于实时在线证书状态查询（OCSP）服务费用，由 SRCA 与订制者在签订的协议中另行约定。SRCA 保留对占用大量资源的证书撤销和状态信息查询操作进行收费的权利。

9.1.5 其它服务费用

SRCA 可根据请求者的要求，订制各类通知服务，具体服务费用在与订制者签订的协议中约定。

9.1.6 退款政策

退款政策——SRCA 数字证书一经订户接受，SRCA 不办理退证、退款手续。

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

9.2 财务责任

SRCA 授权的发证机构（如注册机构、受理点等）应具有维持其运作和履行其责任的经济实力，它应该有能力承担对订户、垫付商以及其他信任其签发的证书的实体造成的责任风险。

9.3 商业信息的保密

9.3.1 保密的商业信息

SRCA 与 SRCA 授权的发证机构之间、SRCA 与证书订户之间、SRCA 授权的发证机构与证书订户之间的协议、保密信息、往来函和商务协定等，除非法律明确规定，不得擅自泄漏、使用和发布给第三方。

对 SRCA 或 SRCA 对其授权的发证机构的审计报告、审计结果等相关信息是保密信息，除了 SRCA 授权和信任的对象，不能泄露给其他任何实体。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 SRCA 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 SRCA 授权的对象。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，SRCA 没有义务公布或透露。除非法律明文规定，SRCA 没有义务公布或透露证书订户证书以外的信息。

9.3.2 非保密的商业信息

与证书有关的申请流程、申请需要的手续、申请操作指南等文档中公布的信息是可以公开的。而且 SRCA 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。SRCA 在目录服务器中公布证书的撤销和挂起信息，供网上查询。当 SRCA 在有关法律、法规或规章条款的要求下，或在国家法律部门的要求下必须披露本 CPS 中具有保密性质的信息时，SRCA 将向执法部门公布相关的保密信息。这种行为不视为违反了保密的要求和义务。

9.4 个人信息的保密

9.4.1 保密的个人信息

与证书订户的证书公钥配对的私钥是保密的，证书订户应该认真保管，不能公布给其他人。如果证书订户擅自泄露私钥，则由此引起的后果由证书订户自负。

证书申请者提供的私人信息中非证书中使用信息，无论该申请是否被批准，SRCA 都有责任予以保密。

9.4.2 非保密的个人信息

证书中的基本信息是可以公开的，通过 SRCA 目录服务等方式向外公布。当保密信息的所有者出于某种原因，要求 SRCA 公开或披露他所拥有的保密信息时，SRCA 一般情况下予以满足。但如果这种行为涉及或有可能引起对任何其他方的赔偿义务，SRCA 有权拒绝其请求，且不应承担任何与此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责 SRCA 与此相关的或由于公开保密信息引起的所有损失、损坏的赔偿责任。

9.4.3 客户资料保存

为了保障客户资料不受非授权侵犯，制定以下制度：

1、客户信息资料保存在专用的资料室内，只能由资料审核人员、档案管理人员通过受限的方式进入、接触，其他非相关人员不得翻阅、查看客户的信息。

2、客户信息资料需要由指定人员归档保管，不得将资料随意放置以免泄露，也不得以任何理由向他人泄露客户信息。

3、对由于各种原因而造成客户信息泄露的相关工作人员要追究相应的责任，情节严重的，给予恰当的处分。

4、离职人员按照离职协议需要保密其接触的用户资料，否则可追究其相应法律责任。

9.5 知识产权

SRCA 享有并保留对证书以及 SRCA 提供的全部著作（包括软件、标识等）的独一无二的一切知识产权，包括保证证书和著作的完整权、名称权和利益分享权等全部权利。因此，SRCA 有权决定证书订户、依赖方、授权发证机构等采用什么软件系统，选择采取的形式、方法、时间、过程和模型，以便保证系统的兼容和互通。按本 CPS 规定，所有与 SRCA 发行的证书和 SRCA 提供的著作相关的一切版权、商标和其他知识产权均属于 SRCA 的产权，这些知识产权包括所有相关的文件和使用手册。授权发证机构在征得 SRCA 的同意后，可以使用相关的文件和手册。

