辽宁 CA 电子认证业务规则

V3.0

辽宁数字证书认证管理有限公司

2026 年 6 月

辽宁数字证书认证管理有限公司版权所有

版权声明

本电子认证业务规则受到完全的版权保护。本文件中所涉及的“辽宁省数字证书认证中心”、“辽宁CA电子认证业务规则”、“辽宁CA”及其标识等，均由辽宁数字证书认证管理有限公司独立享有版权和其它知识产权。

辽宁数字证书认证管理有限公司拥有对本电子认证业务规则的最终解释权。

未经辽宁数字证书认证管理有限公司的书面同意，本文件的任何部分不得以任何方式、任何途径（电子的、机械的、影印、录制等）进行复制、存储、调入网络系统检索或传播。

在被授权情况下，本文副本可以在非独占性的、免收版权许可使用费的基础上进行复制及传播，并应保证复制、传播文件的准确性、完整性。

对任何复制本文件的其他请求，请寄往以下地址：

辽宁数字证书认证管理有限公司

地址：辽宁省沈阳市和平区和平南大街28号甲3

联系电话：4008052281，024-23871492-2001（分机号）

传真：024-23871490

电子邮件：service@lnca.org.cn

邮政编码：110006

目录

1. 概括性描述

1.1. 承诺

辽宁数字证书认证管理有限公司对电子认证服务业务开展作出如下承诺：

1) 辽宁 CA 在开展经营和服务活动时，严格遵守中华人民共和国相关法律、行政法规，坚持树立以人民为中心的服务理念，承担社会责任；

2) 辽宁 CA 在与客户建立业务关系前，将开展应用业务调研，并建立应用接入业务风险评估及内部追究机制，严禁为存在违法违规风险的业务提供电子认证服务；

3) 使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；

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

1.2. 基本信息

辽宁数字证书认证管理有限公司（简称辽宁 CA）是经工业和信息化部、国家密码管理局批准设立的第三方电子认证服务机构，工信部电子认证服务许可证编号 ECP21010225010，有效期 2025 年 11 月 15 日至 2030 年 11 月 14 日；《电子认证服务使用密码许可证》编号 0016，有效期至 2030 年 3 月 5 日。法定代表人李东海，注册地址辽宁省沈阳市和平区和平南大街 28 号甲 3，线下业务受理大厅地址沈阳市和平区北八马路七巷 4 号，客服热线 4008052281。

公司设立安全运营部、技术部、市场部、营业部、客户服务部、财务部、综合部七大职能部门，独立完成证书受理、身份核验、密钥管控、系统运维、合规审计全流程工作，所有身份核验工作由辽宁 CA 直接执行，非同法人合作受理点、RA 仅代收纸质材料，无任何身份审核、证书审批权限。

辽宁 CA 用户证书通过国家密码管理局下发的根证书直接签发，辽宁 CA 根证书信息如下：

- 证书编号：65ef10af4c16df3128ae88604ff638ca
- 颁发机构名称：ROOTCA
- 密码算法：SM2
- 密钥长度：256
- 有效期:：2033年12月19日 9:23:50
- 计划服务时间：2033 年 10 月 1 日

根密钥生成采用 5 选 3 多人在场管控机制，根密钥仅由本机构独立保管，不向任何第三方托管、转移。

本 CPS 严格按照 T/CQAE 11034-2025《电子认证业务规则规范》全条款修订，完整覆盖证书签发、身份查验、密钥管控、灾备、审计、法律责任全生命周期管理要求，所有证书严格区分个人/机构、高/基础风险等级，全程落实意愿留痕、数据归档、可追溯监管要求。

1.3. 文档名称与标识

1.3.1. 辽宁 CA 电子认证业务规则修订表

版本	发布日期	备注
V1.0	2004 年 6 月 2 日	采用 RFC3647 结构
V2.0	2005 年 5 月 12 日	根据《电子认证业务规则规范（试行）》修订
V2.1	2005 年 12 月 12 日	根据《辽宁 CA 电子认证业务规则》V2.0 修订
V2.2	2007 年 11 月 9 日	根据《辽宁 CA 电子认证业务规则》V2.1 修订
V2.3	2018 年 11 月 25 日	根据《辽宁 CA 电子认证业务规则》V2.2 修订
V2.4	2020 年 12 月 25 日	根据《辽宁 CA 电子认证业务规则》V2.3 修订
V2.5	2025 年 12 月 18 日	为符合《电子认证业务规则规范》标准而进行的责任主体明确、技术标准更新等关键修改
V3.0	2026 年 6 月 5 日	按 T/CQAE 11034-2025 全面修订

1.3.2. 名称

本文档名称为《辽宁 CA 电子认证业务规则》V3.0，是辽宁 CA 对所提供的认

证及相关业务的全面描述。

1.3.3. 遵循的证书策略 OID

本机构 CPS 的 OID 为 1.2.156.115339。

证书类型	主管部门证书策略 OID	其他证书策略 OID
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	暂无
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	暂无
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	暂无
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	暂无

1.4. 电子认证活动参与者

1.4.1. 电子认证服务机构

电子认证服务机构包括辽宁 CA 及所有辽宁 CA 下层机构。

辽宁 CA 是所有辽宁 CA 下层机构和实体的根。辽宁 CA 是在十分严格的保密和安全机制控制下，根据根证书有效期的策略生成密钥对，并签发根证书。辽宁 CA 根据授权和协议，签发下一级的证书。辽宁 CA 将决定如何实施辽宁 CA 根密钥对的更新和切换。

辽宁 CA 所签发的证书与每一个证书申领实体的公钥绑定。辽宁 CA 承诺，在有效期内的证书，将采用证书目录服务器和证书黑名单服务器 CRLSERVER（Certificate Revocation List Server），公布该证书可以公开的信息和状态。

辽宁 CA 负责证书用户信息的审核，验证申请人提供信息的准确性、可靠性和完整性。任何合作注册机构、受理点等均无身份审核权限，仅负责材料代收，审核结果全部由辽宁 CA 终审。

1.4.2. 订户

订户是指被颁发给一张证书的证书主体。

辽宁 CA 的证书订户包括所有证书申请人、操作人员及要求数字证书验证和加密服务的系统和服务器。所有订户由辽宁 CA 授予证书，并且是证书的主体。

另外，终端用户可以使用辽宁 CA 授予的证书为其他终端用户加密信息，也可校验其他终端用户的数字签名。这样，终端用户也可是辽宁 CA 中的可信赖方。

在对外运营管理策略和规范中，终端用户通常指证书使用者。

1.4.3. 依赖方

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从事有关活动的人。

依赖于辽宁 CA 颁发的数字证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个辽宁 CA 订户。

在辽宁 CA 体系中，是信任辽宁 CA 证书，可以对使用辽宁 CA 证书机制进行的数字签名进行验证，使用其他辽宁 CA 证书用户的公钥加密信息的实体。

辽宁 CA 负责保证数字证书身份的真实性。

1.4.4. 其他参与者

为以上未提及的隶属于辽宁 CA 证书体系的实体。如目录服务提供者等与 PKI 服务相关的参与者。

1.5. 证书应用

1.5.1. 证书应用分类

1.5.1.1. 电子签名证书

按证书主体对象的类型和风险等级，电子签名认证证书可分为个人高等级电子签名认证证书、个人基础级电子签名认证证书、机构高等级电子签名认证证书、机构基础级电子签名认证证书四种类型。

1.个人高等级电子签名认证证书

证书类型：个人高等级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.1.2；

证书特点：适用于高风险业务、符合《电子签名法》的个人电子签名认证证

书；

应用场景：涉及生命健康、财产权益等高风险活动，且非证书应用限制场景的个人电子签名业务。

2.个人基础级电子签名认证证书

证书类型：个人基础级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.1.1；

证书特点：适用于低风险业务、符合《电子签名法》的个人电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动之外的，且非证书应用限制场景的个人电子签名业务。

3.机构高等级电子签名认证证书

证书类型：机构高等级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.2.2；

证书特点：适用于高风险业务、符合《电子签名法》的机构电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动，且非证书应用限制场景的机构电子签名业务。

4.机构基础级电子签名认证证书

证书类型：机构基础级电子签名认证证书；

主管部门证书策略 OID：2.16.156.339.2.1.2.1；

证书特点：适用于低风险业务、符合《电子签名法》的个人电子签名认证证书；

应用场景：涉及生命健康、财产权益等高风险活动之外的，且非证书应用限制场景的机构电子签名业务。

1.5.1.2. 其他类型证书

辽宁 CA 发放的其他类型证书包括：为服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、SSL 服务器证书、IPSec VPN 设备证书等；代码签名证书，用于代码防篡改；加密证书用于文件加密、邮件加密、传输加密。以上类型证书不属于电子签名认证证书，安全级别为基础级。

1.5.2. 证书应用限制

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用户自己承担。

禁止使用辽宁 CA 颁发的数字证书的应用场景包括但不限于：

a)涉及人身关系的，如婚姻、收养、继承等；

b)涉及停止公共事业服务的，如停止供水、供热、供气等；

c)法律、行政法规规定的其他不适用电子签名的应用场景或类型；

d)国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6. 策略管理

1.6.1. 策略管理机构

1.6.1.1. 组成

辽宁 CA 安全策略委员会是《辽宁 CA 电子认证业务规则》（CPS）的最高管理机构。公司常务副总经理担任主任委员，副总经理担任副主任委员，各部分负责人担任委员。

辽宁 CA 安全策略委员会的任命信息在公司网站公示。

1.6.1.2. 职责

安全策略委员会负责 CPS 和 CP 以及配套制度的维护，包括但不限于以下职责：

- 确定维护 CPS 和 CP 等策略文档的职能分工，建立合理有效的修订和批

准流程；

- 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；
- 每年至少进行一次 CPS 和 CP 全面评审，根据实际需要及时修订策略文档；
- 每年组织运营风险评估并形成报告；
- 妥善保存安全策略委员会重大决议的相关文件和会议记录。

1.6.2. 策略文档的批准程序

1.6.2.1. 起草小组的成立流程

(1) 安全策略委员会根据 CPS 修订或新建需求，发起成立起草小组的申请，明确起草任务的目标、范围和预期完成时限。

(2) 从技术、业务、综合等相关部门选拔具备对应专业能力的人员组成起草小组，确定小组负责人，明确各成员的分工与职责。

(3) 召开起草小组启动会，传达任务要求，梳理相关参考资料，制定起草工作计划与时间节点。

(4) 小组开展策略文档的起草工作，定期同步进度，讨论解决起草过程中遇到的问题。

1.6.2.2. 安全策略委员会的审批流程

(1) 起草小组完成 CPS 初稿后，提交至安全策略委员会，同时附上起草说明、相关依据材料等。

(2) 安全策略委员会组织成员对文档进行预审，提前熟悉内容，梳理疑问和修改意见。

(3) 召开安全策略委员会正式评审会议，由起草小组对文档进行汇报，委员会成员针对文档内容进行质询、讨论，提出修改要求。

(4) 起草小组根据委员会的意见对文档进行修改完善，形成送审稿再次提交委

员会。

(5) 委员会对送审稿进行最终表决，表决通过后，进入后续备案、发布流程；若未通过，需重新修改后再次提交审批。

1.6.2.3. 向主管机关的备案流程

(1) 安全策略委员会按照主管机关的要求，通过指定的线上系统或线下渠道提交备案申请及相关材料。

(2) 跟进主管机关的备案审核进度，及时补充审核过程中要求补充的材料。

(3) 收到主管机关的备案确认通知后，留存好备案凭证。

1.6.2.4. 发布流程

(1) 安全策略委员会在完成备案后，制定策略文档的发布计划，明确发布范围、发布时间和发布渠道。

(2) 通过企业官网、内部办公系统、工作群等渠道发布策略文档，同时对文档内容进行解读说明，确保相关人员理解到位。

(3) 建立策略文档的存档机制，将正式发布的文档归档保存，方便后续查阅和更新。

(4) 跟踪策略文档的执行情况，收集执行过程中的反馈，为后续策略优化提供依据。

1.7. 定义和缩写

1.7.1. 辽宁 CA

辽宁数字证书认证管理有限公司的简称。

1.7.2. CPS（Certification Practice Statement）

认证业务规则的英文简称。明确规定辽宁CA在审批、签发、发布和废止证书等证书生命周期管理以及相关的业务应遵循的各项操作规范。

1.7.3.CA（Certification Authority）

认证机构的英文简称。CA是网络身份认证的管理机构，是网上安全电子交易中具有权威性、公正性和可信赖的第三方机构。CA为电子交易的各参与方签发标识其身份的数字证书，并对数字证书进行更新、废止等一系列管理。

1.7.4.证书持有者

所有拥有任何辽宁CA证书的个人或实体，不包括辽宁CA管理员证书。

1.7.5.终端用户（End-Entities）

辽宁CA中的终端用户包括所有证书申请人、操作人员及要求数字证书验证和加密服务的系统和服务器。所有终端用户由辽宁CA授予证书，并且是证书的主体。

另外，终端用户可以使用辽宁CA授予的证书为其他终端用户加密信息，也可校验其他终端用户的数字签名。这样，终端用户也可是辽宁CA中的可信赖方。

在对外运营管理策略和规范中，终端用户通常指证书持有者。

1.7.6.申请人

指向辽宁CA提出颁发证书申请的个人或单位用户。

1.7.7.订户

即为证书持有者。

1.7.8.辽宁 CA 人员

包括辽宁CA员工、辽宁CA授权的注册中心及受理点人员。

1.7.9.辽宁 CA 管理员证书：

辽宁CA管理员证书的组成情况：CA系统管理员证书，各管理员证书，终端管理员证书，受理点操作员证书，各系统之间的通讯证书，CA根证书等。

1.7.10. 测试证书

测试证书使用范围与正式数字证书一致，主要供系统和用户测试使用，方便用户认识数字证书、了解数字证书、懂得如何使用数字证书。同时数字证书有效期仅为一个较短的时间，一般最长不能超过3个月。

