

中铁数字证书认证中心（SRCA）

证书策略(CP)

V1.0

2009 年 4 月

版权归属中铁数字证书认证中心

（任何单位和个人不得擅自翻印）

版权声明

中铁数字证书认证中心证书策略（CP）受到完全的版权保护。本文件所涉及的“中铁 CA 证书策略”、“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：北京市宣武区马连道南街 2 号院 1 楼

电话：51892565

传真：51892554

电子邮件：srca@sinorail.com

注意

《中铁数字证书认证中心证书策略（CP）》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》、《合同法》、《著作权法》、《保密法》、《商标法》、《民事诉讼法》、《全国人大常委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 将保留依法追究的权利。

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服务管理办公室《电子认证业务规则规范（试行）》修订

目 录

(版本号 1.0)	错误! 未定义书签。
目 录.....	4
1. 概括性描述.....	9
1.1 概述.....	9
1.2 文档名称与标识.....	9
1.3 电子认证活动参与者.....	9
1.3.1 电子认证服务机构.....	9
1.3.2 注册机构 (Registration Authority)	10
1.3.3 受理点 (Business Terminal)	10
1.3.4 证书垫付商 (Sponsor)	10
1.3.5 订户 (Subscriber)	11
1.3.6 依赖方 (Relying Party)	11
1.3.7 证书应用行业组织.....	11
1.3.8 其他参与者 (Other Participants)	11
1.4 证书应用.....	12
1.4.1 适用的证书应用.....	12
1.4.2 限制的证书应用.....	12
1.5 策略管理.....	12
1.5.1 策略文档管理机构.....	12
1.5.2 联系方式.....	12
1.5.3 CP 批准程序.....	13
1.6 定义和缩写.....	13
2.信息发布与信息管理.....	15
2.1 认证信息的发布.....	15
2.2 发布的时间或频率.....	15
2.3 信息库访问控制.....	15
2.3.1 信息库.....	15
2.3.2 信息的发布与处理.....	15
3.身份标识与鉴别.....	16
3.1 命名.....	16
3.1.1 名称类型.....	16
3.1.2 对名称意义化的要求.....	16
3.1.3 订户的匿名或伪名.....	16
3.1.4 不同名称形式的规则.....	16
3.1.5 名称的唯一性.....	17
3.1.6 商标的识别、鉴别和角色.....	17
3.2 初始身份确认.....	17
3.2.1 证明拥有私钥的方法.....	17
3.2.2 组织机构身份的鉴别.....	17

3.2.3 个人身份鉴别.....	18
3.2.4 域名（或 IP 地址）的确认和鉴别.....	18
3.2.5 没有验证的订户信息.....	18
3.2.6 授权确认.....	18
3.2.7 互操作准则.....	18
3.3 密钥更新请求的标识与鉴别.....	19
3.3.1 常规密钥更新的标识与鉴别.....	19
3.3.2 吊销后密钥更新的标识与鉴别.....	19
3.4 吊销请求的标识与鉴别.....	19
4.证书生命周期操作要求.....	20
4.1 证书申请.....	20
4.1.1 证书申请实体.....	20
4.1.2 证书申请过程与责任.....	20
4.2 证书申请审核.....	23
4.2.1 执行识别与鉴别功能.....	23
4.2.2 证书申请审核流程.....	23
4.2.3 处理证书申请的时间.....	23
4.3 证书签发.....	23
4.3.1 证书签发中注册机构和电子认证服务机构的行为.....	23
4.3.2 电子认证服务机构和注册机构对订户的通告.....	24
4.4 证书接受.....	24
4.4.1 构成证书接受的行为.....	24
4.4.2 电子认证服务机构对证书的发布.....	24
4.4.3 电子认证服务机构对其他实体的通告.....	24
4.5 密钥对和证书的使用.....	25
4.5.1 订户私钥和证书的使用.....	25
4.5.2 签名及验证.....	25
4.5.3 依赖方公钥和证书的使用.....	25
4.6 证书更新.....	26
4.6.1 证书更新的情形.....	26
4.6.2 请求证书更新的实体.....	26
4.6.3 证书更新请求的处理.....	26
4.6.4 证书更新的注意事项.....	27
4.6.5 颁发新证书时对订户的通告.....	27
4.6.6 构成接受更新证书的行为.....	27
4.6.7 电子认证服务机构对更新证书的发布.....	27
4.6.8 电子认证服务机构对其他实体的通告.....	27
4.7 证书密钥更新.....	27
4.7.1 证书密钥更新的情形.....	28
4.7.2 请求证书密钥更新的订户实体.....	28
4.7.3 证书密钥更新请求的处理.....	28
4.7.4 密钥更新的注意事项.....	28
4.7.5 颁发新证书时对订户的通告.....	28

