辽宁 CA
电子认证业务规则

V2.1

辽宁数字证书认证管理有限公司

2005 年 12 月 12 日

辽宁 CA 电子认证业务规则

辽宁数字证书认证管理有限公司版权所有

版权声明

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：024-23871483，23871858　　传真：024-23871490

电子邮件：service@lnca.org.cn

邮政编码：110006

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

目　　录

1. 概括性描述

1.1 概述

辽宁数字证书认证管理有限公司（简称辽宁 CA）是经国家信息产业部、国家密码管理局批准，从事数字证书认证服务的专业机构，是辽宁省唯一的获得国家电子认证服务许可证的区域性认证中心(国家密码管理局电子认证服务使用密码许可证编号 0016，信息产业部电子认证服务许可证编号为 ECP21010205010)。

辽宁 CA 是可实现跨地区、跨行业统一认证和安全服务的电子认证服务机构。遵循 PKI 体系标准，可实现交叉认证。

辽宁 CA 主要从事数字证书的制作、颁发和管理工作，可为个人、企事业单位及其网站、软件代码等提供网上身份认证、数字签名、数据加密等一系列服务。

辽宁 CA 为从事互联网业务和交易的各方建立信任关系，通过数字证书实现交易双方身份的真实性、信息传输中的保密性、信息的完整性与操作的不可抵赖性来防范操作风险、增强网络安全。

辽宁 CA 是公平、公正、权威的网上第三方认证机构，所颁发的数字证书可以广泛应用于网上税务申报和税费征收; 网上社会保障申报和费用缴纳; 网上工商年检; 网上统计申报; 网上行政申报、审批; 网上招标、投标; 网上订购; 网上证券交易、安全电子邮件等领域。

辽宁 CA 电子认证业务规则（CPS，Certification Practice Statement)是辽宁 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、吊销、更新证书或密钥）所遵循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，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、证书吊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

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

1.2 文档名称与标识

1.2.1 名称

本文档名称为辽宁 CA 电子认证业务规则，是辽宁 CA 对所提供的认证及相关业务的全面描述。

1.2.2 标识

辽宁 CA 是辽宁数字证书认证管理有限公司（Liaoning Certificate Authority Co., Ltd.）的缩写形式。

1.3 电子认证活动参与者

1.3.1 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，由辽宁省密钥管理中心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 CRL SERVER（Certificate Revocation List Server），公布该证书可以公开的信息和状态。

1.3.2 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，负责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，管理和服务下层注册分支机构和下层受理点。每个注册机构可以按照行业或行政地域分成多个注册分支机构，或直接连接受理点，可以直接对终端用户提供服务。

在申请人申请证书时，注册机构有责任验证申请人提供信息的准确性、可靠性和完整性。

辽宁 CA 将根据客户群体的发展需要，遵循辽宁 CA 认证体系地域或行业的划分情况，授权建立相应的注册机构或受理点。注册机构和受理点有责任妥善保存客户的信息，不允许将客户信息透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。

地区、行业、机构均可以申请成为辽宁 CA 的注册机构。

注册机构必须获得辽宁 CA 的授权。

1.3.3 受理点

数字证书受理点也是辽宁 CA 数字认证体系的一个组成部分，其直接隶属于辽宁 CA 或隶属于辽宁 CA 下属的某个 RA。

受理点的业务范围包括：受理数字证书业务，包括证书申请、证书审核、证书注销、证书恢复、证书更新。

受理点应严格遵守辽宁 CA 制定的所有运行策略、操作管理规范和安全保障措施，严密保守客户及公司的商业秘密和技术秘密，承担因工作人员操作失误对用户造成直接经济损失所应承担的相应责任。

1.3.4 订户

订户是指辽宁 CA 签发的各种类型证书的持有者。

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。

1.3.5 依赖方

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。

1.3.6 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。

1.4 证书应用

1.4.1 适合的证书应用

辽宁 CA 数字证书目前已经在电子政务公共服务、电子交易、电子办公等领域应用，为建设互联网络信任环境提供了基础性的服务。具体请参阅 http://www.lnca.org.cn/。

目前辽宁 CA 所签发的数字证书类型主要有个人身份证书、单位

身份证书、个人代码签名证书、企业代码签名证书、设备证书、WAP证书、电子商务证书等。

个人身份证书，用于确认个人的网上身份。

单位身份证书，用于确认单位的网上身份。

个人代码签名证书，用于证明软件开发者对软件的所有权。

企业代码签名证书，用于证明软件开发企业对软件的所有权。

设备证书，用于表明设备等身份，主要用于网络中设备之间相互认证。

WAP证书，在无线通讯系统中确认设备使用者的身份。

电子商务证书，用于跨地域网上商务活动中身份确认。

证书申请实体可以根据实际需要，自主判断和决定采用相应类型的证书。

1.4.2 限制的证书应用

证书禁止在任何违反国家法律、法规或破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。

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。

1.5 策略管理

1.5.1 策略文档管理机构

辽宁CA电子认证业务规则由辽宁CA安全管理小组负责起草和管理。

1.5.2 联系方式

联系人：辽宁 CA 安全管理小组。

电话：024-23871483，23871858

电子邮件：service@lnca.org.cn

地址：沈阳市和平区和平南大街 28 号甲 3。

邮编：110006。

1.5.3 决定 CPS 符合策略的机构

辽宁 CA 电子认证业务规则由辽宁数字证书认证管理有限公司负责最后的审批和实施。

1.5.4 CPS 批准程序

辽宁 CA 电子认证业务规则做出任何变动之前，辽宁数字证书认证管理有限公司将对提供的变动建议进行研究，做出变更决定。在征询辽宁 CA 律师有关法律方面的意见后，形成决议。