1.7.11. 认证（Certification）

不同实体在进行网上操作时，通过可信赖的、中立的第三方（如CA认证机构）对身份进行审核，并由第三方出具证明证实其身份的可靠性和合法性的过程。

1.7.12. 数字签名（Digital Signature）

数字签名是利用公开密钥算法等方法保证信息传输过程中信息的完整性、提供信息发送者身份的真实性和不可抵赖性的一种技术。

1.7.13. 私人密钥（Private Key）

私人密钥是一种不能公开、由持有者秘密保管的数字密钥，用于创建数字签名、解密报文等。

1.7.14. 公开密钥（Public Key）

公开密钥是可以公开的数字密钥，用于验证相应的私人密钥签名的报文，也可以用来加密报文、文件，由相应的私人密钥解密。

1.7.15. 数字证书

数字证书又称为数字标识(Digital Certificate，DigitalID)。它提供了一种在Internet上身份验证的方式，是用来标志和证明网络通信双方身份的数字信息文件，与司机驾照或日常生活中的身份证相似。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。

1.7.16. CRL（Certificate Revocation List）

数字证书废止列表的英文简称。CRL中记录所有在原定失效日期到达之前被废止的数字证书的用户数字证书序列号，供数字证书使用者在认证对方数字证书时查询使用。CRL通常又被称为数字证书黑名单。内容通常还包含列表发行人的姓名、发行日期、下次废止列表的预定发行日期、更新或废止的数字证书序号，并说明更新或废止的时间与理由。声明了主体的名字或签发中心的身份，确定签名者的身份，包括签名者的公开密钥，表明了数字证书的操作时限，还包括数字证书的序列号。

1.7.17. LDAP（Light weight Directory Access Protocol）

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

1.7.18. OCSP(Online Certificate Status Protocol)

即在线查询数字证书状态协议，用于支持实时查询数字证书状态。

1.7.19. HTTP（Hypertext Transfer Protocol）

超文本传输协议。

1.7.20. HTTPS（Hypertext Transfer Protocol with SSL）

采用 SSL 的超文本传输协议。

1.7.21. PKCS（PublicKey Cryptography）

公开密钥密码法。

1.7.22. PKI（Public Key Infrastructure）

公开密钥基础架构。

2. 信息发布与信息管理

辽宁 CA 的信息发布与信息管理是通过目录服务器自动将证书发布到辽宁 CA 网站（www.lnca.org.cn）上，用户可以通过访问辽宁 CA 的网站获取证书的相关信息。

2.1. 信息发布的内容

辽宁 CA 在公司网站上发布的内容，包括但不限于：

- CPS、CP 的所有版本；
- 证书链；
- 证书信息、状态信息等查询服务；
- 详细的业务办理指南，包括但不限于服务网点地址、营业时间、联系电话等；
- 依赖方协议；
- 投诉处理政策及投诉方式，包括但不限于：投诉处理部门的地址、联系电话、电子邮件地址，以及内部监部门名称。

2.2. 信息更新

信息发布内容如有变化，在变化生效后 1 个工作日内更新。

2.3. 监管备案及信息对接

辽宁 CA 按照国家电子认证服务管理平台的要求进行了备案，并与国家电子认证服务管理平台的完成了技术对接，实现了根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

3. 身份标识与鉴别

3.1. 身份查验通用要求

3.1.1. 通用要求

辽宁 CA 在受理证书申请时，对订户和／或受托人进行告知、身份确认、意愿记录和协议签署;并且，辽宁 CA 未将身份查验义务委托给外部机构或个人（非属同一法人主体的机构视为外部机构）。

3.1.2. 订户告知

3.1.2.1. 告知内容

辽宁 CA 在申请证书时，通过现场和线上服务系统将以清晰、明确的方式向申请人完整展示《数字证书申请表》、《数字证书服务协议》的全部内容，并要求申请人在充分阅读并理解后，通过可靠的电子签名或强制确认勾选等方式，完成协议的在线签署与接受。告知订户以下内容：

a) 订户的权利和义务；

b) 服务收费的项目和标准：

c) 电子签名认证证书、电子签名的使用条件；

d) 信息安全保障措施；

e) CA 和订户的责任划分；

f) 订户签名私钥的存储方式及安全要求；

g) 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.1.2.2. 告知方式

a) 高等级证书采用面对面、电话、视频或主管部门认可的其他方式告知，并保留告知的记录：

b) 基础级证书采用高等级证书的告知方式，或采用强制阅读、短信、邮件等

方式告知，并保留告知的记录。

3.2. 初始身份确认

3.2.1. 证明拥有私钥的方法

辽宁 CA 为订户提供可靠的技术手段和其他必要措施，确保订户私钥应在符合国家相关安全标准的密码模块中生成和存储。同时对私钥的生成和安全存储实施监督，确保订户对私钥专有专控。

a) 按照本文件第 6.2.2 节规定的方式生成订户密钥对；

b) 通过数字签名的方式来确认证书订户拥有某个公钥对应的签名私钥。

3.2.2. 个人身份的查验

3.2.2.1. 个人身份信息有效性的确认

辽宁 CA 在受理个人证书申请时，对个人身份信息的查验方式及内容：

a) 受理个人证书申请时，订户应出示其有效身份证件或有效身份证件信息，有效证件类型仅限法律法规和国家有关文件规定的身份证件：

b) 通过证件机读工具、权威数据库或主管部门认可的其他方式查验，如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证，以确定订户身份证件的真实性和有效性；

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

3.2.2.2. 个人高等级证书的实人查验

辽宁 CA 对订户开展实人查验时，根据项目需求情况将采用下列方式之一：

a) 面对面查验；

b) 远程人工面对面查验；

c) 生物特征验证：如活体人脸、指纹、声纹、掌纹等生物识别技术的应用；

d) 通过主管部门认可的其他方式。

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

3.2.2.3. 个人基础级证书的实人查验

辽宁 CA 对订户开展实人查验时，根据项目需求情况将采用下列方式之一：

a) 通过本文件第 3.2.2.2 节规定的方式；

b) 电信运营商三要素：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；

c) 银行卡四要素：核对姓名、证件号码、银行卡号、银行预留手机号在银行的一致性，并通过预留手机号的随机短信验证码核验；

d) 由申请人持有的有效电子签名认证证书签名验证；

e) 通过主管部门认可的其他方式，如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等。

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

3. 2. 3. 机构身份的查验

3.2.3.1. 机构身份信息有效性的确认

辽宁 CA 受理机构证书申请时，确认订户身份信息查验方式及内容如下：

a) 机构订户应委派法定代表人或者授权申请人持机构有效证件原件和加盖公章的有效证件影印件，有效证件包括：

(1) 营业执照或非企业单位（法人）登记证书；

(2) 组织机构代码证；

(3) 政府主管部门的批文或登记证书；

(4) 法律、法规和国家有关文件规定的其他有效证件。

b) 法定代表人或受托人的身份查验方式

(1) 法定代表人或受托人身份证件信息查验方式参见 3.2.2.1；

(2) 受托人办理时，查验机构加盖公章的有效书面授权证明。

3.2.3.2. 机构高等级证书的实人查验

辽宁 CA 对机构订户开展实人查验是，将根据项目情况采用下列方式之一：

a) 法定代表人实人查验，方法见第 3.2.2.2 节;

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

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

3.2.3.3. 机构基础级证书的实人查验

辽宁 CA 对机构订户开展实人查验是，将根据项目情况采用下列方式之一：

a) 法定代表人实人查验，方法见第 3.2.2.3 节；

b) 受托人实人查验，方法见第 3.2.2.3 节；

c) 由订户持有的同等级或者更高级的有效机构证书签名验证。

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

3.2.4. 设备证书鉴别方法

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，辽宁 CA 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，辽宁 CA 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。

辽宁 CA 指定的审核人员将依据国家法律法规及本 CPS 的规定，核对申请资

料的原件与复印件，业务受理成功后，辽宁 CA 有权留存用户提交的证明材料并妥善存档。

3.3. 订户意愿记录

3.3.1. 订户意愿记录内容

辽宁 CA 意愿记录内容，包括但不限于：

a) 订户身份信息；

b) CA 的信息；

c) 签名私钥保存方及其保存义务；

d) 订户对电子签名的法律责任；

e) 订户对上述 a)至 d)项内容已充分知晓并同意的明确意愿表示。

3.3.2. 个人高等级证书的意愿记录

辽宁 CA 在订户申请证书时，订户意愿的确认采用下列方式之一：

a) 现场办理时，通过面对面确认或手抄提示语的方式，并采用录音录像或通过主管部门认可的其他方式记录订户意愿；

b) 远程办理时，通过音视频或通过主管部门认可的其他方式确认并记录订户意愿。

3.3.3. 个人基础级证书的意愿记录

辽宁 CA 在订户申请证书时，订户意愿的确认采用下列方式之一：

a) 与高等级证书相同的方式，见第 3.3.2 节;

b) 采用强制阅读、短信或邮件确认等电子方式，并保留完整、可追溯的订户意愿记录。

3.3.4. 机构高等级证书的意愿记录

辽宁 CA 在订户申请证书时，订户意愿的确认采用下列方式之一：

a) 法定代表人申请时，按照第 3.3.2 节的方式确认机构法定代表人的意愿；

b) 受托人申请时，查验加盖机构公章的授权文件，并按照第 3.3.2 节的方式确认受托人的意愿。并采用录音录像或通过主管部门认可的其他方式记录订户意愿。

3.3.5. 机构基础级证书的意愿记录

辽宁 CA 在订户申请证书时，订户意愿的确认采用下列方式之一：

a) 法定代表人申请时，按照第 3.3.3 节的方式确认机构法定代表人的意愿：

b) 受托人申请时，查验加盖机构公章的授权文件，并按照第 3.3.3 节的方式确认受托人的意愿。并保留完整、可追溯的订户意愿记录。

3.3.6. 设备证书的意愿记录

辽宁 CA 在订户申请设备证书时，订户意愿的确认参考 3.3.4 规则执行。

3.4. 订户协议

辽宁 CA 订户协议，包括但不限于第 3.1.2.1 节中规定的内容。

3.5. 未验证的订户信息

a) 证书载明信息的查验方法、查验流程，具体按照第 3.2 节中规定的查验：

b) 证书中不包含未经验证的订户信息。

3.6. 互操作要求

认证机构管理员的身份除了必须符合个人证书申请者的条件外，还必须符合各认证机构协议（规范）中的有关规定。

辽宁 CA 根据业务情况，可与其他经过国家主管机构批准的 CA 机构签订互操作协议，不同 CA 机构或不同信任域之间在证书策略一致或基本相同基础之上，互相签发交叉 CA 证书或签发单向交叉 CA 证书。

认证机构资格由辽宁 CA 根据各认证机构协议（规范）来审查批准。

单位、个人身份或电子商务证书用户的身份验证方式由辽宁 CA 来定义和验证。辽宁 CA 有权利选择用户身份验证的方式和方法，以达到全面准确验证用户身份的目的。

3.7. 命名

辽宁 CA 签发的证书主体甄别名称（以下简称“ DN”）的命名规则，包括但不限于：

a) 针对个人和机构等不同类型的证书，分别约定其命名规则：

b) 确保命名具有实际意义，且能追溯到唯一实体的方法：

(1) 个人证书，主体 DN 项中包含订户姓名，在 DN 项或扩展项中包含有效证件类型及其编号〈或相关信息的映射，包括但不限于散列值、掩码等〉：

(2) 机构证书，主体 DN 项中包含机构名称，在 DN 项或扩展项中包含组织机构的有效证件类型及其编号。

c) 对证书名称中商标权的处理策略和方式，妥善处理商标名及其风险：

d) 在不影响证书通用性的前提下，可在证书中增加自定义的其他内容：

e) DN 项结构定义符合 GB/T 16264.8 的要求，DN 项编码规则见下表。

表 1 证书主体甄别名（DN 项）规范表

代码	说明	示例
c	国家	CN
s	省份（可选）	辽宁省
L	城市（可选）	沈阳市
O	订户所在机构信息（可选）	xx 公司
OU	订户所在机构部门信息（可选）	XX 部门

OU	订户身份识别信息 个人高等级/基础级证书：“@”+身份识别码 机构高等级/基础级证书：“@”企业代码证号	以个人为例： OU=@2101062001x xxxxxxxxxx
CN	订户名称（个人姓名或机构法定名称）	张三／xx 公司
IdentifyCode （OID 1.2.156.10260 .4.1.1） （个人）	订户身份标识码 采用上下文标签区分证件类型:标签 0 对应身份证号、标签 2 对应护照号，使用可打印字符串存储；标签 1 对应军官证号，使用 UTF8 字符串存储，该扩展为非关键项	A0 12 323130313035313 937333036313132 343137
ICRegistratio nNumber （OID 1.2.156.10260 .4.1.3） （机构）	企业统一社会信用代码使用可打印字符串明文进行存储，该证书扩展为非关键项	393132313031303 04D413058585858 583846