4.7.6 构成接受密钥更新证书的行为.....	28
4.7.7 电子认证服务机构对密钥更新证书的发布.....	29
4.7.8 电子认证服务机构对其他实体的通告.....	29
4.8 证书变更.....	29
4.8.1 证书变更的情形.....	29
4.8.2 请求证书变更的订户实体.....	29
4.8.3 证书变更请求的处理.....	29
4.8.4 证书变更的注意事项.....	29
4.8.5 证书变更时对订户的通告.....	29
4.8.6 构成接受变更证书的行为.....	30
4.8.7 电子认证服务机构对变更证书的发布.....	30
4.8.8 电子认证服务机构对其他实体的通告.....	30
4.9 证书吊销和挂起.....	30
4.9.1 证书吊销的情形.....	30
4.9.2 请求证书吊销的实体.....	31
4.9.3 吊销请求的流程.....	31
4.9.4 吊销请求宽限期.....	32
4.9.5 电子认证服务机构处理吊销请求的时限.....	32
4.9.6 依赖方检查证书吊销的要求.....	32
4.9.7 CRL 发布频率.....	32
4.9.8 CRL 发布的最大滞后时间.....	32
4.9.9 在线状态查询的可用性.....	32
4.9.10 在线状态查询要求.....	33
4.9.11 吊销信息的其他发布形式.....	33
4.9.12 密钥损害的特别要求.....	33
4.9.13 证书挂起的情形.....	33
4.9.14 证书挂起的订户实体.....	33
4.9.15 证书挂起和解挂的流程.....	33
4.9.16 挂起的期限限制.....	34
4.10 证书状态服务.....	34
4.10.1 操作特征.....	34
4.10.2 服务可用性.....	34
4.10.3 可选特征.....	34
4.11 订购结束.....	34
4.12 密钥生成、备份与恢复.....	35
4.12.1 密钥生成、备份与恢复的策略与行为.....	35
4.12.2 会话密钥的封装与恢复的策略与行为.....	35
5. 认证机构设施、管理和操作控制.....	35
6. 认证系统技术安全控制.....	36
7. 证书、证书吊销列表和在线证书状态协议.....	36
7.1 证书.....	36
7.1.1 版本号.....	36
7.1.2 证书扩展项.....	36

7.1.3 算法对象标识符.....	37
7.1.4 名称形式.....	37
7.1.5 名称限制.....	38
7.1.6 证书策略对象标识符.....	38
7.1.7 策略限制扩展项的用法.....	38
7.1.8 策略限定符的语法和语义.....	38
7.1.9 关键证书策略扩展项的处理规则.....	38
7.2 证书吊销列表.....	38
7.2.1 版本号.....	38
7.2.2 CRL 和 CRL 条目扩展项.....	38
7.3 在线证书状态协议.....	39
7.3.1 版本号.....	39
7.3.2 OCSP 扩展项.....	39
8. 认证机构审计和其他评估.....	39
8.1 审计评估的频率或情形.....	39
8.1.1 SRCA 的审计.....	39
8.1.2 SRCA 对关联单位的审计.....	39
8.2 审计评估者的资质.....	40
8.3 评估者与被评估者之间的关系.....	40
8.3.1 审计评估者与 SRCA 的关系.....	40
8.3.2 审计报告与 SRCA 的关系.....	40
8.4 审计评估内容.....	40
8.5 对问题与不足采取的措施.....	41
8.6 审计评估结果的传达与发布.....	41
9. 法律责任和其他业务条款.....	42
9.1 费用.....	42
9.1.1 费用支付.....	42
9.1.2 证书费用.....	42
9.1.3 证书查询费用.....	42
9.1.4 证书吊销或状态信息的查询费用.....	42
9.1.5 其它服务费用.....	42
9.1.6 退款政策.....	42
9.2 财务责任.....	43
9.3 商业信息的保密.....	43
9.3.1 保密的商业信息.....	43
9.3.2 非保密的商业信息.....	43
9.4 个人信息的保密.....	43
9.4.1 保密的个人信息.....	43
9.4.2 非保密的个人信息.....	44
9.4.3 客户资料保存.....	44
9.5 知识产权.....	44
9.6 陈述与担保.....	44
9.6.1 电子认证服务机构的陈述与担保.....	45