9.6 陈述与担保

除非 SRCA 作出特别约定，若本 CPS 的规定与其他 SRCA 制定的相关规定、指导方针相互抵触，订户必须接受本 CPS 的约束。在 SRCA 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 CPS 的规定执行；对协议中不同于本 CPS 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

SRCA 在提供电子认证服务活动过程中的承诺如下：

（1） SRCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受主管部门的业务监督和指导，对 SRCA 所签发的数字证书承担相应的责任和义务；

（2）SRCA 保证使用的系统及密码符合国家政策与标准，保证 SRCA 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；

（3）SRCA 签发给订户的证书符合 SRCA CPS 规定的所有实质性要求；

（4）SRCA 保证证书在有效期内的有效性和可靠性，将向证书订户通报任何已知的、可能在本质上影响证书的有效性和可靠性事件；

（5）SRCA 将及时撤销证书，并发布到 CRL 上供订户查询；

（6）证书公开发布后，SRCA 向证书依赖方保证，除未经鉴证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构、受理点的陈述与担保

SRCA 的注册机构和受理点在参与电子认证服务过程中的承诺如下：

（1）严格执行 SRCA 制定的证书管理和发放策略，服从 SRCA 整体的管理和规范要求；提供给证书订户的注册过程完全符合 SRCA CPS 的所有实质性要求；

（2）在 SRCA 生成证书时，不会因为注册机构、受理点的失误而导致证书中的信息与证书申请人的信息不一致；

（3）及时响应并向 SRCA 提交订户证书申请、撤销、更新等服务请求。

9.6.3 订户的陈述与担保

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

（1）订户已阅读并理解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；

（2）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 SRCA 或注册机构检查和核实；

（3）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；

（4）订户对使用私钥的行为负责；

（5）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 SRCA 和注册机构，及时申请采取证书撤销等业务处理；

（6）订户已知其证书被冒用、破解或被他人非法使用时，应按 SRCA CPS 的相关条款及时申请办理撤销其证书业务。

9.6.4 依赖方的陈述与担保

证书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，验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理解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

其他参与者的陈述与担保同 9.6.4。

9.7 担保免责

SRCA 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。

SRCA 在提供给证书订户的“SRCA 数字证书申请（更新）与使用责任书”中，都有事先告知证书订户的免责条款的规定:SRCA 发放的各类型证书只能用于网络上标识用户身份、保证数据传输安全以及进行电子签名，证书不能作为其他用途，若用户数字证书用于其他用途，SRCA 不承担由此产生的任何责任。如果由于 CA 中心的设备或网络故障而导致签发数字证书错误、延迟、中断或者无法签发，CA 中心将重新签发证书，但不承担任何赔偿责任。

SRCA 在签发证书之前，证书申请者已同意遵守“SRCA 数字证书申请（更新）与使用责任书”中的各项规定。责任书中明确规定 SRCA 不承担任何形式的担保和义务。如

果证书申请者故意或无意地提供虚假信息或未及时更新用户资料，导致 CA 中心签发证书错误，造成用户及他人损失时，由用户承担一切责任。

9.8 责任范围

9.8.1 CA 的责任

根据《中华人民共和国公司法》《中华人民共和国电子签名法》和其它法律规定，作为依法设立的有限责任公司，SRCA 在承担任何责任和义务时，只承担法律范围内的有限责任。

SRCA 应承担的责任和义务是：

（1）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；

（2）保证 SRCA 的签名私钥在 SRCA 内部得到安全的存放和保护；

（3）SRCA 建立和执行的安全机制符合国家政策的规定。

针对上述内容补充解释如下：

（1）除上述所规定的职责条款，SRCA、SRCA 的服务机构、SRCA 授权的发证机构、SRCA 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 SRCA 必须承担其它的义务或 SRCA 必须对其行为作出其它的承诺。

（2）在上述内容中所罗列不可抗力的任何情况下，SRCA 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。

（3）由于技术的进步与发展，为保证证书的安全性，SRCA 会要求证书订户及时更换证书以保证 SRCA 能更好地履行本节所述之责任。

9.8.2 注册机构的职责

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 SRCA 决定，并在本 CPS 或相应的注册机构协议中规定，以后 SRCA 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。