4. 证书生存周期操作要求

辽宁 CA 提供数字证书授权、申请、发放、修改、查询和管理等服务，提供网络安全及身份认证、电子公正、密钥管理等与数字证书密切相关的配套服务。本章节说明在证书生存周期方面对电子认证服务机构及相关实体或其他参与者的要求。

4.1. 通用要求

辽宁 CA 在证书生存周期方面承担的责任包括但不限于：

a) 辽宁 CA 承担建立、运营和维护注册通道的责任；

b) 辽宁 CA 承担与订户签汀电子认证服务协议的责任；

c) 辽宁 CA 承担妥善记录并保存相关信息的责任。

订户在证书生存周期方面承担提供准确信息的责任。

4.2. 证书申请

在证书申请处理过程中，辽宁 CA 鉴别证书申请实体身份，具体按本文件“3. 身份标识与鉴别”相关规定，完成对订户的告知、身份确认、意愿记录、协议签署等动作。

辽宁 CA 证书申请处理的流程与时限，包括：

a) 处理流程：按本文件“3.身份标识与鉴别”相关规定，完成对订户的告知、身份确认、意愿记录、协议签署等动作，并依据既定准则批准或拒绝该申请：

b) 处理时限：自受理之日起完成证书申请处理的最长期限不超过二个工作日，因特殊情况确需超期的，辽宁 CA 与订户协商确定处理时限。

4.2.1. 证书申请批准准则

同时满足下列全部条件时，辽宁 CA 准予审核通过、签发对应等级数字证书：

（1）申请主体身份证件、主体资质文件真实有效、处于合法存续状态，经由官方权威数据库核验比对一致；

（2）依照证书分级要求完成对应身份核验、活体核验、意愿录制/手写承诺留痕，意愿资料为申请人真实自主行为；

（3）申请表单信息填写完整、资料齐全，机构申请配套授权文件、公章材料合法有效，用户身份信息、域名等字段已完成权属核验并出具对应证明文件；

（4）申请人完整阅读并签署数字证书服务协议，充分知悉私钥保管义务、证书使用约束与相应法律责任；

（5）证书申请用途合法合规，不存在用于法律法规禁止的非法业务情形；

（6）申请主体无恶意申领、历史证书违规撤销、冒用证书等不良风控记录。

4.2.2. 证书申请拒绝准则

申请存在下列任一情形的，辽宁 CA 有权直接驳回本次证书申请，并书面告知申请人具体驳回原因：

（1）主体资质证件伪造、变造、过期、被行政机关注销/冻结，官方核验信息不一致；

（2）实人核验、活体检测核验失败，存在翻拍、视频篡改等冒用身份行为；

（3）申请资料关键信息涂改缺失，机构授权文件、印鉴不真实、不具备法律效力；DN 字段填入用户身份信息、域名等知识产权标识，无法提供合法权属及使用许可材料；

（4）申请人拒不签署服务协议、拒不完成法定意愿留存流程；

（5）申请证书拟用于电信诈骗、非法金融、伪造公文等违法活动，申请人被列入失信、涉案风险名单；

（6）同一主体短时间批量高频提交证书申请，存在倒卖证书、恶意申领的风险特征；

（7）申请人提交虚假材料、隐瞒关键事实，核验查实资料不实。证书批准、驳回的全部审核操作、资料、日志统一归档保存，留存期限不少于对应证书失效

后5年；申请人对驳回结果存有异议的，可向我司客服渠道提交补充材料申请二次复核。

4.3. 证书签发

a) 签发过程：包括对申请信息的验证、证书的生成与签发等：

b) 结果通告：证书申请处理完毕后辽宁CA将视情况（与依赖方或订户的约定）采用以下方式的一种或几种向订户通告处理结果的方式：

(1) 通过认证应用工具进行信息提示；

(2) 通过信函、站内信或电子邮件发送；

(3) 通过短信通知；

(4) 通过电话通知；

(5) 当面通知或通过实时视频等相当于面对面的方式通知；

(6) 通过主管部门认可的其他方式。

4.4. 证书接受

辽宁CA证书交付、接受与拒绝的规则，包括：

a) 向订户交付证书的方式：受理窗口面对面交付。

b) 订户接受证书或拒绝接受证书的步骤和条件：用户得到通知后，携带《数字证书申请表》到办理证书的窗口领取证书，领取证书前要在证书领取表单上签上用户姓名，如订户拒绝接受证书可在领取证书时提出，并办理退费手续，订户从获得数字证书起，就视为已经接受证书。

c) 保存订户接受证书的记录，包括接受时间、方式、操作人等信息。

4.5. 密钥对和证书的使用

在为订户生成新的密钥对并为其新公钥签发新证书时，辽宁CA将遵守以下规则：

a) 交付前的安全保护：辽宁 CA 在将密钥对交付订户保管之前，将采取有效措施保障其安全性，包括但不限于：

(1) 保障签名私钥生成和传输过程的安全；

(2) 审核订户密钥是否符合国家或行业相关安全标准要求，对不符合要求的（如 RSA 密钥长度小于 2048 位、使用 MD5,SHA-1 等不安全算法），辽宁 CA 将拒绝颁发证书。

b) 私钥管理服务要求：辽宁 CA 针对特定业务场景可提供私钥托管服务，并遵循以下原则：

(1) 未经订户书面授权，绝不保存或委托他人保存其签名私钥；

(2) 仅在获得法定代表人或受托人明确授权的情况下，才能使用机构证书签名私钥；

(3) 仅在获得订户明确授权的情况下，才能使用其签名私钥；

(4) 订户的签名私钥将以加密形式存储在专用的密码设备中，存储条件和配套管理流程符合安全标准；

(5) 所有涉及签名私钥的操作均有完整、可追溯的记录；

(6) 订户可随时、便利的撤销、终止或暂停/恢复私钥托管服务。

c) 安全事件反馈：订户或依赖方可通过辽宁 CA 网站、电子邮件、电话等渠道，向辽宁 CA 反馈证书相关安全事件，辽宁 CA 将及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

4.6. 证书续期

辽宁 CA 证书续期的规则，包括：

a) 证书续期的情形：在不改变订户主体信息的情况下，在原证书到期前，为订户签发新证书；

b) 申请人必须为订户或其受托人；

c) 若自申请人上次完成身份查验之日起至本次续期申请日未满三年，可使用

有效的原证书进行电子签名验证的方式进行确认，否则，将按照第 3.2 节的规定重新进行身份查验；

d) 证书的签发与接受流程按照第 4.3 与 4.4 节的规定执行。

4.7. 证书密钥更新

辽宁 CA 证书密钥更新的规则，包括：

a) 证书密钥更新的情形：为订户生成新的密钥对并为其新公钥签发新证书；

b) 申请人必须为订户或其受托人；

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

c) 证书签发与接受的流程按照第 4.3 与 4.4 节的规定执行。

4.8. 证书变更

辽宁 CA 证书变更的规则，包括：

a) 证书变更的情形：改变证书中除订户公钥之外的信息而签发新证书的情形，例如：订户名称改变等；

b) 申请人必须为订户或其受托人；

c) 辽宁 CA 将按照第 3.2 节的规定重新对订户进行身份查验，若发起方不是证书订户，CA 应取得订户同意；

d) 证书签发与接受的流程按照第 4.3 与 4.4 节的规定执行。

4.9. 证书撤销或冻结

4.9.1. 证书撤销流程

4.9.1.1. 证书撤销的情形

以下情形下可执行证书撤销操作：

a) 与证书中的公钥相对应的私钥被泄密或用户怀疑自己的密钥泄密；

b) 由于证书不再需要用于原来的用途，但密钥并未失密，而要求中止（例如用户离开了某个组织）；

c) 证书的更新费用未收到；

d) 用户不能履行电子认证业务规则或其他协议、法律及法规所规定的责任和义务；

e) 用户申请初始注册时，提供不真实材料；

f) 有证据表明证书已被盗用、冒用、伪造或者篡改；

g) 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；

h) 其他因法律或政策的要求辽宁 CA 采取的临时撤销措施

i) 用户申请撤销证书时填写的其他原因。

4.9.1.2. 证书撤销的流程:

申请者到辽宁 CA 受理窗口填写《数字证书申请表》，并注明撤销的原因。辽宁 CA 受理窗口识别撤销用户身份的真实性,对用户提交的证书撤销申请进行审核。

强制撤销：辽宁 CA 授权的发证机关管理员可以对用户证书进行强制撤销，撤销后必须立即通知该证书用户。强制撤销的命令来自于：辽宁 CA 或辽宁 CA 受理窗口。

4.9.2. 证书冻结流程

4.9.2.1. 证书冻结的情形

如果有以下情况，辽宁 CA 将会考虑冻结证书：

a) 用户提出暂停使用该证书；例如：证书持有者由于某种原因如长期出差，短期内无法使用证书，可以申请证书冻结等情形。

b) 用户未能履行与辽宁 CA 签订的协议中应尽的责任，如用户未按期缴纳证书服务费；

c) 注册机构、受理点、政府主管部门或国家司法机关，向辽宁 CA 和其授权的认证服务机构提出证书冻结请求并获得批准。

4.9.2.2. 证书冻结请求的流程

冻结申请人需向辽宁 CA 提交冻结申请表和身份证明材料，同时说明冻结的理由，如果为证书持有者以外的人（如证书注册机构或国家司法机关）提交冻结申请，同样需要填写申请表并加盖公章；

辽宁 CA 或其下属证书服务机构鉴别冻结申请者身份的真实性，并确认申请者是否有权提出该申请；

证书服务机构审核冻结申请后，将该申请提交至其所属的电子认证服务机构，等待认证机构对该申请的处理；

电子认证服务机构在处理冻结申请后，会定期（24 小时）或实时产生 CRL 列表，并要求下属证书服务机构通知用户证书已被冻结。

证书冻结的最长期限不得超过证书的有效期，如超过证书有效期而用户没有提出恢复申请，则该证书将会自动被注销。

4.9.3. 申请实体

有权提交证书撤销或冻结申请的实体包含：订户本人/机构受托人、证书合法依赖方、辽宁 CA 运营管理部门、司法及行政监管机关可为订户或其合法受托人。

4.9.4. 请求处理

辽宁 CA 为申请人提供以下便捷的证书撤销或冻结申请渠道：

(1) 服务热线：4008052281；

(2) 电子邮箱：service@lnca.org.cn；

(3) 辽宁 CA 线下服务窗口。

辽宁 CA 针对所有涉及私钥泄露、介质丢失、证书冒用等影响证书安全的上报事件，将完整记录上报时间、上报主体、事件描述、核验过程、处置措施、处置

结果，形成独立安全事件台账；

安全事件原始记录、处置单据、沟通凭证加密归档保存，留存期限不少于对应证书失效后5年，接受主管部门日常核查、专项检查调阅。

证书撤销、冻结全部审批单据、身份核验资料、审批操作日志统一归档留存，全程可追溯审计。

4.10. 证书状态信息服务

a) 辽宁CA通过LADP、OCSP及CRL提供证书状态查询服务，订户可通过此类服务获得证书状态。

b) 辽宁CA提供7×24小时证书状态查询服务，服务可用率不低于99%，响应时间不超过10秒。

c) 若上述查询服务失效，订户可通过辽宁CA服务热线、邮箱等渠道获取证书状态信息。

4.11. 停止使用认证服务

4.11.1. 停止订户服务的情形

辽宁CA停止向订户提供认证服务的情形如下：

a) 订户主动申请停止：订户根据自身需要向辽宁CA提交停止服务申请的，且经辽宁CA审核过的。

b) 本机构单方面终止服务：出现下列情形之一的，辽宁CA有权单方面终止向订户提供全部或部分认证服务。

1) 订户证书有效期届满且未在规定时限内完成续期申请的；

2) 订户违反本CPS条款、电子认证服务协议或相关法律法规规定的；

3) 订户在证书申请或使用过程中提供虚假、伪造、无效的身份信息或证明材料的；

4) 订户的签名私钥发生泄露、丢失、被冒用或存在其他重大安全风险的；

5) 司法机关、密码管理部门等有权机关依法要求本机构停止向订户提供服务的；

6) 订户主体资格依法终止（如机构注销、自然人死亡等）且无合法权利义务承受人的；

7) 存在其他可能危及电子认证服务安全、公共利益或本机构合法权益的情形的。

4.11.2. 处理停止服务请求的时限和方式

订户申请停止服务时，须向辽宁 CA 提交申请，申请流程为本 CPS 第 4.9 节的规定。辽宁 CA 在正式受理申请后，将在两个工作日内按照本 CPS 第 4.9 节的规定完成审核。

停止服务请求审核通过后，辽宁 CA 将撤销证书并安全销毁订户签名私钥。若证书有效期内终止使用辽宁 CA 的认证服务，辽宁 CA 将实时把该订户的证书撤销，并按照本 CPS 第 4.9 节的规定，发布策略进行发布。

停止服务后的用户数据管理规则如下：

（1）用户数据保存政策：订户办理停止服务、证书撤销后，该用户全部业务档案（身份材料、申请表、意愿留存文件、核验记录、双录音视频、证书操作日志等）加密归档留存，保存期限不少于对应证书失效之日起 5 年，用于历史验签举证、司法取证、监管核查使用，留存期间采用国密算法加密存储，严格管控访问权限。

（2）用户数据销毁方式：达到法定最长保管期限后，由档案管理、安全管理双人复核审批，对离线备份介质执行物理粉碎销毁；在线存储数据采用多次覆写清零方式进行逻辑销毁，全程留存销毁审批单据、销毁操作记录、影像台账，销毁资料永久归档备查。