9.6.2 注册机构、受理点的陈述与担保.....	45
9.6.3 订户的陈述与担保.....	45
9.6.4 依赖方的陈述与担保.....	46
9.6.5 其他参与者的陈述与担保.....	46
9.7 担保免责.....	46
9.8 责任范围.....	47
9.8.1 CA 的责任.....	47
9.8.2 注册机构的职责.....	47
9.8.3 受理点的职责.....	47
9.8.4 证书订户的职责.....	47
9.9 赔偿.....	48
9.9.1 SRCA 赔偿责任.....	48
9.9.2 注册机构赔偿责任.....	48
9.9.3 受理点赔偿责任.....	48
9.9.4 订户的赔偿责任.....	48
9.9.5 赔偿额度.....	49
9.10 有效期和终止.....	49
9.10.1 有效期限.....	49
9.10.2 终止.....	49
9.10.3 效力的终止与保留.....	49
9.11 信任体间的责任关系.....	49
9.11.1 信任体和证书订户的赔偿责任.....	49
9.11.2 信托关系.....	50
9.12 修订.....	50
9.13 争议解决.....	50
9.14 监管法律.....	51
9.15 适用的法律.....	51
9.16 一般条款.....	51
9.16.1 完整协议.....	51
9.16.2 分割性.....	51
9.16.3 强制执行.....	51
9.16.4 不可抗力.....	51
9.16.5 其他条款.....	52

1. 概括性描述

1.1 概述

中铁数字证书认证中心（简称 SRCA），即中铁信弘远（北京）软件科技有限责任公司（简称弘远公司），成立于 1999 年，它是铁道部信息技术中心为了保证铁路信息化建设能持续、顺利地发展，按照政企分开、事企分开的原则，依据原铁道部的指示精神，按照市场运作的规律，牵头组建的以信息技术工程设计、软件开发、信息安全服务、计算机网络管理、系统集成和运营维护为主的高新技术企业。

证书策略（CP，Certification Policy）“一套指定的规则集，用以指明证书对具有相同安全需求的一个特定团体和（或者）应用类型的适用性”。依赖方可使用 CP 来帮助其决定一个证书（连同其中的绑定）是否足够可信、是否适用于特定的应用。本文件是中铁数字证书认证中心（SRCA）证书策略（CP，Certification Policy），使用范围为 SRCA 发放的所有证书。在 SRCA 证书策略中，它为审批、签发、管理、使用、更新、吊销证书等制定的技术规范，这些规范是 SRCA 证书的标准，她应用于保护 SRCA 证书的完整性和安全性

本 CP 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 CP 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 CP 的质量或其中铁 CA 信任域参与者的适用性。而且 SRCACP 的结构不一定会与 RFC3647 以后的版本保持一致。

1.2 文档名称与标识

本文档名称为《中铁 CA 证书策略 (CP)》，版本号为 1.0。已注册的对象标识符（OID）为 1.3.6.1.4.1.18760.1.10。

1.3 电子认证活动参与者

1.3.1 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。

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吊销列表 CRL (Certificate Revocation List) 服务公布该证书可以公开的信息和状态。

1.3.2 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, 发起或传递证书吊销请求, 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 机构有责任依照《中华人民共和国电子签名法》和本 CP 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。

1.3.3 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, 负责办理和审批数字证书的申请、吊销、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、证书吊销、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 CP 及 SRCA 公布的服务和技术支持。

1.3.4 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 CP 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。

1.3.5 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、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。

1.3.6 依赖方 (Relying Party)

本证书策略对于依赖方的身份认证没有做任何的假设或者限制。当依赖方是普通的使用者时，依赖方并不被要求与 SRCA 或者其他实体 CA 建立关系。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。

1.3.7 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。

1.3.8 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、目录服务提供者等等。

1.4 证书应用

1.4.1 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。

1.4.2 限制的证书应用

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。其他限制的证书应用包括：由于证书的使用可能导致人员死亡、伤残的情形；由于证书的使用可能导致环境破坏的情形等。