1.6 定义和缩写

1.6.1 辽宁 CA

辽宁数字证书认证管理有限公司及辽宁省数字证书认证中心的简称。

1.6.2 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。

1.6.3 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。

1.6.4 RA（Registration Authority）

注册机构的英文简称。RA 是CA 认证体系的一个功能组件，负责对数字证书申请进行资格审核，并决定是否同意给该申请者发放数字证书，承担因审核错误而引起的一切后果(包括受理点引起的后果)。

1.6.5 受理点（Business Terminal）

受理点的英文简称。是CA 认证体系的一个功能组件，负责对数字证书申请进行资格审核，并决定是否同意给该申请者发放数字证书，它的直接上级为RA，并隶属于RA。

1.6.6 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。

1.6.7 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。

1.6.8 申请人

指向辽宁CA提出颁发证书申请的个人或单位用户。

1.6.9 订户

即为证书持有者。

1.6.10 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。

1.6.11 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。

1.6.12 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。

1.6.13 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。

1.6.14 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。

1.6.15 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。

1.6.16 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。

1.6.17 数字证书

数字证书又称为数字标识 (Digital Certificate ，Digital ID)。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。

1.6.18 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。

1.6.19 LDAP（Lightweight Directory Access Protocol）

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

1.6.20 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。

1.6.21 HTTP （Hypertext Transfer Protocol）

超文本传输协议。

1.6.22 HTTPS （Hypertext Transfer Protocol with SSL）

采用 SSL 的超文本传输协议。

1.6.23 PKCS （Public Key Cryptography）

公开密钥密码法。

1.6.24 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 认证信息的发布

辽宁 CA 在辽宁 CA 网站(www.lnca.org.cn)上发布认证的相关信息.证书在申请签发成功后，辽宁 CA 通过目录服务器自动将该证书发布到辽宁 CA 网站上。辽宁 CA 定期公布证书在有效期之内被废止的数字证书。用户可以在辽宁 CA 的网站中查询并获得有关信息。

2.2 发布的时间或频率

辽宁 CA 的 CRL 每四小时自动更新，也可通过人工发布最新 CRL。证书用户可在辽宁 CA 网站(www.lnca.org.cn)上查询、下载数字证书、CRL。

2.3 信息库访问控制

辽宁 CA 设置了信息访问及控制权限,保证只有经过授权的辽宁

CA 工作人员才能编写和修改辽宁 CA 公告的信息和发布的信息。

3.身份标识与鉴别

3.1 命名

3.1.1 名称类型

甄别名（Distinguished Name）包含于每张证书的主题中，唯一标识证书用户的身份。

辽宁CA证书符合X.509 V3标准，甄别名格式遵守X.500标准。

3.1.2 对名称意义化的要求

一个完整的名称应当全部或部分包含下面的信息:

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	辽宁CA
Organizational Unit（OU） =	“@”+企业机构代码证号	@01212345-2
Organizational Unit（OU） =	“!”+证书应用预留字段，具体定义在证书应用中完成	
Organizational Unit（OU） =	单位部门	软件部
State or Province （S） =	省	辽宁省
Locality （L） =	市	沈阳市
Common Name （CN） =	通用名: 域名或IP（设备证书）; 个人名称（个人证书、电子商务证书、代码签名证书）; 单位名称（单位证书、电子商务证书、代码签名证书）。	晓超

3.1.3 用户的匿名或伪名

辽宁 CA 不对任何匿名的个人或法人提供数字证书认证服务。

3.1.4 理解不同名称形式的规则

各类证书通用名命名方式不同，但是所有证书用户的通用名都需要严格审查。命名方式如下:

编号	证书类型	通用名
1	个人身份证书	个人姓名及身份证号码(与身份证上标明的一致)
2	单位身份证书	单位名称及组织机构代码证号（与营业执照等有效证件上标明的一致）
3	个人代码签名证书	个人姓名及身份证号码(与身份证上标明的一致)
4	单位代码签名证书	单位名称及组织机构代码证号（与营业执照等有效证件上标明的一致）
5	设备证书	域名或者IP地址
6	电子商务证书	个人证书为个人姓名及身份证号码（与身份证上标明的一致）；单位证书为单位名称及组织机构代码证号（与营业执照等有效证件上标明的一致）

3.1.5 名称的唯一性

辽宁 CA 签发的数字证书，利用个人的身份证号码或法人的组织机构代码证号码保障命名的唯一性。

用户申请证书时，证书系统会自动对其唯一性进行审核。如果不能通过唯一性审核，证书系统将拒绝签发证书。

3.1.6 商标的识别、鉴别和角色

辽宁 CA 仅对组织机构或个人进行身份鉴定并提供认证服务。辽宁 CA 不能够也不对商标或知识产权提供鉴定或认证服务，且不承担相关的任何责任。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