（3）用户数据转移途径：仅在订户本人提出书面合法数据迁移申请、且接收方为具备合法电子认证资质机构的前提下，经我方内部审批流程后，采用加密数据包形式向指定合法机构转移用户非涉密业务资料；私钥原始数据一律不允许对外转移交付。

4.11.3. 责任延续条款

对服务停止前产生的认证服务相关操作，辽宁 CA 仍按照双方签订的认证服务协议履行相应责任；

订户在服务停止后，仍继续使用已撤销、失效证书进行电子签名或其他密码运算所产生的一切法律责任，由订户自行承担；

因订户违反本 CPS 条款或相关法律法规导致本机构单方终止服务的，由此产生的一切损失及法律责任由订户自行承担。

4.11.4. 记录操作过程

辽宁 CA 完整记录停止认证服务的申请、审核到撤销证书的操作过程，并定期将停止使用认证服务结束后的证书及相应订户数据进行归档。

5. 认证机构设施、管理和操作控制

5.1. 物理控制

5.1.1. 基础设施

辽宁 CA 主机房位于沈阳市和平区和平南大街 28 号甲 3 二层，进入机房内部须经过五道门禁，分别是：大楼入口、机房入口、办公区入口、屏蔽门、核心入口。

机房建设标准符合《GB/T2887 计算机场地通用规范》、《GB/T6650 计算机机房用活动地板技术条件》、《GB/T9361 计算机场地安全要求》、《GB50174 电子信息系统机房设计规范》、《BMB3-1999 处理涉密信息的电磁屏蔽室的技术要求和测试方法》，机房电磁屏蔽效能满足《GJBz20219－94》标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

5.1.2. 分区管理与访问控制

所有机房的建设和管理严格按照辽宁 CA 的规定要求，采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等监控技术，设施内部分为公共区、服务区、管理区和核心区，以确保物理通道的安全。进入机房屏蔽室（内含管理区与核心区），需要双人认证，采用刷卡+指纹双因素认证，实现“双人共管”与“双因素认证”的强制访问控制策略，并记录访问信息。

机房内部一律禁止参观，只有经过辽宁 CA 授权的人员才能进入相应的部门和工作地点。在进入辽宁核心区与管理区时实施双人共管与双因素认证的强制访问控制策略，并记录访问信息实行全天 24 小时自动监控。

存储媒体全生命周期管理遵循以下规定：

（1）存储媒体使用权限管控：机房硬盘、磁带、光盘、加密 U 盘、服务器存储介质等全部存储媒体实行专人专管、最小权限分配；仅密钥管理员、系统运维、档案管理员经双人审批后方可领用；严禁私自带出机房、转借外部人员，禁止使

用外来不明存储介质接入核心业务系统。

（2）领用、归还台账登记要求：建立存储介质动态管理台账，每条记录包含介质编号、介质类型、存储数据密级、领用人员、领用日期、用途、归还时间、归还核验人；领用、归还必须双人签字确认，台账永久归档备查。

（3）报废判定标准：满足以下任一条件的存储介质启动报废流程：介质硬件故障无法修复、存储数据超出法定留存期限、介质达到使用年限、存储敏感密钥/证书数据且不再复用。

（4）报废销毁审批与执行流程：a.报废申请：使用人填写《存储介质报废审批单》，注明介质编号、存储内容、报废原因，经安全运营部、安全策略委员会两级审批；b、销毁方式区分：磁性存储介质执行 5 次以上随机数据覆写+专业消磁；固态盘、光盘采用物理粉碎切割；c、销毁操作全程双人在场、视频录像留存，同步登记销毁台账，记录介质编号、销毁时间、操作人员、监销人，销毁影像与审批单据一并归档，保存不少于 5 年；

（5）存储介质存放防护：涉密密钥、证书归档存储介质单独存放防磁保密柜，机房温湿度、磁场环境持续监控，防止介质损坏、数据丢失。

5.1.3. 电力保障

辽宁 CA 系统采用的单路供电，在电源中断时，使用不间断电源（UPS）供电，能确保在外部电力中断后，支撑关键系统正常运行至少 4 小时。备用柴油发电机应能在规定时间内（2 小时内）启动并接管负载，确保业务连续性。

5.1.4. 门禁与监控

机房管理严格按照辽宁 CA 的规定要求，采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等监控技术，设施内部分为公共区、服务区、管理区和核心区，以确保物理通道的安全。

非公共区域（包括服务区、管理区、核心区）的视频监控记录和门禁访问记录的保存时限为 6 个月。过期记录在销毁前进行安全审计，形成的审计报告存档备查；

5.1.5. 灾备

辽宁 CA 对重要数据实施异地备份，备份地点为沈阳数据中心，地址为：沈阳市和平区北八马路七巷 4 号，距离辽宁 CA 机房 5 公里。

数据备份每日备份，每周同步至备份中心。

5.1.6. 环境保障

辽宁 CA 机房配备恒温恒湿机房精密空调，确保机房 24 小恒温恒湿，相对湿度在 40%-60%范里内，保持温度在 18-28℃范围内。同时配备了漏水检测系统，防止水侵蚀，充分保障系统安全运行。

5.1.7. 消防措施

辽宁 CA 机房配备了联动的火灾自动报登系统和自动灭火系统，包含温度和烟雾检测功能，同时机房配备了气体灭火系统和专用空气呼吸器，辽宁 CA 定期组织进行消防安全检测。

5.1.8. 设备管理

辽宁 CA 制定了规范的设备管理制度以确保设备安全稳定。基于管理制度建立了设备台账，明确了每台设备的责任人、使用状态、维护周期和报废标准；同时，定期讲行设备盘点和核对，确保设备实际情况与设备台账相符。

5.1.9. 存储媒体管理

辽宁 CA 确保存储媒体安全可靠的存放，采用必要手段避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏。

辽宁 CA 制定了详细的存储媒体使用、报废管理规定，规定包含使用权限、报废标准、销毁方法和审批流程，同时完整记录存储媒体领用、归还、报废等情况。

5.1.10. 废物处理

当电子认证服务机构保存的相关数据已不再需要或存档的期限已满时，辽宁CA将完全销毁这些数据。数据销毁前进行安全审计，形成的审计报告存档备查，销毁行为遵守我国的法律。

5.2. 操作过程控制

5.2.1. 可信角色

电子认证服务机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。可信角色包括：

1. 系统管理员：负责系统策略配置、用户与权限管理等；
2. 技术运维员：负责物理环境、网络、服务器及系统软件的日常监控与维护等；
3. 数据库管理员：负责数据库进行日常运维、性能优化及数据备份等；
4. 系统审计员：负责系统和网络日志的审计、管理、审计报告生成等；
5. 密钥管理员：负责根证书密钥材料管理、根证书密钥生命周期管理等；
6. 业务操作员：负责证书申请的受理、审核，订户的身份与意愿签证；
7. 客户档案管理员：负责客户证书相关档案资料的归档与保密等；
8. 运营审计员：负责对客户签发、客户服务等核心业务进行独立。

5.2.2. 职责分离

辽宁CA对与运行和操作相关的职能有明确的分工,贯彻互相牵制的安全机制。所有辽宁CA的在职人员，必须通过认证后，根据作业性质和职位职能的需要，发放系统操作卡、门禁卡、登录密码、操作证书、作业帐号等安全令牌。辽宁CA系统将独立完整地记录其所有的操作行为。

辽宁CA所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色均实现双人操作或复核机制；涉及业务连续性相关操作（运维、鉴证、审计等）的角

色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止相互兼任：

a) 系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任；

b) 同一证书业务的录入与审核环节不得由同一业务操作员完成；

c) 业务操作员、客户档案管理员、运营审计员之间不得兼任；

d) 密钥管理员不得与系统管理员、技术运维员兼任；

e) 密钥管理员不宜与除策略管理机构成员外的其他可信角色兼任。

5.3. 人员控制

辽宁 CA 建立了覆盖人员入职、在岗、离岗全生命周期的人员安全管理体系，确保所有接触核心系统、密钥材料、订户信息的可信人员均满足严格的资格要求与持续培训标准。

5.3.1. 可信人员资格要求

辽宁 CA 对所有被定义为“可信角色”的人员（包括系统管理员、技术运维员、数据库管理员、系统审计员、密钥管理员、业务操作员、客户档案管理员、运营审计员等）在录用前及岗位变更时，执行以下资格核实流程：

a）从业经历与背景调查：通过公安、人社等权威渠道核实人员履历，完成包括无犯罪记录在内的严格背景审查。关键岗位（密钥管理员、系统管理员、审计员）的调查年限覆盖其最近不少于 5 年的从业经历。调查结果形成书面报告，由安全策略委员会审核并存档。

b）专业能力要求：具备履行岗位职责所必需的专业技能，包括但不限于：PKI/密码技术基础知识、电子认证服务相关法律法规、本机构 CPS 及管理制度、岗位专属操作流程等。关键岗位人员须持有国家认可的密码或信息安全相关资格证书。

c）保密协议：所有可信人员上岗前必须签署具有法律约束力的保密协议，明确承诺不得私自保存、复制、泄露或向任何第三方提供电子认证服务过程中接触

的任何秘密或敏感信息（包括但不限于密钥材料、订户信息、审计日志、系统配置等），并承担违反协议的法律责任。

d）劳动合同：所有可信人员须与辽宁 CA 签订正式劳动合同，合同期限与其岗位重要性相匹配。劳动合同中应明确信息安全责任条款及违规后果。

e）定期复核：对可信人员的资格进行年度复核，包括重新检查无犯罪记录、岗位能力考核、保密协议续签等。发现不符合资格要求的，立即调整其岗位或权限。

5.3.2. 培训要求

辽宁 CA 建立了覆盖所有可信角色的持续培训体系，具体规定如下：

a）岗前培训：所有可信人员上岗前，必须完成不少于 20 学时的岗前培训，并通过严格的理论与实践考核。未通过考核者不得上岗。培训记录（包括培训内容、学时、考核成绩、讲师签字、学员签字）由人力资源部门归档保存。

b）持续培训：每名可信人员每年至少接受一次集中培训，每人每年培训总时长不少于 20 学时，并通过年度考核。考核不合格者暂停权限，经补考合格后方可恢复。连续两次考核不合格的，调离可信岗位。

c）培训内容：培训内容应全面覆盖电子认证服务的各项知识与技能要求，至少包括以下 10 项：

(1) 电子认证服务相关法律法规与标准（如《电子签名法》《密码法》《个人信息保护法》《电子认证业务规则规范》等）；

(2) 岗位通用职责要求及各角色特定的工作要求；

(3) 内部管理政策、制度及流程（包括安全策略、事件报告、变更管理等）；

(4) PKI 和密码技术基础知识（包括对称/非对称密码、数字签名、哈希算法、SM2/SM3/SM4 等国密算法）；

(5) 本机构《电子认证业务规则》（CPS）及所遵循的证书策略（CP）；

(6) 安全管理策略和机制（包括访问控制、密钥管理、审计、灾难恢复等）；

(7) 订户身份查验和审核策略与流程（包括各类证书的身份验证方法、意愿记录、资料保存等）；

(8) 电子认证服务运营体系构成（包括CA、RA、受理点架构、服务流程、投诉处理等）；

(9) 电子认证服务技术体系构成(包括证书签发系统、密钥管理系统、OCSP/CRL服务、时间戳服务等）；

(10) 灾难恢复和业务连续性管理(包括应急预案、演练流程、故障处置等)。

d）培训记录与效果评估：所有培训活动（包括计划、签到、课件、考试答卷、成绩单、效果评估报告）应完整归档，保存期限不少于相关证书失效后五年。每年进行一次培训效果综合评估，评估结果用于改进后续培训计划和人员考核。

5.4. 审计日志程序

5.4.1. 记录的范围

辽宁CA的CA和RA运行系统，记录所有与系统相关的事件，以备查阅。这些记录，无论是手写、书面或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段及事件相关的实体等。

辽宁CA持续、完整地记录的操作与事件，包括但不限于：

a）根证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；

b）系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；

c）系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；

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

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

明确记录；

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

5.4.2. 记录的内容

每个事件记录均包含时间、类型、内容、操作人、作用对象及结果。对系统的关键操作均由操作人员进行电子签名。

5.4.3. 保存期限

辽宁 CA 在数据库保存相关记录至少两个月，系统日志离线存档至少保存至相关证书失效后五年，并实施严格的访问控制以防篡改或删除。

5.4.4. 日志审计

审计人员对记录进行审计，核实系统和操作人员的合规性，包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件；

审计周期:应至少每季度对系统日志进行一次审计，形成审计报告，并基于结果采取改进措施。

5.4.5. 处理日志的周期

辽宁 CA 安全管理员每季度对系统日志进行一次全面的安全审计日志分析，形成审计报告，并基于审计结果采取改进措施。

5.4.6. 审计日志的保护

辽宁 CA 执行严格的通道管理，确保只有辽宁 CA 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，并且有异地备份，严格禁止访问、阅读、修改和删除等操作。

5.4.7. 审计日志备份

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

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

所有审计日志必须进行异地备份。异地备份点具备与主系统相当的安全防护等级，每月进行一次异地备份，备份数据的保留期限应符合本 CPS §5.4.3 的规定。

5.5. 记录归档

5.5.1. 归档范围

辽宁 CA 会对 CA 的数据库定期存档，间隔时间由辽宁 CA 自行决定，存档的内容包括辽宁 CA 发行的证书和 CRL、审查数据记录、证书申请审批资料等。（签名私钥由实体本身保存，有关私钥的责任由实体本身承担）。