1.5 策略管理

1.5.1 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 CP。

中铁 CA 运营安全管理小组，是 SRCA 证书策略 CP 的最高管理机构，由中铁 CA 召集管理人员、技术人员、客服人员、法律顾问等组成，负责审核并批准 CP，并作为 CP 实施检查监督的最高决定机构。

1.5.2 联系方式

SRCA 对证书策略进行严格的版本控制，并由中铁 CA 负责解释。

电话： 010-51892565

传真： 010-51892554

地址： 北京市宣武区马连道南街 2 号院 1 楼

邮编： 100055

电子邮件: crca@sinorail.com

1.5.3 CP 批准程序

SRCA 的 CP 由中铁 CA 运营安全管理小组指定的专人或编写组起草拟定后,提交中铁 CA 运营安全管理小组审核。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 运营安全管理小组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。

1.6 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。本规则指中铁数字认证系统或 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系统注册机构。

证书策略 (CP): 本证书策略文档,是关于 SRCA 证书策略的主要说明

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、吊销、更新证书或密钥等)所遵循的规则详细描述和声明,提供其它业务、法律和技术方面的细节。

证书吊销列表 (CRL): Certificate revocation list, 认证机构的失效证书列表。证书吊销可能由于证书过期、私钥失窃或者其他原因产生。又称证书废止列表、证书黑名单。**在线证书状态协议 (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包含公开密钥拥有者信息以及公开密钥的电子文档。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）：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）：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 同时提供证书吊销列表（CRL）查询服务。

SRCA 证书订户可以通过 LDAP 查询、下载并验证订户证书。SRCA 证书订户都可以通过 SRCA 网站 www.sinorailca.com 查询有关信息。

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。发证机构在挂起或吊销证书后，在 24 小时内，在 SRCA 信息库中发出挂起和吊销的公告，更新证书吊销列表。根据需要，也可以人工发布最新 CRL。

2.3 信息库访问控制

2.3.1 信息库

SRCA 信息库是一个对外公开的信息库，包括但不限于以下内容：证书、CRL、CPS、CP、证书服务协议、技术支持手册、网站信息等。

2.3.2 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。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

。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。

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。

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)	证书办法机构	O= Sinorail Certification Authority
Organization Unit (OU)	单位或部门名称	OU=设计中心 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	CN=张三

	称	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/部门证书	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）

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。

3.1.6 商标的识别、鉴别和角色

无

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。

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。

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”。

然而，在某些情况下，SRCA 允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。

3.3.2 吊销后密钥更新的标识与鉴别

SRCA 不提供以下情况的证书被吊销后的密钥更新：

- (1) 证书的吊销原因是证书签发给了非证书主体的人；
- (2) 受理点发现或有理由相信证书申请中的资料有误。

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 吊销请求的标识与鉴别

订户吊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，递交吊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，再对证书进行吊销处理。订户本人吊销时的身份标识和鉴别使用原始身份验证相同的流程。

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。

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、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；

(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 CP 中指 SRCA；

(4) 订户，从 SRCA 接受证书的实体。

(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 CP 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 CP 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 CP 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 CP 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 CP、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 CP 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 CP 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 CP 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；证书申请者愿意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 CP 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 CP 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 CP 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。

7、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。

8、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 CP 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 CP 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。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。

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。

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，并且存储于安全电子令牌中或根据用户要求存储于其他存储介质，因此采取的是现场证书发放方式，由用户填写或监督 SRCA 工作人员填写申请信息，证书签发成功后将公钥证书安装

到安全电子令牌中发放给用户。由于其他原因用户未能现场领取证书的，则直接通知用户领取证书。

SRCA 没有上门为用户安装证书的义务。如果申请人需要，SRCA 可以上门安装，但需要收取相应的服务费用。

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。订户凭证书申请表和交费单据领取证书，订户在领取证书后，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。订户接受数字证书后，应妥善保管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。包括该证书是否被吊销、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 CP 的规定享有相应的权利和应尽的义务。

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。

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 CP 要求的行为；
- (4) 签名方和依赖方遵守本 CP 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，依赖方要独立地作做出应有的努力和合理的判断。除非本 CP 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 CP 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。如果证书订户需要更新证书，应当在证书有效期到期前到 SRCA 办理。

4.6.1 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。

4.6.2 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。

4.6.3 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。

4.6.4 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。

4.6.5 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。

4.6.6 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。

4.6.7 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。

4.6.8 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限一致。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) 证书被吊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。