申请数字证书的个人或法人必须提供国家权威机构颁发的证明文件（机构代码证、工商营业执照、居民身份证、军官证、护照、学生证等有效证件）。

在辽宁 CA 的体系中，私钥保存在安全介质中发放给用户，用户可以通过专用工具对私钥进行使用（如数字签名）。合法的用户是其私钥的唯一持有者。因此，辽宁 CA 要求用户必须妥善保管自己的私钥。

3.2.2 组织机构身份的鉴别

本条对组织机构的身份鉴别适用于单位身份证书、单位代码签名证书、单位电子商务证书以及单位申请的设备证书。

单位申请者填写《数字证书申请表》（一式三份），经过单位授权代表的签署及单位盖章后，携带以下资料到辽宁CA授权的发证机构进行身份审核及办理交费手续 （以下证件的复印件和申请表需要单位盖章证明）：

a）申请单位的组织机构代码证的复印件;

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

营业执照

企业法人营业执照

事业单位登记证

事业单位法人登记证

税务登记证（国税）

税务登记证（地税）

组织机构代码证

社会团体登记证

社会团体法人登记证

人民团体登记证

人民团体法人登记证

政府批文

其他有效证件

c）经办人身份证原件与复印件。

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

3.2.3 个人身份的鉴别

本条对个人身份的鉴别，适用于个人身份证书、个人代码签名证书、个人电子商务证书以及个人申请的设备证书。

辽宁CA的个人证书签发给合法的个人申请者，辽宁CA需要审核个人申请者的身份。

个人申请者填写《数字证书申请表》（一式三份），个人签字后，

携带个人身份证（或军官证、护照等）原件与复印件到辽宁CA授权的发证机构进行身份审核及办理交费手续。

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

3.2.4 没有验证的用户信息

辽宁 CA 不对没有经过验证的用户发放数字证书。

3.2.5 授权确认

用户一旦提交《数字证书申请表》便表明用户正式授权辽宁CA为其提供数字认证服务，并遵守辽宁CA《数字证书申请责任书》的规定。

授权有效并持续到数字证书过期或用户申请撤销数字证书时。

3.2.6 互操作准则

辽宁CA认证机构的管理员、操作员必须是辽宁CA认证机构的正式职员。

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。

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。

3.3 密钥更新请求的标识与鉴别

3.3.1 更新申请情况

当出现以下情况时证书用户可以到辽宁CA授权的发证机构申请更新证书。

证书到期;

证书补发;

证书DN或EMAIL更改;

密钥更新。

3.3.2 更新操作

证书用户申请更新证书时,填写《数字证书申请表》(一式三份),按照初始身份验证步骤提交相关资料(同§3.2)并由辽宁CA授权的发证机构审核。

3.3.3 更新申请的确认

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

3.3.4 废止后密钥更新的标识与鉴别

证书吊销后的密钥更新操作流程等同于用户重新申请辽宁CA的证书服务。

证书挂起后,必须先进行证书恢复操作,然后才能进行密钥更新。

3.4 废止请求的标识与鉴别

3.4.1 证书废止情况

证书废止包括证书吊销、证书挂起。

出现下列情况证书将被废止:

密钥泄漏;

证书有效期内用户终止使用证书;

其它影响数字证书安全的情况。

3.4.2 废止操作

证书用户申请废止证书时,填写《数字证书申请表》(一式三份),按照初始身份验证步骤提交相关资料(同§3.2),并由辽宁CA授权的发证机构审核。

3.4.3 废止申请的确认

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

3.5 恢复请求确认

3.5.1 恢复情况

只能恢复被挂起的证书。

3.5.2 恢复操作

证书用户申请恢复证书时,填写《数字证书申请表》(一式三份),

按照初始身份验证步骤提交相关资料（同§3.2），并由辽宁CA授权的发证机构审核。

3.5.3 恢复申请的确认

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

4.证书生命周期操作要求

辽宁 CA 授权的发证机构提供数字证书授权、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命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 证书申请

证书申请实体根据辽宁 CA 的要求提供所需证明材料并填写《数字证书申请表》的过程。

4.1.1 证书申请实体

证书申请实体包含个人、企业单位、事业单位、社会团体、人民团体等各类组织机构以及 CA、RA、受理点和 CA 机构或 RA 机构的系统及相应的管理员。

4.1.2 注册过程与责任

证书申请实体提供所需材料，根据材料填写《数字证书申请表》到所在地区注册中心进行注册。

证书申请者一经接受证书，证书申请者就应承担如下责任：既始终保持对其私钥的控制，使用可信的系统和采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。

申请者的赔偿。

一经接受证书，证书申请实体即同意辽宁 CA、辽宁 CA 授权的发证机构对于由下列原因直接或间接造成的任何责任和损失不承担法律责任：

- 证书申请者（或其授权的代理人）虚假地或错误地陈述了事实；
- 证书申请者未能披露重要事实，而证书申请实体的这种有意或无意的错误陈述或失职造成了对发证机构、辽宁 CA、任何信任其证书的人的欺骗；
- 证书申请实体没有使用可信系统或没有采用必要的合理措施防止其私钥被损害、丢失、泄露、被篡改或被未经授权使用。