归档范围：证书申请材料和订户意愿记录；所有审计日志；密码设备全生存周期管理记录；密码设备的日常操作与使用记录；根证书或密钥生存周期管理相关的全部记录；证书认证系统运行日志；已识别的安全事件及处置记录；证书认证系统关键操作日志；电子认证服务过程中其他操作记录。

5.5.2. 保存期限

订户相关档案、系统日志和审计记录将保存至相关证书失效后五年。

5.5.3. 保护措施

辽宁 CA 的档案室具备完善的物理安全措施，包括但不限于：独立的门禁系统、视频监控、防水（如远离水源、窗户密闭防渗）、防火、温湿度检测，以及防磁、防尘等。归档记录的存储环境满足国家关于档案长期保存的相关标准。

只有经过授权的工作人员按照特定的安全流程才能进入档案室。

所有存档文件的数据库除了保存在辽宁 CA 的主要存储库，还将在异地保存其

备份。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。辽宁 CA 在安全机制上保证禁止对档案及其备份进行修改、删除等操作。

辽宁 CA 每年会验证存档信息的完整性。

5.6. 电子认证服务机构根证书密钥更替

5.6.1. 密钥更替程序

辽宁 CA 根证书密钥更替的流程与情形，包括但不限于：

1. 密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，具体见本 CPS 6.6.2；

2. 根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；

3. 旧密钥处理：在完成签名密钥更替后，按 GB/T 25056-2018 中 8.2.4.3 规定的方式，销毁旧私钥及其备份，并保留相关操作记录。。

5.6.2. 密钥更替的时间：

紧急更替：辽宁 CA 在发现密钥泄露或存在安全隐患时，将立即启动密钥更替程序；

到期更替：在密钥到期前二年完成密钥更替。

5.7. 损害与灾难恢复

为应对机房故障、系统瘫痪、数据损坏、根密钥泄露等突发事件，保障电子认证业务连续性，辽宁 CA 建立损害与灾难恢复预案与流程，定期开展恢复演练，确保在各类灾害场景下，业务服务可按预定目标恢复。

5.7.1. 业务连续性目标

恢复的时间目标(RTO)——最大可允许中断时间为 24 小时。

恢复的数据点目标(RPO)——数据损失可允许将数据恢复到24小时内的水平；

5.7.2. 恢复流程

5.7.2.1. 证书库恢复流程

环境重建：恢复安全运行环境（包括网络、服务器、密码模块、防火墙等），并完成安全加固与访问控制配置。

数据恢复：从异地备份介质中恢复证书库、CRL/OCSP 数据、签发日志及相关业务数据，恢复后进行数据完整性与一致性校验。

受影响证书处理：根据故障时间点，梳理受影响的证书列表，对因故障导致服务中断期间无法正常使用的证书，按业务规则进行撤销或冻结处理，并生成撤销列表发布。

订户密钥处理：对未受影响的订户私钥，不做额外处理；对因故障导致证书失效或撤销的订户，按流程通知其重新申请证书，并指导用户生成新的密钥对。

证书重发与恢复服务：完成数据恢复与校验后，恢复证书签发、查询、状态服务，并向受影响订户提供公钥证书的补发、下载与状态验证服务。

5.7.2.2. 根密钥损害的恢复流程

当辽宁CA的根密钥损害时，将会执行以下程序进行恢复：

安全环境重建：在物理隔离的核心区，重建根证书签发的安全运行环境，启用专用密码模块与密钥管理系统。

根密钥更替准备：启动根密钥更替预案，生成新的根密钥对与根证书，确保新根证书符合国家密码算法与格式要求。

订户证书重签发：根据原根证书签发的所有证书列表，使用新根密钥重新签发订户证书，并更新证书链信息。

证书链更新与发布：更新并发布新的证书链，同步更新 CRL/OCSP 服务，通知依赖方更新信任列表。

旧根证书处置：按国家密码管理相关要求，安全销毁旧根私钥，并对旧根证

书进行标记与归档。

5.7.2.3. 其他关键资产恢复流程

- **物理设施恢复**

机房机柜、加密机、电源、安防等物理设施发生故障或损毁时，应第一时间排查故障原因、损坏程度及影响范围，并隔离故障设备。若为轻微故障，可现场维修调试；若设备彻底损毁，则启用备用件替换，优先保障核心 CA 设备、密钥存储及证书服务设备的运行。设备修复或替换后，需完成通电测试、功能调试与安全检测，同步恢复机房供电、温湿度、消防、安防等环境，并排查线路与接地系统隐患，确保机房物理安全。

- **计算资源恢复**

当服务器、虚拟机或集群出现宕机、过载、节点离线等异常时，通过运维监控平台定位故障节点及异常日志。下线并隔离异常节点，重启故障服务；若集群发生故障，启动自愈机制，将核心业务迁移至正常备用节点。修复服务器系统与集群配置，清理异常进程；若资源不足，及时扩容内存与存储。完成后校验算力稳定性、集群同步性及业务承载能力，恢复全量业务运行。

- **网络环境恢复**

针对内外网、专线、防火墙等网络设备及链路出现的中断、入侵、策略失效等问题，应临时关闭异常端口、封禁非法 IP、阻断恶意访问，隔离安全风险。随后修复故障设备与链路连接，还原合规访问策略与路由配置，优化网络防护规则，确保内网隔离、外网可控、专线稳定。最后测试网络连通性、传输稳定性与权限合规性，确认安全后恢复正常业务交互。

- **软件系统恢复**

当 CA 系统、数据库等出现闪退、篡改、瘫痪等故障时，应根据程序漏洞、配置错误、病毒攻击等不同原因分类处置。若为轻微配置异常，可直接还原标准配置；若存在程序损坏、文件缺失或病毒感染情况，则需彻底清理后通过备份数据进行恢复。修复完成后，需对证书签发、查询、审计等核心功能开展全量测试，确保软件运行稳定、业务功能正常。

- **业务数据恢复**

当证书数据、操作日志、订户信息等发生丢失或篡改时，应首先评估数据损坏范围与恢复难度，采用最近的离线及异地定时备份数据进行恢复；恢复过程中需严格遵循 RPO（恢复点目标）、RTO（恢复时间目标）指标，控制恢复时效与数据丢失量，并禁用可疑备份数据。恢复完成后，需核查数据的完整性、准确性与一致性，补录并修正异常数据，确保业务数据完整且可追溯。。

5.7.3.根私钥应急处理

a）应急响应时间：发生根私钥泄露或疑似泄露事件时，辽宁 CA 将在 1 小时内启动应急预案。

b）责任人员：由公司主要负责人担任应急总指挥，运维部、技术部、综合部负责人为核心成员，成立根密钥泄露应急小组。

c）处置步骤：

(1) 立即隔离受影响系统，暂停根证书签发及相关服务；

(2) 启动根密钥更替流程，生成新的根密钥对与根证书；

(3) 撤销原根证书及所有由其签发的证书，发布 CRL 并通知所有依赖方；

(4) 排查泄露原因，采取技术与管理措施防止再次发生；

(5) 完成系统恢复与业务切换，恢复正常服务。

d）上报机制：事件发生后 24 小时内上报公司管理层与行业主管部门，并按监管要求提交事件报告。

e）应急演练：每年开展一次根私钥泄露应急演练，检验预案的有效性与团队的处置能力。

5.7.4.事件报告

灾难事件发生后，按本 CPS 第 5.9 节 “重大事项报告” 的要求，及时向公司管理层、行业主管部门及相关方报告事件情况、处置进展与结果。

5.7.5.定期验证与演练

备份验证：每季度对备份设备与数据进行可用性测试，包括数据恢复测试、功能验证与完整性校验。

灾难恢复演练：每年至少开展一次全面的灾难恢复演练，覆盖证书库恢复、根密钥恢复、系统切换、应急响应等关键流程，形成演练报告，并根据演练结果修订预案。

5.8. 电子认证服务机构或注册机构的终止

为规范辽宁CA电子认证服务终止后的业务处置，保障订户与依赖方的合法权益，根据《电子签名法》《电子认证服务管理办法》及相关标准，制定本条款。

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

具有资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围与 责任；向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；停止证书状态服务并归档相关数据；停止其他电子认证相关服务并归档相关数据；停止密码设备并归档相关密钥数据；及时撤销或冻结业务管理员和业务操作员的操作权限；对所有存档文件记录进行整理和封存；对所有敏感文档和数据进行安全处理和封存；清除主机和密码硬件设备中的敏感数据；其他涉及CA 运营的数据、密钥安全的操作。

5.8.1.终止类型与条件

主动终止：因经营调整、业务转型等原因主动申请终止电子认证服务。

被动终止：因资质被撤销、吊销、业务许可到期未续期或被主管部门责令停止服务。

终止前提：无论主动或被动终止，均须完成证书撤销、数据移交、用户告知、主管部门报备等全部合规流程。

5.8.2. 终止前准备

预案制定：提前制定机构终止专项预案，明确处置流程、责任部门、时间表与工作分工。

承接机构确认：完成与具备电子认证服务资质的承接机构的沟通和协议签署，确保用户证书业务平稳移交。

5.8.3. 用户与依赖方告知

提前告知时限：

提前 90 日通过官网公告、短信、邮件、系统通知等方式，向所有订户、依赖方发布终止公告。

公告内容包括：终止日期、证书处理方式、数据移交安排、新服务机构信息、用户操作指引、咨询渠道。

特殊用户通知：

对高等级证书用户、重要机构用户进行一对一电话或书面通知，确保其知悉并完成证书迁移或变更。

5.8.4. 证书与密钥处置

证书撤销：在终止日前，对所有有效证书进行批量撤销，发布最终 CRL 并长期维护，直至所有证书过期。

私钥处置：根私钥、RA 私钥、系统私钥等核心密钥，按密码管理规定进行安全销毁，形成销毁记录并长期归档。

订户密钥：通知订户及时备份或迁移自身私钥，机构终止后不再提供订户私钥托管、恢复服务。

5.8.5. 数据移交与留存

数据移交：将用户申请材料、身份核验记录、证书签发日志、审计日志、归

档证书等数据，完整移交至承接机构，并签署移交确认文件。

数据留存：对法律法规要求留存的数据，按规定期限（证书失效后至少 5 年）加密归档，妥善保管，满足后续法律、审计、监管追溯需求。

5.8.6. 主管部门报备

提前报备：在终止前 60 日，向工信部、密码管理局等主管部门提交终止申请与处置方案。

后续报告：终止完成后，提交处置情况报告、数据移交证明、密钥销毁记录，接受主管部门监督检查。

5.8.7. 服务终止与过渡

业务关停：终止日起，停止所有证书签发、更新、续期、撤销、状态查询等电子认证服务。

服务过渡：与承接机构配合，为用户提供证书迁移、变更指引，确保用户电子签名业务平稳过渡，不因机构终止影响业务连续性。

5.9. 重大事项报告

为落实监管要求，规范重大事项报告流程，辽宁 CA 建立重大事项报告制度，明确事件发生后向公司管理层、上级机构和主管部门报告的程序、时限与内容。重大事件包括但不限于：证书认证系统迁移或改造、重大安全事故、订户信息泄露事件、合规性事件、人力资源类事件。

5.9.1. 证书认证系统迁移或改造

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

(1) 机房迁移，或机房内服务区、管理区或核心区划分范围改变；

(2) 变更电子签名认证证书签发逻辑；

(3) 新增远程证书注册子系统；

(4) 新增、更改或者删除用于签发电子签名认证证书的证书链；

(5) 其他对电子认证服务安全、用户资料安全有影响的改变。

实施改造/迁移方案正式定稿后 3 个工作日内完成向主管部门事前报备；改造施工完成、系统上线试运行当日完成事后书面报送。

5.9.2. 重大安全事故

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

(1) 证书签发及验证服务连续停机时间超过 24 小时；

(2) 发生根证书密钥等关键数据泄露；

(3) 持续或较大范围未经授权的私钥访问记录或其他异常活动；

(4) 系统日志持续或较大范围显示异常操作，如非授权时间或网络地址访问敏感功能。

事件确认发生后，第一时间电话紧急告知监管单位，两个工作日内提交加盖公章正式书面报告；处置过程出现事态变化、次生风险及时续报，事件闭环后提交完整处置复盘报告。

5.9.3. 订户信息泄露事件

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

(1) 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；

(2) 数据丢失导致无法恢复证书状态信息。

事件核实认定完成后 3 个工作日内向主管部门提交书面报告，同步落实用户告知、漏洞封堵工作。

5.9.4. 合规性事件

订户信息泄露事件包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：

(1) 涉及电子认证服务的司法判定；

(2) 收到行政部门违规通知或处罚决定。

收到司法文书、行政文书当日内部上报公司管理层，3 个工作日内向监管主管部门报送情况说明。

5.9.5. 人力资源类事件

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

(1) 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；

(2) 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

人事异动、生效法律文书出具后 3 个工作日完成内部管理层报备及主管部门报送。

6. 认证系统技术安全控制

6.1. 技术安全管理制度要求

辽宁 CA 建立并实施覆盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，并 定期接受安全策略委员会的评审，频率不低于每年一次。

6.2. 密钥对的生成和安装

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则，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。

6.2.1. 根证书密钥对的生成与安装

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

6.2.2. 订户密钥对的生成和交付

订户签名密钥对的生成与交付符合以下要求之一：

1．由订户持有符合国家密码管理要求的密码模块中生成并存储；

2．由辽宁 CA 生成并保存的订户签名密钥对，辽宁 CA 将通过技术措施确保订户对签名私钥的独占控制权。辽宁 CA 会完整记录与订户签名私钥相关的所有操作日志，包括操作时间、操作方式、操作人员等信息，保存期限应不少于证书失效后五年；