9.8.3 受理点的职责

同注册机构的职责。

9.8.4 证书订户的职责

所有的证书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：

（1）证书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、真实正确的，可供 SRCA 检查和核实；证书订户必须严格遵守和服从本 CPS 规定的或者由 SRCA 推荐使用的安全措施；

（2）证书订户需熟悉本 CPS 的条款和与证书相关的证书策略，还需遵守证书持有者证书使用方面的有关限制；

（3）一旦发生任何可能导致安全性危机的情况，如证书订户遗失私钥、遗忘或泄密以及其他情况，证书订户应立刻通知 SRCA 或 SRCA 授权的发证机构，申请采取撤销、挂起等处理措施。

9.9 赔偿

SRCA 在认证活动中产生的赔偿，都以本 CPS 的规定为处理依据，法律法规另有要求的除外。

对于由于 SRCA 自身原因，如没有严格按业务流程进行证书审批导致证书的错误签发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书订户、依赖方的损失，SRCA 将承担相应的赔偿责任，但这种责任是有限的。在任何情况下，在 SRCA 的信任链中，CA、注册机构及受理点对所有当事人的关于每份证书最高赔偿限额总计不得超过每张证书价格的五倍（当事人包括但不限于证书用户、证书申请者、接受者或依赖方）。SRCA 只对由于自身原因造成的用户直接损失承担责任，对间接的损失不承担责任。

9.9.1 SRCA 赔偿责任

如 SRCA 违反了前文第 9.8 款条例规定的职责，SRCA 承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

（1）SRCA 所有的赔偿义务不得高于这种证书适用的赔偿限额上限每张证书价格的五倍，这种赔偿责任上限可以由 SRCA 根据情况重新制定，SRCA 会将重新制定后的情况立刻通知相关当事人。

（2）SRCA 只在法律规定有效期限内承担损失损害赔偿。

9.9.2 注册机构赔偿责任

注册机构的赔偿责任在注册机构和 SRCA 之间签订的协议中表明。

9.9.3 受理点赔偿责任

受理点的赔偿责任在受理点和 SRCA 之间签订的协议中表明。

9.9.4 订户的赔偿责任

（1）订户申请证书时，提供不真实材料，导致造成 SRCA 或第三方遭受损失的，订户应承担一切赔偿责任；

（2）订户过失造成私钥泄漏、遗失，而未及时告知 SRCA 撤销或挂起的，造成 SRCA 或第三方遭受损失的，订户应承担一切赔偿责任；

（3）订户使用或依赖方信任证书的行为，有违反本 CPS 及相关操作规范的，订户或依赖方应自行承担一切损害赔偿责任；

（4）SRCA 与订户之间签署协议另有赔偿规定的，参照其规定。

9.9.5 赔偿额度

SRCA 及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿额度，依据物价管理部门的批文制定，在中铁 CA 网站上公布。

本条款所称的“合计赔偿额度”，适用于所有当事人因信任 SRCA 所签发证书而造成一切形式的损害，以每张证书为计量单位，不考虑证书所造成的损害事件的数量。SRCA 及订户或其它当事人所承担的赔偿责任，其具体额度由国家相关法律法规进行规定，或由各方协商确定。协商不成可提交 SRCA 所在地的司法机关进行解决。

9.10 有效期和终止

9.10.1 有效期限

本CPS自发布之日起正式生效，其中将详细注明版本号及发布日期。除非SRCA特别声明CPS提前终止，在SRCA颁布新版本CPS之前，本CPS一直有效。

9.10.2 终止

当新版本的 CPS 正式发布生效时，旧版本的 CPS 自动终止。当 SRCA 中止业务时，SRCA CPS 终止。在终止服务六十日前向信息产业主管部门报告，并作出妥善安排。

9.10.3 效力的终止与保留

CPS 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，各参与方需要归还或保障销毁从其他方得到的保密信息。

9.11 信任体间的责任关系

9.11.1 信任体和证书订户的赔偿责任

（1）信任体和证书订户在使用或信赖证书时，若有任何行为或疏漏而致使 SRCA、SRCA 授权的发证机构产生损失，信任体和证书订户应承担连带赔偿的责任、相应的损失及诉讼、仲裁等费用，SRCA 及 SRCA 授权的发证机构有权要求赔偿；