证书申请实体对辽宁 CA 和辽宁 CA 授权的发证机构造成的责任和损失包括：由于上述原因直接或间接造成的责任、损失、任何诉讼、仲裁及一切相关费用，包括但不限于诉讼费用、仲裁费用以及律师费等。对于此处的责任和损失，证书申请实体将予以经济赔偿。

当证书是应证书申请者代理人的要求签发时，代理人和证书申请

者应向辽宁 CA 和辽宁 CA 授权的发证机构，依照本节规定进行连带赔偿。证书申请者有责任就代理人的疏忽和错误陈述通知证书签发者。

4.2 证书申请处理

在证书申请处理过程中，注册机构鉴别证书申请实体身份，对《数字证书申请表》进行审核。

4.2.1 执行识别与鉴别功能

电子认证服务机构根据数字证书申请实体所提供的资料对其进行身份识别，具体鉴别《数字证书申请表》填写的正确性。

4.2.2 证书申请批准和拒绝

1） 鉴别申请实体提供材料的正确性;

2） 鉴别申请实体身份;

3） 鉴别申请实体所填写《数字证书申请表》的正确性。

根据以上的步骤在电子认证服务机构确定申请表正确给予批准，如果有误则返还给用户。

4.2.3 处理证书申请的时间

电子认证服务机构或注册机构处理证书申请在其规定的时间（三个工作日）内完成。

4.3 证书签发

证书申请处理后，电子认证服务机构或注册机构制作证书及通知

用户的过程。

4.3.1 证书签发中注册机构和电子认证服务机构的行为

辽宁 CA 处理证书申请后，由录入员根据用户所填写的《数字证书申请表》进行信息录入，然后由审核员对所录入的信息进行审核，注册机构审核通过后再由上级认证中心进行审核，上级认证中心审核通过后将制证相关信息发送给制证员进行制证，如果审核没有通过则返回给录入员进行更改，更改后再由审核员进行审核。

4.3.2 电子认证服务机构和注册机构对用户的通告

辽宁 CA 服务机构和注册机构颁发新证书时对用户的通告有两种方式:

1） 电话通知

2） 网上在线查询

4.4 证书接受

辽宁 CA 将已签发的数字证书发放给用户的过程。

4.4.1 构成接受证书的行为

用户得到通知后，携带《数字证书申请表》到办理证书的注册机构领取证书，领取证书前要在证书领取表单上签上用户姓名。

4.4.2 电子认证服务机构对证书的发布

证书在签发成功后，辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站上。辽宁 CA 定期公布在证书有效期内被废止的数

字证书。证书用户都可以在辽宁 CA 的网站中通过查询获得有关信息。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户私钥是由自己保存，并且在存储介质中不可导出。订户用私钥进行签名和解密。

4.5.2 信赖方公钥和证书的使用

信赖方公钥是发布出去的，用户可用信赖方公钥对发送给对方的信息进行加密，同时可用信赖方公钥对可信赖方签名信息进行验证。

4.6 证书更新

为保证证书及其密钥对的安全有效，辽宁 CA 为签发的证书设置有效期，一般为一年。这也是为了保证证书用户的权利。订户必须在证书有效期到期前，到辽宁 CA 授权的发证机构申请更新证书。更新证书时发证机构根据订户的要求决定新证书是否更新证书密钥。出于安全考虑建议证书订户更新证书时更新密钥。

4.6.1 证书更新的情形

证书到期;

证书补发;

证书DN或EMAIL更改;

密钥更新。

4.6.2 请求证书更新的实体

由辽宁 CA 颁发的证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是辽宁 CA 各类证书的有效期限未到的证书持有者。

4.6.3 证书更新请求的处理

申请者到辽宁 CA 授权的发证机构填写《数字证书申请表》，并注明更新的原因。如果申请人是终端用户，则由终端用户填写该表单；

辽宁 CA 授权的发证机构对申请者资料及申请表单进行识别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。

4.6.4 颁发更新证书时对用户的通告

辽宁 CA 服务机构和注册机构颁发更新证书时对用户的通告有两种方式：

１） 电话通知

２） 网上在线查询

4.6.5 构成接受更新证书的行为

用户得到通知后，携带《数字证书申请表》到办理证书的注册机构领取证书，领取证书时要在证书领取表单上签上用户姓名。

4.6.6 电子认证服务机构对更新证书的发布

证书在更新成功后，辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站上。

4.6.7 电子认证服务机构对其他实体的通告

证书在更新成功后，辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站上。辽宁 CA 用户可以在辽宁 CA 的网站（www.lnca.org.cn）中查询获得相关信息。

4.7 证书密钥更新

由于技术的不断更新，为了加密的安全性与灵活性，辽宁 CA 有权定期更换证书用户的密钥。

4.7.1 证书密钥更新的情形

证书的密钥泄露。对此，证书持有者负有立即告知辽宁 CA 的义务;

证书到期，证书更新。

4.7.2 请求证书密钥更新的实体

由辽宁 CA 颁发的证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是持有辽宁 CA 各类证书而有效期限未到的证书持有者。

4.7.3 证书密钥更新请求的处理

申请者到辽宁 CA 授权的发证机构填写《数字证书申请表》，并注明更新的原因。如果申请人是终端用户，则由终端用户填写表单。

辽宁 CA 授权的发证机构对申请者资料及申请表单进行识别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。