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 4.6.5。

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 4.6.6。

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 4.6.7。

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 4.6.8。

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，将证书吊销后重新签发证书。

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 4.6.2。

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 4.6.5。

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 4.6.6。

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 4.6.7。

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 4.6.8。

4.9 证书吊销和挂起

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吊销或者挂起。

4.9.1 证书吊销的情形

证书吊销分为主动吊销和被动吊销，主动吊销是指订户主动申请吊销其数字证书，受理点审核申请后吊销其证书。被动吊销是指电子认证服务机构确认用户违反 CP 规则内容申请使用证书，或者证书主体消亡，则吊销数字证书。

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吊销：

- 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吊销的实体提出；
- 3、由于证书的不当使用而违反国家的法律法规及本 CP 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 CP 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，订户必须提出吊销请求：

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 CP 或其它协议、法规及法律所规定的责任和义务。

三、其它 SRCA 认为可以进行吊销的原因。

四、SRCA 没有义务一定要公开某一张证书被吊销的原因。

4.9.2 请求证书吊销的实体

能够要求吊销证书的实体包括：

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 吊销请求的流程

SRCA 在主动发现订户证书符合强制吊销条件，则提出申请及书面证明材料，并进行归档，在签署强制吊销命令后 24 小时内吊销订户证书。强制吊销订户证书前，SRCA 没有必要通知订户，但在强制吊销后，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吊销证书请求，必须按照规定出具书面证明材料，填写吊销申请表并签字盖章。SRCA 在审核材料通过后 24 小时内吊销证书，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。

主动吊销的流程如下：

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 进行吊销申请，同时提交合法的证明材料。

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

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

4.9.4 吊销请求宽限期

一旦发现需要吊销证书，订户应该实时提出吊销请求，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 在应该吊销证书的情况下强制吊销订户证书，强制吊销立即生效，订户不能请求宽限。

4.9.5 电子认证服务机构处理吊销请求的时限

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

4.9.6 依赖方检查证书吊销的要求

证书吊销列表 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 一般在批准吊销请求后 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 中公布被吊销的证书。

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

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有偿查询方式。

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 吊销信息的其他发布形式

OCSP 作为可选的有偿的吊销信息发布形式。

4.9.12 密钥损害的特别要求

当 SRCA 的根密钥损害发生时，SRCA 将主动地即时吊销证书，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，而不申请吊销该证书，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、吊销或恢复等其他证书相关业务，SRCA 将对该证书做解挂处理，请订户注意及时吊销、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吊销通知，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吊销时，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，SRCA 或授权受理点可吊销

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吊销或挂起该用户数字证书。用户申请吊销或挂起证书时，填写申请表（一式三份），SRCA 授权受理点按照 4.9.3 的吊销流程或 4.9.15 的挂起流程进行批准或拒绝的操作。

4.12 密钥生成、备份与恢复

由于密钥对是安全机制的关键，所以在证书策略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密钥管理中心负责生成的，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

订户加密证书密钥对可以由中铁 CA 的密钥管理中心系统集中安全产生和保存，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) 注册机构提出申请，并有充分的理由；
- 3) 国家执法、司法机关因执法、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。

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

本章节要求与 SRCA 的电子认证规则 CPS 保持一致。

6. 认证系统技术安全控制

本章节要求与 SRCA 的电子认证规则 CPS 保持一致。

7. 证书、证书吊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 RFC3280 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) authorityKeyIdentifier: 颁发机构密钥标识符；
- (2) subjectKeyIdentifier: 主题密钥标识符；
- (3) keyUsage: 密钥用法；
- (4) subjectAlternativeName: 主题备用名；
- (5) crlDistributionPoints: 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)

该扩展项指定证书密钥对的用法，不同证书该扩展项不同。这个扩展项的criticality域通常设置为FALSE。

② 证书策略扩展项 (Certificate Policies)

证书策略扩展项中有SRCA证书策略中对应证书类的 CP 对象标识符及策略限定符。这个扩展项的criticality域设置为FALSE。

③ 主题备用名 (subjectAltName)

扩展项的使用符合RFC 3280。此扩展项的criticality 设为FALSE。

④ 基本限制扩展项 (BasicConstraints)

SRCA 证书的基本限制扩展项中的主题类型被设为CA。最终订户证书的基本限制扩展项的主题类型设为最终实体 (End-Entity)。这个扩展项的criticality 域设置为FALSE。CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的CA 级数。对于最终订户证书签发CA，其CA 证书 “pathLenConstraint” 域的值设为0，表示证书路径中仅有一个最终订户证书可以跟在这个CA 证书后面。