3．采用通过主管部门认可的其他创新性保护方案。

订户加密密钥对由辽宁省密钥管理中心（以下简称 KMC）负责生成、控制与保存管理。

6.3. 私钥保护和密码模块工程控制

6.3.1. CA 私钥保护和密码工程控制

辽宁 CA 根证书私钥保护使用通过国家密码主管部门认可的密码产品，符合 GB/T 37092—2018 第 5 章的要求；根证书私钥实施严格的 5 选 3 分割保护机制，实现单人无法获取完整私钥；根证书私钥备份由密钥管理员分别保存在有防盗措施的安全场所。

辽宁 CA 采用多人控制策略激活、使用、停止辽宁 CA 的签名密钥。

6.3.2. 订户私钥保护和密码模块工程控制

订户签名私钥保护方式有订户持有与订户委托保管两种方式。

订户签名私钥由订户持有：协议中要求订户采取预防措施防止私钥及其激活数据的丢失、泄 露、更改或未经授权的使用。

CA 受订户委托保管订户签名私钥，明确以下内容：

- 采用的电子签名模式；
- 采用的安全控制措施，并定期进行安全评估；
- 每次签名私钥调用必须获得订户的明确授权，授权记录应完整保存；
- 向订户提供关于签名私钥及激活数据安全使用的指导与建议；
- 电子签名模式和控制措施应符合相关标准或采用经主管部门认可的其他方式。

6.4. 密钥对管理的其他方面

6.4.1. 公钥归档

辽宁 CA 建立公钥证书定期归档机制，对所有签发的公钥证书（包括当前有效、已过期、已撤销证书）进行自动归档。

归档工作按日执行，归档间隔不超过 24 小时，归档数据包含证书文件、签发日志、撤销记录及相关状态信息。

归档数据采用加密方式存储于离线安全介质，保存期限不短于证书失效后5年，以满足历史电子签名验证、审计及监管追溯需求。

6.4.2. 证书操作期和密钥对使用期限

无论是订户证书还是辽宁CA证书，证书到期后，签名私钥不可用于电子签名，辽宁CA根证书密钥对有效期不超过20年，订户证书密钥对有效期不超过10年，其他证书密钥，包括相关服务器证书密钥、时间戳密钥等有效期不超过10年。特殊情况下，对于签名证书，为验证在证书有效期内签名的信息，公钥可以在证书有效期限以外使用。

6.5. 激活数据

6.5.1. 激活数据的产生和安装

激活数据包括辽宁CA提供的证书私钥口令、被加密的数据等。

根密钥激活数据由不少于5名密钥管理员分别独立生成、分段保管，单份激活数据无法单独启用根密码设备；

订户硬件介质激活数据由用户自主设置，CA仅提供复杂度规范，不代为生成、存储用户完整激活口令；

激活数据设置强制复杂度规则：长度不少于8位，硬件条件允许时建议采用大小写字母+数字+特殊符号组合，禁止简单连续字符、生日、手机号弱口令。

（1）激活启用方式（多方式安全控制）

核心密码设备、根密钥加密机强制采用多因子复合激活方式，采用“分段口令+人员身份核验”组合校验模式；

订户USB-KEY硬件介质支持口令激活方式，由订户自主设置。

（2）激活数据使用过程安全管控

根密钥激活分段口令仅可在机房物理隔离核心屏蔽区内当面核验输入，禁止远程传输、线上发送激活明文数据；

每次激活密码设备、调取私钥资源，均留存操作人员、核验人员、操作时间、

操作用途审计日志，日志长期加密归档；

激活口令连续5次错误输入，密码设备自动锁定，必须经两名管理员现场核验身份后方可执行解锁操作；

运维人员仅可临时使用当期有效激活数据，使用完毕不得缓存、复制、截屏留存任何激活明文信息。

（3）激活数据销毁安全控制措施

根密钥迭代更替、密码设备报废、系统下线场景情况下，原有分段激活数据由全体密钥管理员现场见证，完成明文擦拭、配置文件删除，同步销毁纸质口令封存载体；磁性存储载体执行多次数据覆写销毁，纸质载体现场粉碎销毁；

订户介质挂失、注销、停止服务场景：介质内本地激活标识随密钥一同清零销毁，CA不留存用户激活口令备份数据；

所有激活数据销毁行为履行双人审批、全程视频录制，填写销毁记录表，记录销毁对象、时间、监销人、处置方式，销毁资料归档留存不少于5年。

6.5.2. 激活数据的保护

激活数据传输、静态存储全程采用国密SM4算法加密，禁止明文存储、明文网络传输；

采用多因子验证机制启用核心密码设备，单一激活数据无法完成密钥调用；

连续10次错误输入激活数据，设备自动锁定，需管理员现场核验身份后方可解锁；

根密钥分段激活数据异地分介质分开存放，互不互通，杜绝单人集齐全部激活因子；

6.6. 计算机安全控制

辽宁CA的数字证书签发系统的数据文件和设备由辽宁CA系统管理员维护，未经辽宁CA系统管理员授权，其它人员不能操作和控制辽宁CA系统；辽宁CA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；辽宁CA系统密码有最

小密码长度要求，而且必须符合复杂度要求；辽宁 CA 系统管理员定期更改系统密码。

辽宁 CA 机房管理员至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；对所有服务器和操作终端安装杀毒软件； 病毒库更新间隔；病毒扫描时间间隔。

6.7. 生命周期技术控制

辽宁 CA 按照《GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范》相关要求，建立并实施了以证书认证中心、密钥管理中心以及证书操作流程为核心的生存周期安全控制体系。

6.8. 网络的安全控制

辽宁 CA 建立并实施符合《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056—2018）要求的网络安全控制体系，覆盖网络结构、边界防护、访问控制、安全审计、安全防护、监控分析等环节，确保证书签发系统、证书注册系统、数据库及相关关键系统的网络安全可控、可追溯、可验证。

6.8.1. 网络结构

辽宁 CA 核心业务系统网络结构采用符合 GB/T 25056—2018 附录 A 规定的多级隔离架构，按功能划分为核心区、管理区、服务区、公共区，各区域间通过防火墙或安全网闸进行逻辑隔离，禁止跨区域无限制访问。

证书签发子系统、数据库、密码设备部署在核心安全网段，证书注册子系统、业务服务系统部署在服务区，管理运维终端仅允许接入管理区，互联网访问通过 DMZ 区实现，严格限制进出核心区的流量。

6.8.2. 网络管理

建立并维护网络拓扑图，包含所有网络设备、服务器、安全设备、连接关系

和安全边界，定期更新，与机房实际情况保持一致，并归档留存，可现场核验；所有授权用户必须有合法的安全令牌，并且通过密码验证。

6.8.3. 网络边界与 Web 服务防护

所有互联网边界、区域边界均部署下一代防火墙，配置严格的访问控制策略，仅开放业务必需的端口与协议，禁止不必要的外部访问。

面向互联网的 Web 服务统一部署 Web 应用防火墙（WAF），启用 SQL 注入、跨站脚本（XSS）、命令注入、恶意爬虫等防护规则，规则定期更新，日志留存不少于 6 个月。

网络边界部署入侵检测系统（IDS/IPS），实时监测并阻断端口扫描、暴力破解、异常流量、恶意代码传播等攻击行为，告警信息实时推送至运维监控平台。

对互联网出口流量实施内容过滤，禁止访问恶意站点、违规资源，防范钓鱼、木马等外部威胁。

6.8.4. 网络访问控制

证书签发子系统及数据库仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问，建立 IP 地址白名单机制，非白名单地址一律禁止访问。

证书注册子系统及相关业务数据库同样实施访问白名单机制，仅允许业务系统、授权运维终端接入，禁止外部直接访问。

所有远程运维操作仅通过国密 VPN 或加密通道接入，运维终端 IP、账号、权限实行最小化管理，双人双因素认证后方可登录，操作全程留痕。

禁用 Telnet、FTP、HTTP 等明文协议，所有管理访问统一使用 SSH、HTTPS 等加密协议，禁用弱加密算法。

6.8.5. 网络监控

辽宁 CA 至少每月对系统日志进行分析；分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

所有网络安全设备（如防火墙、入侵检测系统）均开启日志功能，并对日志进行集中收集、保护并定期审计，保存期限不低于 6 个月。

对安全事件进行分类、溯源与复盘，分析事件原因、影响范围，更新防护策略与应急预案，防止同类事件再次发生。

6.8.6. 安全审计系统

建立集中式安全审计系统，对涉及系统安全的行为、人员、时间进行跟踪、统计与分析，支持对各子系统日志的集中查询与审计，可直接查询证书/证书撤销列表存储与发布系统的数据库日志。

日志记录的主要内容包括：

a) 操作员姓名；

b) 操作项目（如证书签发、撤销、更新、密钥管理、系统配置变更等）；

c) 操作起始时间；

d) 操作终止时间；

e) 证书序列号（涉及证书操作时）；

f) 操作结果（成功 / 失败）；

g) 操作 IP 地址、终端信息。

日志管理的主要内容包括：

a) 日志参数设置：配置日志保存的最大规模、日志备份目录与自动备份策略；

b) 日志查询：支持按操作员、操作事件、时间范围、证书序列号等条件查询；

c) 日志备份：当日志达到预设规模或定期周期时，自动备份日志至离线存储介质；

d) 日志处理：对正常业务流量、各类事件进行分类整理、统计分析，识别异常行为；

e) 证据管理：对审计发现的证据数据进行审计、统计和记录，确保证据完整、不可篡改。

日志保存期限不少于证书失效后 5 年，关键安全事件日志永久归档，每季度开展一次日志审计，形成审计报告。

6.8.7. 安全防护系统

访问控制：通过防火墙、安全网闸、白名单、账号权限管理等技术手段，实现对网络资源的分级、分域、分角色访问控制，禁止越权访问。

入侵检测：部署入侵检测系统，实时监测网络中的异常访问、攻击行为，发现违规访问立即告警并阻断。

漏洞扫描：定期对网络设备、服务器、业务系统进行漏洞扫描，每季度至少一次，发现高风险漏洞及时修复，形成扫描报告与整改记录。

病毒防治：服务器、运维终端部署防病毒软件，定期更新病毒库，启用实时防护，防止恶意代码感染与传播。

数据传输加密：核心业务数据、身份信息、日志数据传输过程中采用国密算法加密，防止数据被窃听、篡改。

6.9. 时间戳

辽宁 CA 暂时不提供时间戳服务。

7.证书、证书撤销列表和在线证书状态协议

7.1. 证书

辽宁 CA 全部电子签名认证证书采用 X.509V3 版本，严格遵循 GB/T20518《信息安全技术 公钥基础设施 数字证书格式》标准。证书承载内容包括：

1．支持的数字证书格式版本号；

2．密码算法对象标识符；

3．辽宁 CA 的机构名称和订户的名称；

4．证书策略对象标识符，其中包含主管部门制定的相应等级证书策略 OID(见 1.5.1)，也根据业务需求包含辽宁 CA 制定或遵循的证书策略 OID；

5．证书序列号；

6．证书有效期；

7．订户的电子签名验证数据；

8．辽宁 CA 的电子签名。

依据 T/CQAE 11034-2025 要求，本 CPS 在各章节明确了证书用途与适用限制、

证书申请签发建立流程、订户签名私钥保存方式、证书适用法律法规与法律权责等内容，便于订户、依赖方完整知悉证书内容、使用边界与法律权责。

7.2. 证书撤销列表

7.2.1.CRL 格式

CRL 格式符合 GB/T 20518 要求，采用 X.509 V2 版本。

7.2.2.CRL 发布与更新

发布频率：每 24 小时至少发布一次；

最大滞后时间：证书撤销后 1 小时内进入 CRL；

发布地址：辽宁 CA 官网（www.lnca.org.cn）公开下载；

7.2.3. CRL 内容

CRL 包含以下内容：

- 颁发者信息
- 本次更新时间、下次更新时间
- 已撤销证书序列号、撤销时间、撤销原因
- 颁发者数字签名

7.3. 在线证书状态协议（OCSP）

7.3.1. OCSP 服务符合标准

辽宁 CA 为证书用户提供 OCSP（在线证书状态查询服务），服务符合 GB/T 19713-2025《信息安全技术 在线证书状态协议规范》。

7.3.2. 服务可用性

OCSP 实时查询服务可用率≥99%，7×24 小时连续运行。

7.3.3. OCSP 响应内容

- 证书状态：正常/撤销/未知
- 证书序列号
- 验证时间
- 响应者签名
- 有效期

7.3.4. OCSP 访问地址

OCSP 地址在证书 AuthorityInfoAccess 扩展中携带，通过官网公开。

8. 认证机构审计和其他评估

8.1. 审计与评估概述

辽宁 CA 依据《电子签名法》、《商用密码管理条例》及《电子认证业务规则规范》（T/CQAE 11034-2025）要求，建立常态化审计与符合性评估体系，对电子认证服务活动、技术系统、管理流程、人员操作、安全控制等实施全面、独立、可追溯的审计与评估，确保持续满足合规与安全要求。