4.7.4 颁发更新证书时对用户的通告

辽宁 CA 服务机构和注册机构颁发更新证书时对用户的通告有两种方式:

1） 电话通知

2） 网上在线查询

4.7.5 构成接受密钥更新证书的行为

用户得到通知后，携带《数字证书申请表》到办理证书的注册机构领取证书，领取证书前要在证书领取表单上签上用户姓名。

4.7.6 电子认证服务机构对密钥更新证书的发布

证书在更新成功后，辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站上。

4.7.7 电子认证服务机构对其他实体的通告

证书在更新成功后，辽宁 CA 通过目录服务器自动将该证书发布到辽宁 CA 网站上。辽宁 CA 用户可以在辽宁 CA 的网站（www.lnca.org.cn）中查询获得有关信息。

4.8 证书变更

数字证书是用户的电子身份证，数字证书内的信息应与用户本身的信息保持一致。

4.8.1 证书变更的情形

证书持有者的信息发生变更。

4.8.2 请求证书变更的实体

由辽宁 CA 颁发的证书有效期限未到的个人、单位、服务器、企业、组织、 网站等提供网上服务和享受网上服务的各种实体，以及其他凡是持有辽宁 CA 各类证书而有效期限未到的证书持有者。

4.8.3 证书变更请求的处理

申请者到辽宁 CA 授权的发证机构书面填写《数字证书申请表》，并注明更新的原因。如果申请人是终端用户，则由终端用户填写表单。

辽宁 CA 授权的发证机构对申请者资料及申请表单进行识别与鉴定，然后对用户提交的证书更新申请进行审核，最后进行更新制证。

4.8.4 颁发新证书时对用户的通告

辽宁 CA 服务机构和注册机构颁发更新证书时对用户的通告有两种方式:

1） 电话通知

2） 网上在线查询

4.8.5 构成接受变更证书的行为

用户得到通知后，携带《数字证书申请表》到办理证书的注册机构领取证书，领取证书前要在证书领取表单上签上领取人姓名。

4.8.6 电子认证服务机构对变更证书的发布

证书在更新成功后，辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站（www.lnca.org.cn）上。

4.8.7 电子认证服务机构对其他实体的通告

证书在更新成功后，辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站上。辽宁 CA 用户可以在辽宁 CA 的网站（www.lnca.org.cn）中查询获得有关信息。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

新的密钥对替代旧的密钥对;

密钥失密：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;

操作中止：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）;

证书的更新费用未收到;

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;

用户申请初始注册时，提供不真实材料;

证书已被盗用、冒用、伪造或者篡改;

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

其他情况。

这些情况可以是因法律或政策的要求辽宁 CA 采取的临时注销措施，也可以是用户申请注销证书时填写的其他原因。

4.9.2 请求证书吊销的实体

由辽宁 CA 颁发的证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是持有辽宁 CA 各类证书而有效期限未到的证书持有者。

4.9.3 吊销请求的流程

申请者到辽宁 CA 授权的发证机构填写《数字证书申请表》，并注明吊销的原因。辽宁 CA 授权的发证机构识别吊销用户身份的真实性，对用户提交的证书吊销申请进行审核。

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

4.9.4 吊销请求宽限期

辽宁 CA 证书的使用者在出现以上证书吊销的情形之一的情况下，应在一周内向辽宁 CA 或辽宁 CA 授权的发证机构提出吊销申请。

4.9.5 电子认证服务机构处理吊销请求的时限

辽宁 CA 规定在一个工作日内处理完吊销请求。

4.9.6 依赖方检查证书吊销的要求

证书在吊销成功后，辽宁 CA 通过 CRL 发布证书吊销信息。辽宁 CA 用户可以在辽宁 CA 的网站（www.lnca.org.cn）中查询获得有关信息。

4.9.7 CRL 发布频率

辽宁 CA 通常在 4 小时内自动发布最新 CRL，也可人工发布最新 CRL。证书用户可在辽宁 CA 网页 http://www.lnca.org.cn/上查询、下载 CRL。

4.9.8 CRL 发布的最大滞后时间

辽宁 CA CRL 更新到对外发布最大滞后时间为 1 小时。

4.9.9 在线状态查询的可用性

辽宁 CA 通过目录服务器自动将该证书复本发布到辽宁 CA 网站上。辽宁 CA 用户可以在辽宁 CA 的网站（www.lnca.org.cn）中查询获得有关信息。

4.9.10 在线状态查询要求

辽宁 CA 用户可以在辽宁 CA 的网站（www.lnca.org.cn）中，根据用户本身的特性进行查询，来获得用户的详细信息。

4.9.11 吊销信息的其它发布形式

辽宁 CA 根据吊销证书的特殊性，建立了证书吊销列表对已经吊销的证书进行发布。

4.9.12 密钥损害的特别要求

数字证书密钥一旦损坏，证书只能被吊销而不能做挂起操作。

4.9.13 证书挂起的情形

证书用户暂停使用证书。

其他，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，可以申请证书挂起。

4.9.14 请求证书挂起的实体

由辽宁 CA 颁发的证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是持有辽宁 CA 各类证书而有效期限未到的证书持有者。

4.9.15 挂起请求的流程

申请者到辽宁 CA 授权的发证机构书面填写《数字证书申请表》，并注明挂起的原因。辽宁 CA 授权的发证机构识别挂起用户身份的真实性，对用户提交的证书挂起申请进行审核。