⑤ CRL 的分发点 (cRLDistributionPoints)

SRCA签发的证书中包含CRL 的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载CRL。此扩展项的criticality 项应设为FALSE。

⑥ 签发CA 密钥标识符

SRCA最终订户证书及中级CA 证书中有签发CA 密钥标识符扩展项，当证书签发者包含主题密钥标识扩展项时，签发CA 密钥标识符由160 位的签发证书的CA 的公钥进行SHA-1 散列运算后的值构成；否则，它将包含签发CA 的主题DN 和序列号。这个扩展项的criticality 域设置为FALSE。

⑦ 主题密钥标识符

当证书包含主题密钥标识符扩展项时，该值由证书主题的公钥产生。使用该扩展项时，其扩展项的criticality 域设为FALSE。

⑧ 名称限制

SRCA 签发的证书中的通用名不能使用假名、伪名。

7.1.3 算法对象标识符

SRCA 签发的证书按照 RFC 3280 标准，用 sha1RSA 算法签名，用于标识该签名算法的 ASN.1 对象标识符是：

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) 5}。
```

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）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 RFC3280 规定一致。

7.2 证书吊销列表

7.2.1 版本号

SRCA 定期签发 CRL（证书吊销列表），其所签发的 CRL 遵循 RFC 3280 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 sha1RSA 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 CP 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。

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。

SRCA 对关联单位的审计将收取审计费。审计费用在 SRCA 与关联单位的协议书中体现。

8.2 审计评估者的资质

对 SRCA 实施规范审计的审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且在业界享有良好的声誉。

了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作。

具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

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：

SRCA 支持的证书认证操作规程是否完全与本证书策略表达一致，包括 SRCA 的技术、手续和员工的相关管理政策和业务声明。

SRCA 是否实施了相关技术、管理、相关政策和业务声明物理与环境安全控制是否达到国家有关规定及本 CP 的规定。审计者或 SRCA 认为有必要审计的其他方面。

8.5 对问题与不足采取的措施

如果在审计、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。

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 证书吊销或状态信息的查询费用

对证书吊销列表查询，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吊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、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 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吊销和挂起信息，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 CP 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）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。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 CP 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 CP 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 CP 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 CP 的规定执行；对协议中不同于本 CP 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 CP 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 将及时吊销证书，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 CP 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、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 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证书策略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，及时申请采取证书吊销等业务处理；

(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 CP 的相关条款及时申请办理吊销其证书业务。

9.6.4 依赖方的陈述与担保

证书依赖方必须熟悉本证书策略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证书策略的所有条款，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。

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 CP 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证书策略的条款。

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 CP 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 CP 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，申请采取吊销、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 CP 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责任上限，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 吊销或挂起的，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 CP 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；

（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CP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CP提前终止，在SRCA颁布新版本CP 之前，本CP 一直有效。

9.10.2 终止

当新版本的 CP 正式发布生效时，旧版本的 CP 自动终止。当 SRCA 中止业务时，SRCA CP 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

CP 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限于本 CP 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 and 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。

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、修改和改变本证书策略中任何术语、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 CP 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（吊销）证书，就视为同意这种修正、修改和变化。所有以书面形式提供给证书订户的内容，按以下规则发送：

- (1) 接受者是公司或其它单位组织，向其登记的联系地址或办公室发送信息；
- (2) 接受者是个人，向其申请书上规定的地址发送；

这些通知可能用快递或挂号信的方式发送。SRCA 有权选择通过电子邮件或其他方式向证书订户发送通知，邮件地址在证书订户申请证书时已注明。所有发送给 SRCA 的通知应以书面形式传递。所有这些通知应采用快递或挂号信的方式发送。若通过电子邮件方式发送通知给 SRCA，则这种通知只有在 SRCA 收到证书订户的电子邮件通知后 24 小时内，收到证书订户书面确认材料，方为有效。

9.13 争议解决

如果当事人之间无法很好的解决出现的问题和争端，应该提交 SRCA 所在地的仲裁机构，

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

本证书策略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 证书策略的执行、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 一般条款

9.16.1 完整协议

本证书策略将替代先前的、与主题相关的书面或口头解释，本协议与订户协议、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。

9.16.2 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。

9.16.5 其他条款

无