评估类型包括：年度全面符合性评估、定期业务审计、专项安全审计、事件触发审计。

8.2. 评估频率与触发条件

a) 年度全面符合性评估：每年至少开展一次，于次年 1 月底前将上一年度评估报告报送行业主管部门。

b) 定期业务审计：每季度至少开展一次认证业务审计。

c) 专项安全审计

发生以下情形时立即开展：

- 密钥泄露、系统入侵、数据泄露等重大安全事件；
- 核心系统重大升级、架构变更、机房迁移；
- 主管部门要求开展专项检查。

d) 评估方式：通常采用内部评估，在监管部门要求下也可委托具备资质的第三方机构开展评估。

8.3. 评估者资质与独立性

8.3.1. 内部评估

内部评估时，由安全策略委员会组织会议组建内部评估小组，由评估小组执行内部审计评估工作。

评估人员具备以下背景之一：

- 电子认证、密码学、网络安全、信息安全相关专业；
- 具备 2 年以上 CA/RA 运营、证书业务、安全审计经验；
- 熟悉《电子签名法》《电子认证业务规则规范》及证书策略（CPS）；
- 无利益冲突、与被审计岗位无直接隶属关系

8.3.2. 外部审计

采用外部审计时，外部评估机构需满足：

- 具备密码安全/电子认证相关服务资质或省级以上主管部门认可的第三方评估资质；
- 近 3 年无违法违规记录、无行业处罚；
- 项目团队成员具备电子认证、密码、网络安全专业能力；
- 签署保密协议，对审计过程及数据严格保密。

评估人员应具备以下条件之一：

信息安全、密码学、电子认证相关专业背景；

2 年以上 CA/RA 运营、安全审计或风险评估经验；

熟悉《电子签名法》、电子认证服务相关标准及 CPS/CP 要求。

8.3.3. 独立性

评估人员必须保持独立性：

- 与被审计岗位无直接隶属关系；
- 无利益冲突；
- 不得审计本人参与的业务或系统。

8.4. 认证业务审计

a）审计周期：每季度一次；

b）审计内容包括但不限于证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、 身份查验、意愿记录、协议签署、资料保存的合规性；

c）审计采用抽样审计方式，抽样率不低于 1%；

8.5. 全面符合性评估

a）评估周期：每年一次；

b）评估内容包括但不限于：年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等；

c）审计采用抽样方式，抽样率不低于 1%；

d）对于审计发现的问题，5 个工作日内通报被审计部门；制定整改计划、明确责任人与时限；评估部门跟踪至完全闭环，纳入下年度评估重点；

e）在 1 月底前将上一年度符合性评估报告报送主管部门。

8.6. 问题整改与闭环管理

审计发现问题在 3 个工作日内 书面通报责任部门；一般问题整改期限不超过 15 天，重大问题不超过 30 天；整改完成后进行复核验证，形成闭环管理；未按期整改的，纳入部门与岗位考核，并向安全策略委员会报告。

8.7. 评估结果应用

审计与评估结果作为以下事项的重要依据：

- CPS 与证书策略（CP）修订完善；
- 系统安全改造与流程优化；
- 人员培训、岗位考核与权限管理；

- 风险处置、应急预案更新及资源投入决策；
- 主管部门合规报备与检查支撑材料。

9. 法律责任和其他业务条款

本部分涵盖了辽宁 CA 处理一般性的业务和法律问题的规范与原则。在业务条款中说明了辽宁 CA 不同服务项目的取费问题；辽宁 CA 体系的关联单位包括辽宁 CA 注册机构、受理点等，为了保证资源维持运营，针对各参与方的诉讼和审判提供支付所需承担的财务责任；法律责任条款则涉及保密、隐私、知识产权、担保及免责等内容。

9.1. 费用

辽宁 CA 依据服务成本核算制定价格策略，费用收取按辽宁 CA 明确指定时间生效的价目表执行，若没有指定生效时间的，自价目表公布之日起七天后生效。

收费项包括：证书颁发或更新费用；证书访问费用；撤销证书的费用；状态信息访问费用；电子签名的费用；签名验证的费用；签名验证报告的费用；其他服务的费用。

退款策略：辽宁 CA 数字证书一旦发放，辽宁 CA 不办理退证、退款手续。在用户已经交纳服务费期间，用户要退出辽宁 CA 数字证书服务的，辽宁 CA 不退还剩余使用时间的服务费。

收费标准公布：不同项目的服务收费不同，辽宁 CA 将通过营业厅价目表展示、服务电话或电子邮件告知、依赖方应用通知等方式公布对应收费标准和退款策略。

9.2. 财务责任

辽宁CA 准备赔付专项备用资金，资金保障额度不低于上一年度营业收入 1.5%，资金来源为自筹，由安全策略管理委员会指定专人专项管理，月度报告、年度审计的管理方式。

9.3. 业务信息保密

辽宁 CA 根据国家相应的法律法规制定并落实严格的信息保密规章制度，所有

相关人员（包括辽宁 CA 及辽宁 CA 授权的注册机构和受理点的工作人员）必须遵守该规章制度。由辽宁 CA 制定及实施的信息保密规章制度符合国家保密机构的相关规定。辽宁 CA 有权根据情况修改相关内容。

除非有法律明确规定和要求，否则有关递交证书申请的用户信息将由辽宁 CA 保密，并且在没有得到申请人授权的情况下不得泄露。

除非有法律明文规定，否则辽宁 CA 没有义务公布或透露用户所持有证书以外的信息。

9.3.1. 保密信息范围

保密信息范围是指有明确事实、数据表明此类信息的泄露、复制、传播等已经、正在或将要对证书持有方造成经济损失的信息。

以下信息应视为保密信息但不限于以下方面：

辽宁 CA 用户的数字签名及解密密钥，并且 CA 和 RA 均无权访问这些密钥。

保存在审计记录中的信息应由辽宁 CA 保密，除受法律要求，不可在公司外部发布。审计记录包括：本地日志、服务器日志、归档日志的信息，应对辽宁 CA 可视为保密，只有审计员和安全官员可以查看。除法律要求，否则不可在公司外部发布。年度审计结果也同样视为保密。

除去作为证书、CRL、和证书策略或本 CPS 一部分而公开出版的信息，其他由 CA 和 RA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

在双方披露时标明为保密（或有类似标记）的、双方根据合理的商业判断应理解为机密数据和信息的、以其他书面或有形式确认为保密信息的或从上述信息中衍生出的信息，也视为保密信息。

其他：辽宁 CA 信息的保密性取决于特殊的数据项和申请。

9.3.2. 不属于保密的信息

以下信息可视为不保密信息

由辽宁 CA 签发公钥证书和 CRL 中的信息。

由辽宁 CA 支持的证书策略中信息。

辽宁 CA 许可，只有辽宁 CA 用户方使用，在辽宁 CA 网站公开发布的信息。

用户证书撤消原因可以在撤消证书的 CRL 入口查到。其中撤消原因不视为保密信息，可为所有辽宁 CA 用户和可靠用户共享。

其他可以通过公共渠道获得的或经过用户许可的信息。

当辽宁 CA 在法律、法规或规章条款的要求下，或在法院的要求下必须披露本电子认证业务规则中具有保密性质的信息时，辽宁 CA 可以依从法律、法规或规章条款以及法院的判定的要求，向执法部门公布相关的保密信息。此种信息披露不视为违反保密的要求和义务。

9.3.3. 保护保密信息的责任

辽宁 CA 保证采取以下措施，实施对保密信息的保护：

除受相同保密义务约束的辽宁 CA 及辽宁 CA 授权的注册机构和受理点的工作人员外，辽宁 CA 不得向任何其他第三方披露保密信息；

除为办理认证业务的目的外，辽宁 CA 不得以任何其他方式使用保密信息；

辽宁 CA 采取与其保护自身保密信息和专有信息相一致的措施，防止保密信息被无权披露，在任何情况下，辽宁 CA 采取的保护措施应不低于合理的标准。

9.4. 个人隐私保护

对于个人隐私信息，辽宁 CA 会依据 GB/T 35273 管理规定，尽最大的努力进行保护。

a) 本机构收集、处理订户个人信息严格遵守 GB/T 35273 及个人信息保护相关法律法规，遵循合法、正当、必要原则，事前明示并取得信息主体同意，敏感个人信息获取单独同意。

b) 对个人信息实施加密存储、权限管控、日志留痕、异地备份，区分普通信息与敏感信息落实分级安全防护。

c) 个人信息仅限电子认证业务使用，未经同意不擅自共享、对外披露；依法保障主体查询、更正、删除、撤回同意等权利。

d) 业务资料按规定期限留存，到期数据安全销毁；发生个人信息安全事件按规范应急处置并上报。

e) 个人信息保护工作纳入常态化审计评估，持续合规运营。

9.4.1. 隐私保密方案

辽宁 CA 保证采取以下措施，实施对保密信息的保护：

a) 除受相同保密义务约束的辽宁 CA 及辽宁 CA 授权的注册机构和受理点的工作人员外，辽宁 CA 不得向任何其他第三方披露保密信息；

b) 除为办理认证业务的目的外，辽宁 CA 不得以任何其他方式使用保密信息；

c) 辽宁 CA 采取与其保护自身保密信息和专有信息相一致的措施，防止保密信息被无权披露，在任何情况下，辽宁 CA 采取的保护措施应不低于合理的标准。

9.4.2. 作为隐私处理的信息

证书申请实体在办理认证业务时提供的属个人隐私范围的信息，如家庭住址、私人电话号码。

9.4.3. 不被视为隐私的信息

证书申请实体的除隐私信息以外的其它信息。

其中与证书相关的信息是可以公开的，通过辽宁 CA 目录服务等方式向外公布。

9.4.4. 保护隐私的责任

辽宁 CA 保证采取以下措施，实施对个人隐私信息的保护：

a) 除受相同保密义务约束的雇员、代理人或独立订约人外，辽宁 CA 不得向任何其他第三方披露个人隐私信息；

b) 除为办理认证业务的目的外，辽宁 CA 不得以任何其他方式使用个人隐私信息；

c) 辽宁 CA 采取与其保护自身保密信息和专有信息相一致的措施，防止个人隐私信息被无权披露，在任何情况下，辽宁 CA 采取的保护措施应不低于合理的标准。

9.4.5. 使用隐私信息的告知与同意

在接受证书申请实体的申请并获得授权使用后，辽宁 CA 在办理证书业务时使用隐私信息。除此，辽宁 CA 在办理其它业务时需要使用隐私信息时，须征得证书持有者的同意。

9.4.6. 依法律或行政程序的信息披露

在政府事务或其他任何法律事务中，辽宁 CA 及关联机构依据司法程序必须协助配合调查的情况下，可以依据相关法律法规公开隐私信息。

9.4.7. 其他信息披露情形

除非获得隐私信息个人的授权，否则，辽宁 CA 无权在其它任何情况下披露此类信息。

9.5. 知识产权

辽宁 CA 所提供的电子认证系统、软件、证书策略（CPS）、业务规则、标识、技术方案等涉及的商标、著作权、专利权等知识产权，均受法律保护并归本机构所有。证书订户可在正常使用电子认证服务的范围内合理使用相关内容与技术，未经本机构书面许可，不得复制、篡改、反向工程、商业传播或擅自对外授权使用。订户自有电子签章、标识等知识产权归其本人所有。因知识产权侵权引发的一切纠纷，由过错方承担全部责任。

9.6. 陈述与担保

9.6.1. 辽宁 CA 电子认证服务机构的陈述与担保

在签发证书时，(a)不会因为辽宁 CA 的原因，使证书中出现对事实陈述的严重错误；(b)不会因为辽宁 CA 未能合理审慎而造成该证书信息上的错误；(c)该证书符合辽宁 CA 认证业务声明中的所有实质性要求；(d)辽宁 CA 于签发该证书时充分遵照了认证业务规则。

9.6.2. 用户的陈述与担保

接受电子认证服务的用户应：（a）在申请、接受或使用数字证书之前，必须先详细阅读并签署“数字证书服务协议”，并承诺提供真实信息，线上签署的协议与线下纸质协议具有同等法律效力；（b）藉由交付用户表单(与证书申请)，即表示您要求发证机构签发数字证书予您，亦表示您已同意本表单中的条款。辽宁 CA 的认证服务受辽宁 CA 电子认证业务规则所规范；（c）同意完全按照辽宁 CA 电子认证业务规则及本表单的条件使用本数字证书及相关的发证机构服务，否则，辽宁 CA 将按照认证业务规则中所述，不提供所有保证。

9.6.3. 依赖方的陈述与担保

依赖方应：（a）承认能够获得足够的信息以确保能信赖证书中的信息做出考虑充分的选择；(b)有责任自主决定是否信赖一张证书;(c)承认并同意，在使用辽宁 CA 资料库、或信赖任何证书时，都将完全遵照辽宁 CA 电子认证业务规则；(d)承认除了辽宁 CA 电子认证业务规则中的明确陈述之外，发证机关和辽宁 CA 否认所有其他的保证和责任.