证书挂起审核后，由审核员进行对证书挂起的操作。

4.9.16 挂起的期限限制

证书挂起的期限不能超过证书的有效期。

4.10 证书状态服务

证书用户可以通过在辽宁 CA 网站（ www.lnca.org.cn ）上对证书进行查询以获得证书状态。

辽宁 CA 提供 CRL 下载服务，其下载地址为：

HTTP://www.ln-ca.com/crl.crl。

辽宁 CA 同时提供 OCSP 服务，为高级证书用户提供证书状态查询。

4.10.1 操作特征

用户可根据所要查找用户的相关信息进行查询，查询后可获得用户数字证书的状态。

4.10.2 服务可用性

证书状态是通过 LDAP 发布服务器进行发布的，其可信度及安全性由根证书的签名来保证。

CRL 用户需要将 CRL 下载到本地后进行验证，包括 CRL 的合法性验证。辽宁 CA 每 4 小时进行 CRL 的更新。必要时，辽宁 CA 也可以采用手动方式对 CRL 进行立刻更新。

OCSP 服务器实现每周 7 天，每天 24 小时在线服务。

4.10.3 可选特征

可选特征包括：用户名、用户的电子邮件、地址等。

4.11 订购结束

4.11.1 证书废止情况

密钥泄漏;

证书有效期内用户终止使用证书;

其它（如：证书注销、证书挂起）。

4.11.2 废止操作

证书用户申请废止证书时，填写《数字证书申请表》（一式三份），按照初始身份验证步骤提交相关资料并由辽宁 CA 授权的发证机构

审核。

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

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。

加密密钥对是由中华人民共和国国家密码管理局许可的、辽宁 CA 数字证书签发系统支持的加密机设备生成的，由辽宁省国家密码管理局所属的 KMC 控制管理。

签名密钥对由客户端生成，证书申请实体可使用辽宁省国家密码管理局认可的、辽宁 CA 数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证辽宁 CA 无法复制签名密钥对。

KMC 备份托管的加密私钥，确保加密私钥的安全。

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

辽宁 CA 主机房位于沈阳市区，分为五层安全区域，是监控和管

理机房（辽宁 CA Network Operation Center，简称 NOC）的物理通道。辽宁 CA 还在沈阳市区的另一地点建立了备份中心。

5.1.2 物理访问

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，以确保物理通道的安全。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 CA NOC 时，必须经过身份识别。NOC 实行全天 24 小时自动监控。

5.1.3 电力与空调

辽宁 CA 系统采用双电源供电，在单路电源中断时，可以维持系统正常运转。同时，使用一个不间断电源（UPS），避免电源波动。

辽宁 CA 中心机房采用专用机房空调设施，保持机房在恒温、恒湿的状态下运行。

5.1.4 水患防治

辽宁 CA 在机房建设时已采取相应措施，防止水侵蚀，充分保障系统安全运行。

5.1.5 火灾防护

辽宁 CA 通过与专业防火部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，充分保障系统安全运行。

5.1.6 介质存储

存储介质必须得到安全可靠的存放，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。具体的要求在辽宁 CA 的技术标准和规程中做出了明确规定。

5.1.7 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。所有处理行为将记录在案，以供审查的需要，销毁行为遵守我国的法律。

5.1.8 异地备份

辽宁 CA 在沈阳数据中心建立了备份中心，提供异地数据及系统备份。异地备份介质安全要求应符合辽宁 CA 备份标准和程序。

5.2 程序控制

5.2.1 可信角色

辽宁 CA 明确执行 CA 系统的关键职能职位，他们包括:

辽宁 CA 超级管理员享有以下权限:

1）负责输入启动各个服务（CA、RA-SERVER）的超级管理员口令;

2）监督系统管理员维护各个模块的服务;

3）签发系统管理员;

4）如果系统管理员忘记口令，可重新签发一个系统管理员;

5）授权数据库管理员备份数据、重新加密以及在必要的时候对

辽宁 CA/Authority 的数据库进行恢复。

辽宁 CA 系统管理员享有以下权限:

1）建立和变更辽宁 CA 安全策略;

2）增加和减免其他管理员，及辽宁 CA 用户;

3）管理交叉认证，发布辽宁 CA 交叉认证协议，更新及注销交叉认证; 处理审计日志;

4）享有辽宁 CA 所有管理员的特权;

5）管理 CRL、证书模板的制定。

CA 录入员（SOO: System Operation Operator）:

1）负责用户证书申请信息的录入，并将其提交给审核员;

2）协助客户办理数字证书申请、作废、更新等手续。

CA 审核员（RAO: Registry Approval Operator）:

1）负责数字证书的审批受理;

2）如实向上级机构传送证书申请实体的信息;

3）协助客户办理数字证书申请、作废、更新等手续。

CA 审计员（auditor）:

1）负责 CA、RA 数字证书的统计、审计;

2）负责 CA、RA 日志的备份、恢复。

CA 证书制作员（Cert Maker）:

1）证书的制作、发放;

2）协助客户办理数字证书申请、作废、更新等手续。

其他管理员包含:

网络管理员

数据库管理员

加密机管理员

目录服务管理员

证书发布系统管理员安排上述职位是为了确保责任明确，建立有效的安全机制，保证内部管理和操作的安全。

5.2.2 每项任务需要的人数

辽宁 CA 确保单个人不能接触、导出、恢复、更新、废止辽宁 CA 的 CA 系统存储的根证书对应的私钥。

至少两个人才能使用一项对参加操作人员保密的密钥分割和合成技术来进行任何钥匙恢复的操作。

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。

5.2.4 需要职责分割的角色

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。对于使用安全令牌的员工，辽宁 CA 系统将独立完整地记录其所有的操作行为。

所有辽宁 CA 职位人员必须确保:

发放的安全令牌只直接属于个人或组织所有;

发放的安全令牌不允许共享。

辽宁 CA 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。

5.3 人员控制

5.3.1 资格、经历和无过失要求

辽宁 CA 的员工录用必须符合辽宁 CA 录用员工资格规定，与有关的政府部门和调查机构合作，完成对辽宁 CA 可信任员工的背景、经历情况调查。

5.3.2 背景审查程序

辽宁 CA 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。一般员工需要有 3 个月的考察期，关键部位的员工考察期为半年，核心部位的员工考察期为壹年。根据考察的结果安排相应的工作或者辞退；辽宁 CA 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。

辽宁 CA 会对其关键的 CA 职员进行严格的背景调查。受理点操作员的审查可以参照辽宁 CA 对可信任员工的考察方式。受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背辽宁 CA 证书受理的规程和辽宁 CA 电子认证业务规则。

辽宁 CA 确立流程管理规则，据此 CA 员工受到合同和章程的约束，不许泄露辽宁 CA 证书服务体系的敏感信息。所有员工与辽宁 CA 签定保密协议，合同期满以后 1 年内仍然不得从事与辽宁 CA 相类似的工作，报第三方公证。

5.3.3 培训要求

辽宁 CA 对辽宁 CA 员工进行以下内容的综合性培训:

辽宁 CA 电子认证服务规则;

辽宁 CA 安全原则和机制;

辽宁 CA 使用的软件介绍;

辽宁 CA 操作的系统和网络;

辽宁 CA 质量控制体系;

岗位职责;

辽宁 CA 政策、标准和程序;

相关法律、仲裁规则、管理办法等。

5.3.4 再培训周期和要求

根据辽宁 CA 策略调整、系统更新等情况，辽宁 CA 将对员工进行继续培训，以适应新的变化。

5.3.5 工作岗位轮换周期和顺序

按辽宁 CA 工作岗位轮换的有关规定进行部门内部的岗位轮换。

5.3.6 未授权行为的处罚

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

一旦发现上述情况，辽宁 CA 立即终止该人员的安全令牌。

5.4 审计日志程序

5.4.1 记录事件的类型

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 记录其它与 CA 系统本身不相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理日志的周期

辽宁 CA 每两周对记录进行审查，对审查记录行为备案。

5.4.3 审计日志的保存期限

辽宁 CA 在数据库保存审计记录至少两个月,离线存档至少七年。

5.4.4 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。

5.4.5 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。

5.4.6 审计收集系统

辽宁 CA 审计收集系统涉及:

证书管理系统; 证书签发系统; 证书目录系统; 远程通信系统;

证书审批受理系统;

应急反应系统; 访问控制系统(包括防火墙);

专网办公系统;

客户服务系统;

网站、数据库安全保障系统;

其他辽宁 CA 认为有必要审查的系统。

辽宁 CA 全天候准备上述系统的检查管理和审查工具。在需要的时候, 辽宁 CA 会随时应用这些工具来满足各项审查的要求。

5.5 记录归档

5.5.1 归档记录的类型

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)。

5.5.2 归档记录的保存期限

辽宁 CA 中的存档期限一般规定为七年。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证, 也有密码技术的保证。只有

经过授权的工作人员按照特定的安全方式才能接近它们。辽宁 CA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力的破坏。

5.5.4 归档文件的备份程序

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。

5.5.5 记录时间戳要求

所有 5.5.1 条款所述的存档内容都要加时间标识。

5.5.6 归档收集系统

辽宁 CA 中的档案收集系统由人工操作和自动操作两部分组成。

5.5.7 获得和检验归档信息的程序

辽宁 CA 每年会验证存档信息的完整性。

5.6 电子认证服务机构密钥更替

这里密钥更替是指当辽宁 CA 根证书到期而需要更换根密钥对时所采取的措施。辽宁 CA 根密钥对由加密机产生。证书到期更换密钥时将签发 3 张证书。

使用旧的私钥对新的公钥及信息签名生成证书;

使用新的私钥对旧的公钥及信息签名生成证书;

使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更替的目的，使新旧证书之间互相认证、信任。

5.7 损害与灾难恢复

5.7.1 计算资源、软件和/或数据的损坏

辽宁 CA 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，辽宁 CA 将按照灾难恢复计划实施恢复。具体由辽宁 CA 灾难恢复计划决定。

5.7.2 实体私钥损害处理程序

当辽宁的根私钥作废时，辽宁 CA 应根据辽宁 CA 灾难恢复计划规定的灾难恢复步骤进行操作。

5.7.3 灾难后的业务连续性能力

自然灾难或其他灾难后采取的安全措施，按照辽宁 CA 灾难恢复计划实施。

5.8 电子认证服务机构或注册机构的终止

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 授权的发证机构、垫付商和证书持有者书面通知，并在终止服务六十日前向国务院信息产业主管部门报告,按照相关法律规定的步骤进行操作。