（2）证书订户的责任并不仅限于本 CPS 的规定，证书订户如果向第三方传递信息时表述有误，而第三方用证书验证了一个或多个电子签名后理所当然地相信这些表述，证书订户必须对这种行为的后果负责；

（3）证书订户接受证书就表示同意在以下情况下承担赔偿责任：证书订户（或由证书订户授权，按证书订户指示行事的人）对事实表达有误或曲解时，证书订户没有公开任意一项实质性的事实，而且造成这种错误或遗漏的原因是出于他的疏忽或是他有意欺瞒 SRCA 或其授权的其他机构时，证书订户没有采取必要的防护措施来防止私钥的遗失、泄密、被修改或被未经授权的人使用时；

（4）当一个证书应证书订户的代理人要求被签发后，代理人和证书订户两者负有连带责任。如出现第三中所述的情况，他们负共同赔偿责任。证书订户有责任就代理人所做任何不实陈述与遗漏，通知 SRCA 或 SRCA 授权的机构。

（5）其他法律法规、协议约定信任体和证书订户应当赔偿的情形。

9.11.2 信托关系

电子认证服务机构与证书订户和信任体之间的关系不存在代理和信托关系。

证书订户和信任体都没有权利以合同形式或其他方法让 SRCA 承担信托责任。

9.12 修订

SRCA 有权在合适的时间修订、修改和改变本电子认证业务规则中任何术语、条件和条款，而且无须预先通知任何一方。

SRCA 有权在 SRCA 的自主数据库中设置和公布修改结果,或以其他方式(如修改 CPS 版本的形式或在网站上）公布。

所有的修订、修改和改变在公布后立刻生效。证书订户如不在修改结果后公布的限定时间内申请废止（撤销）证书，就视为同意这种修正、修改和变化。所有以提供给证书订户的内容，以中铁 CA 网站 www.sinorailca.com 上公布的最新版本为准。

9.13 争议解决

铁路企业当事人之间问题和争端通过双方友好协商解决，协商不成的按照中国国家铁路集团有限公司相关规定调解解决。铁路行业外的当事人协商不成的应向中铁 CA 所在地人民法院提起诉讼。

根据仲裁条例在时效内裁决。仲裁的决定是终决性的，对每个当事人都有约束力。

9.14 监管法律

本电子认证业务规则在各方面服从中华人民共和国法律的管制和解释。

9.15 适用的法律

无论合同或其他法律条款的选择及无论是否在中国建立商业关系，SRCA 电子认证业务规则的执行、解释、翻译和有效性均适用中华人民共和国和法律。法律的选择是确保对所有订户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

9.16 其他规定

9.16.1 各种规范的冲突

若本电子认证业务规则的规定与其他规定、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，除非本电子认证业务规则的规定在法律所禁止的范围内，或有关规定、指导方针明确地言明优于本电子认证业务规则。

9.16.2 安全资料的财产权益

下列与安全相关的资料视为下列指定的当事人所拥有：

（1）证书：证书的权利行使受 SRCA 的管理约束，本规则旨在保护订户的隐私，避免未经授权者公布其证书；

（2）电子认证业务规则：本电子认证业务规则的产权为 SRCA 所有；

（3）甄别名：甄别名归命名实体所有(或他们的雇主和负责人所有)；

（4）私人密钥：不论该密钥是以何种实体媒介存放或保护，私人密钥为合法使用或有权使用该密钥订户（或其雇主或委托人）所有；

（5）公开密钥：不论该密钥以何种实现媒介存放或保护，公开密钥为订户（或其雇主或委托人）所有；

（6）SRCA 的公开密钥：SRCA 作为自身的根节点的公开密钥，是 SRCA 的财产，这个公钥由 SRCA 授权分配，放在值得信任的硬体或软件上。

9.17 一般条款

9.17.1 完整协议

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，本规则与订户协议、依赖方协议及其他补充协议构成了 CA 中心信任域中的完整协议。

9.17.2 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。

9.17.3 强制执行

免除一方对协议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协议其他项的违反应该承担的责任。

9.17.4 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。

9.17.5 其他条款

本《电子认证业务规则》的解释权归中铁数字证书认证中心。