9.6.4. 其他参与者的陈述与担保

与上述陈述与担保内容相同。

9.7. 担保免责

9.7.1. 担保责任的否定描述（明示无担保）

1)本 CA 机构仅按照《电子签名法》、相关监管规定及本 CPS 约定，提供电子证书签发、管理、状态查询、签名验签及相关举证服务，不构成任何形式的保证或担保。

2)CA 不担保：

(1) 证书绝对无误、绝对安全、绝对不被破解或伪造；

(2) 订户实际身份、资质、权限与其提交材料完全一致；

(3) 依赖方使用证书进行交易 / 签约必然合法、有效、无争议；

(4) 服务永不中断、无漏洞、完全无故障。

3)证书仅为身份与签名真实性的技术证明，不担保订户履约能力、信用状况及交易本身的法律有效性与商业风险。

9.7.2. 隐含担保责任的排除（法律默示担保免责）

1)在法律允许的最大范围内，CA 排除所有默示担保，包括但不限于：

(1) 适销性默示担保；

(2) 特定用途适用性默示担保；

(3) 无瑕疵、不间断、安全可靠的默示担保；

(4) 无侵权、完全合规的默示担保。

2)CA 不承担因以下情形产生的任何默示责任：

(1) 订户或依赖方误操作、泄露密钥、转借证书、越权使用；

(2) 依赖方未核实证书状态（CRL/OCSP）、未验证签名；

(3) 依赖方过度信赖证书而未做其他风控。

9.7.3. 担保免责条款的适用规定

9.7.3.1.9 适用场景

本免责适用于证书全生命周期：申请、审核、签发、使用、存储、吊销、更新、归档、验签、举证等全部环节，约束订户、依赖方及所有第三方。

9.7.3.2. 免责情形

在本机构严格遵守法律法规及本 CPS、且已履行合理审慎义务前提下，对以下损失不承担责任：

- 订户提供虚假、不全、失效材料导致的错误签发或损失；
- 订户密钥泄露、丢失、被盗用未及时告知本机构导致的损失；
- 依赖方未查询证书状态、未验签或验签后仍交易导致的损失；
- 不可抗力（战争、自然灾害、政府行为、网络攻击、电力 / 通信中断等）导致的服务中断、延迟或错误；
- 因第三方系统、网络、设备故障导致的损失；
- 订户或依赖方故意或重大过失导致的损失；
- 间接损失（利润损失、商誉损失、业务中断、数据丢失、预期收益损失等）。

9.7.3.3. 免责效力与可分割性

本条款独立有效，不因服务协议或 CPS 其他条款无效而失效。

如某一免责条款被认定无效或不可执行，其余免责条款继续有效并最大限度执行。

9.8. 偿付责任规则

9.8.1. 偿付责任范围

如辽宁 CA 违反《电子签名法》《商用密码管理条例》、本 CPS、服务协议规定的职责，且无法定/约定免责情形，依法承担直接经济偿付责任。本机构赔付覆盖因下列 CA 过错行为产生的损失：

人为操作错误类：受理人员虚假核验、审核漏项、违规签发证书、错误撤销 / 冻结证书、档案遗失、人工录入主体信息错误；

系统技术故障类：证书签发系统、OCSP/CRL 服务中断、程序缺陷、算法配置错误、证书参数配置失误、备份恢复失效；

安全漏洞与密钥风险类：防火墙/WAF 配置缺陷、网络入侵防护失效、根/RA 密钥泄露、私钥保管管控漏洞、审计日志缺失导致无法举证；

合规管理疏漏类：未按要求完成身份实人核验、未完整留存订户意愿记录、逾期上报重大安全事项、未履行档案归档义务；

服务管理过失类：客服错误指引、未及时处置证书安全预警、收到侵权投诉未采取管控措施。 因订户、依赖方自身操作失误、未履行合理风控义务产生的损失，不在赔付覆盖范围内。

9.8.2. 赔偿标准

辽宁 CA 赔偿上限统一为涉事证书当年实际缴纳服务费的 5 倍，分场景核算赔付金额：

身份审核/证书签发过错：按依赖方经有效证据佐证的直接财产损失核算，赔付总额不超过责任上限；

系统服务中断故障：按服务不可用时长折算对应周期服务费退还，叠加实际直接损失，合计不超过上限；

密钥泄露、系统安全漏洞类：以司法、第三方审计认定的直接损失为准，最高不超过单证 5 倍服务费；

档案、日志灭失无法举证：按订户维权产生的合理取证费用+直接损失合并计算；

任何情形下，间接损失（经营利润、商誉、预期收益、停工损失等）不予赔付；

赔付上限每年随订户缴费金额动态调整，调整后通过官网公告公示。辽宁 CA 仅在证书有效期限内承担对应赔付义务，证书过期后不再新增赔付责任。

9.8.3. 赔付监督机制

辽宁 CA 设立内部赔付监督机制（CA 自查+审计）。

1）赔付台账管理：建立《赔付事件台账》，记录：事件编号、时间、类型、损失、责任认定、赔付金额、整改措施、跟踪状态；永久留存。

2）审计强制覆盖

(1) 认证业务审计：抽样核查赔付相关业务（身份核验、证书撤销、日志）是否合规。

(2) 全面符合性评估：必查赔付机制合规性、准备金计提、台账完整性、整改闭环；年度报告必须含赔付专项章节，1 月底前报主管部门。

(3) 整改闭环：审计发现赔付相关问题→3 个工作日内通知责任部门→限期整改（≤15 天）→审计跟踪复查→纳入下年度审计重点。

9.9. 赔偿处理

9.9.1. 赔付申请流程及时限

申请主体：证书订、善意依赖方均可提交书面赔付申请；

申请材料：赔付申请书、涉事证书材料、损失佐证票据、事故经过说明、相关核验 / 沟通记录；

受理时限：客服渠道收到完整申请材料后 5 个工作日内出具受理回执；材料不全的一次性告知补正，补正周期不计入审核时限。

9.9.2. 内部事实审核流程及时限

责任部门（安全运营+营业部）联合核查事故成因、CA 过错占比、实际损失金额；

标准案件（损失≤2 倍服务费）10 个工作日内完成事实核查并出具审核意见书；

复杂案件（大额损失、涉及司法、密钥泄露重大事故）延长至 15 个工作日，

同步向安全策略委员会同步进展；

审核结果载明：是否属于赔付范围、损失核算金额、赔付依据、不予赔付的书面理由。

9.9.3. 赔付审批流程及时限

小额赔付（≤2 倍年费）：财务部+合规岗双签审批，审核完成后 3 个工作日内办结审批；

大额赔付（＞2 倍年费）：上报安全策略委员会审议，出具书面审批意见，审议周期不超过 5 个工作日；

审批驳回的，书面告知申请人驳回理由与补充举证方向。

9.9.4. 赔付支付流程及时限

审批通过后，财务部在 7 个工作日内完成赔付资金划转；赔付完成后同步更新赔付台账，归档全套申请、审核、审批、转账凭证，档案保存不少于证书失效后 5 年。

9.9.5. 异议复核机制

申请人对赔付结论存在异议，可在收到结果 10 个工作日内提交复核申请，公司重新组织审计、技术部门联合二次复核，复核 15 日内出具最终结论，最终结论为处置依据。

9.10. 有效期限与终止

9.10.1. 生效

辽宁 CA 的电子认证业务规则自发布之日起正式生效，文档中将详细注明版本号及发布日期。

本版 CPS 有效期：自文档发布当日起生效，有效期持续至新版合规 CPS 完成工信部、密码管理局备案并正式发布之日；在无新版本替代期间持续有效，不存

在固定年限到期失效机制

9.10.2. 终止

当新版本正式发布生效，旧版本将自动终止。

9.10.3. 效力的终止与保留

在有效期限结束后，仍将具有排它的法律效力，视为各参与方共同遵守的法律协议，享受国家相关法律法规的保护。

9.10.3.1. 文档部分终止条件

出现以下情形时，本 CPS 对应条款单独失效、其余条款继续有效：

国家法律、行政法规、T/CQAE 11034 等强制标准出台修订版本，与本 CPS 单条内容冲突的，冲突条款自动部分终止；

主管部门出具整改通知，明确要求废止、修改 CPS 某一节内容，整改完成前该条款临时终止适用；

证书策略 OID、根密钥规则、赔付标准等专项制度单独更新，仅对应章节条款终止，其余章节保持效力。

9.10.3.2. 针对特定参与者适用性终止条件

出现下列任一情形，本 CPS 对该主体终止约束效力：

订户主动申请注销全部证书、办理终止认证服务，证书全部撤销归档后，CPS 不再对该订户产生约束力；

依赖方长期不再使用我司证书进行签名验签业务，无任何交互行为的，相关权责条款不再约束该依赖方；

司法、行政机关判定相关主体无电子认证业务关联，可单独终止 CPS 对其适用效力。

9.11. 对参与者的个别通告与沟通

最新版本请访问辽宁 CA 网站（www.lnca.org.cn）以获得，对具体个人不做另行通知。

9.12. 修订

辽宁 CA 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。

9.12.1. 修订程序

辽宁 CA 的安全官、技术总监及用户服务负责人均有权向公司的安全策略委员会提出修改申请，安全策略委员会将会同相关人员在 24 小时内做出修改与否的决定，若决定修改，则责成相关人员对部分条款进行修正，并在得到安全策略委员会的认可后，上报辽宁 CA 批准予以公布并通知。

修订流程为：

1) 策略委员会提出修订意见，征询各方的建议，包括用户和依赖方；

2) 搜集各方意见并进行研究讨论；

3) 进行修改并公司决策层批准；

4) 再次进行审议和生效，并通过公司网站或其它方式发布。

9.12.2. 通知机制和期限

辽宁 CA 有权在辽宁 CA 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。证书持有者如不在修改结果后公布的限定时间内申请废止证书，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持有者的内容，按以下规则发送：

接受者是公司或其它单位组织则向其登记的联系地址或办公室发送信息；

接受者是个人则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。辽宁 CA 有权选择通过电子邮件或其他方式向证书持有者发送通知，邮件地址在证书持有者申请证书时已注明。

所有发送给辽宁 CA 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辽宁 CA，则这种通知只有在辽宁 CA 收到证书持有者的电子邮件通知后 24 小时内，收到证书持有者书面确认材料，方为有效。

9.12.3. 必须修改业务规则的情形

- 本规则无法保障辽宁 CA 的正常运营；
- 本规则无法确保证书接受方享受到标准的认证服务；
- 国家相应法律、法规及规章的修改影响本规则的继续实施;
- 其他必须修的情形。

9.13. 争议处理与举证

9.13.1. 争议处理

9.13.1.1. 适用范围与受理范围

1）适用主体

本机制适用于：辽宁 CA 机构、证书订户、依赖方、注册机构（RA）之间因电子认证服务、证书策略（CP）、认证业务规则（CPS）、服务协议产生的各类争议。

2）受理范围（必须受理）

- 证书申请、身份核验、签发、续期、更新、密钥变更、冻结、撤销、注销等业务争议；
- CP/CPS 条款解释、适用、修订引发的争议；
- 服务协议履行、违约、费用、服务质量争议；

- 身份冒用、证书被滥用、系统故障、安全事件导致的责任与赔偿争议；
- 订户 / 依赖方损失赔偿、责任认定、赔付执行争议；
- 个人信息保护、数据留存、日志查询与保密相关争议；
- 审计评估、合规检查、整改闭环引发的争议。

3）不予受理范围

- 与电子认证服务无关的个人恩怨、人身关系、劳动争议；
- 已进入诉讼 / 仲裁程序或已生效裁判 / 裁决的同一争议；
- 超出法定诉讼时效（3 年）且无正当理由的争议；
- 订户 / 依赖方故意提供虚假材料、恶意欺诈引发的争议（CA 无责）。

9.13.1.2. 争议处理流程与时限

- 受理回执：3 个工作日内；
- 友好协商：15 日内（必经）；
- 调解申请：协商不成后 7 日内；
- 调解期限：30 日内（可延 15 日）；
- 仲裁：按法定程序。

9.13.1.3. 仲裁

如果当事人之间无法很好的解决出现的问题和争端，应该提交仲裁机构（约定为“沈阳仲裁委员会”），根据仲裁条例在时效内裁决。仲裁的决定是终局性的，对每个当事人都有约束力。

9.13.2. 举证

9.13.2.1. 举证环节及资料

辽宁 CA 建立覆盖证书全生命周期标准化举证制度，固化全流程举证留存规范、取证流程、响应时效与能力保障体系，满足纠纷处置、监管核查、司法取证、审计核查各类举证需求，确保 CA 具备完整、合法、可溯源、可核验的举证能力。包

括但不限于以下环节：

1) 证书签发环节，身份验证记录、材料审查记录、告知记录、意愿确认记录等；

2) 签名环节，签名请求验证、签名操作日志、时间戳记录等；

3) 验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等；

9.13.2.2. 举证响应时效承诺

日常业务核查举证：收到举证需求后 2 个工作日内整理完整合规举证材料并出具正式举证说明。

内部审计、合规自查举证：1 个工作日内完成台账调取、资料归集。

监管部门核查取证：收到正式文书后 24 小时内先行报送核心资料，3 个工作日内提交全套完整举证卷宗。

民事纠纷、司法诉讼取证：依据司法文书要求，3 个工作日内出具符合司法采信标准的举证材料、电子存证报告、行为溯源证明。

紧急突发冒用、侵权事件举证：4 小时内出具核心事实举证材料，同步出具风险情况说明。

9.14. 管辖法律

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，辽宁 CA 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用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。

9.15. 与适用法律的符合性

电子认证服务的相关参与者需遵守在中华人民共和国境内适用的法律法规，包括但不限于《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《商用

密码管理条例》、《电子认证服务管理办法》、《电子认证服务密码管理办法》。

9.16. 一般条款

1) 本 CPS 是辽宁 CA 提供电子认证服务的唯一有效规则文件。

2) 订户、依赖方使用辽宁 CA 证书服务，即视为知晓并同意本 CPS 全部条款。

3) 本 CPS 任何条款被认定无效的，不影响其余条款的效力。

4) 辽宁 CA 对本 CPS 拥有最终解释权。

5) 本规则自公布之日起作为辽宁 CA 开展认证服务的规则生效。

9.17. 其他条款

辽宁 CA 认证服务规则中的标题、副标题和其他标题仅是方便读者和参考所用，并不是用于解释、说明或执行辽宁 CA 认证服务规则的规定。