6.认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键,所以在电子认证业务规则中制定了相应的规则，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。

6.1.1 密钥对的生成

加密密钥对:

加密密钥对是由中华人民共和国国家密码管理局许可的、辽宁 CA 数字证书签发系统支持的加密机设备生成的，由辽宁省国家密码管理局所属的 KMC 控制管理。

签名密钥对:

签名密钥对由客户端生成,证书申请者可使用辽宁省国家密码管理局认可的、辽宁 CA 数字证书签发系统支持的介质生成签名密钥对。签名密钥在存储介质中不可导出,保证辽宁 CA 无法复制签名密钥对。

辽宁 CA 支持多种介质，如智能密码钥匙。辽宁 CA 可根据实际情况选择签名密钥对的生成介质。

服务器证书的密钥对由服务器自身生成，用户应妥善保管。

辽宁 CA 在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 私钥传送给用户

证书用户的加密私钥是在 KMC 生成的，该私钥只保存在 KMC。在加密私钥从 KMC 到用户的传递过程中采用国家密码管理局许可的

对称密钥算法加密。辽宁 CA 无法获得，保证了证书用户密钥的安全。

6.1.3 公钥传送给证书签发机构

辽宁 CA 从 KMC 取得用户公钥后为其签发证书，在此过程中也采用国家密码管理局许可的对称密钥算法加密，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

辽宁 CA 的根公钥包含在辽宁 CA 自签的根证书中。证书用户可以从辽宁 CA 的网站上下载辽宁 CA 根证书。

6.1.5 密钥的长度

辽宁 CA 所使用的密钥对长度支持 1024 位。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、辽宁 CA 数字证书签发系统支持的硬件生成，同时进行质量检查。

6.1.7 密钥使用目的

在辽宁 CA 证书服务体系中的密钥用途和证书类型紧密相关。

辽宁 CA 的签名密钥用于签发 RA 证书和证书废止列表（CRL）。

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

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。

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

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

6.2.2 私钥多人控制（m 选 n）

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。

6.2.3 私钥托管

KMC 可以根据客户和法律的需要，对加密密钥进行托管。签名私钥从不进行托管，以保证其不可否认性。

6.2.4 私钥备份

证书的持有者可以备份他们的私钥，以确保这些私钥的安全。

6.2.5 私钥归档

KMC 提供过期的托管私钥的存档服务。

6.2.6 私钥导入、导出密码模块

在辽宁 CA 证书服务体系中，使用辽宁 CA 的软件可以把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。必须通过密码验证之

后，才可能使用存储在密码模块中的私钥进行加解密操作。

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。

辽宁 CA 的签名私钥保存在硬件密码模块中。

6.2.8 激活私钥的方法

在辽宁 CA 证书服务体系中，必须通过密码验证后，方可激活私钥。

6.2.9 解除私钥激活状态的方法

在辽宁 CA 证书服务体系中，通过终止程序来停止私钥的使用。

6.2.10 销毁私钥的方法

凡用户需要销毁私钥，应通知辽宁 CA，由 KMC 进行销毁。

6.2.11 密码模块的评估

辽宁 CA 使用国家密码管理局许可的密码模块，密码模块的标准应符合国家规定的要求。所有密码模块的使用应在辽宁省 KMC 进行登记备案。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

公钥属于安全数据，由辽宁省 KMC 定期存档、管理。

6.3.2 证书操作期和密钥对使用期限

辽宁 CA 根证书有效期为 10 年。用户证书由于考虑到安全性，目前提供的证书有效期一般为一年，但系统支持在根证书有效期内的任意期限，最短可定制到一天。

6.4 激活数据

6.4.1 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。

6.4.2 激活数据的保护

辽宁 CA 采取加解密机制等多种方式保护激活数据，以避免未授权的使用。未授权用户尝试使用激活数据时，尝试达到预定的次数，激活数据会自动锁定。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

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。

6.5.2 计算机安全评估

辽宁 CA 使用的密码设备是通过国家密码管理局批准生产的密

码设备。

6.6 生命周期技术控制

6.6.1 系统开发控制

辽宁 CA 的软件设计和开发过程遵循以下原则:

- 第三方的验证和审核
- 安全风险和可靠性设计

6.6.2 安全管理控制

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

6.7 网络的安全控制

辽宁 CA 有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。 只有经过授权的辽宁 CA 员工才能够进入辽宁 CA 签发系统、辽宁 CA 注册系统、辽宁 CA 目录服务器、辽宁 CA 证书发布系统等设备或系统。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 时间戳

数字时间戳（DTS: Digital Time Stamp）是对时间信息的电子签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

7.证书、证书吊销列表和在线证书状态协议

7.1 证书

辽宁 CA 签发的证书符合 X.509 V3 证书格式,遵循 RFC3280 标准。

7.1.1 版本号

X.509: V3

7.1.2 证书扩展项

颁发机构密钥标识符:

颁发机构密钥标识符与验证签名的公开密钥相联系。辽宁 CA 根证书公钥与此标识符相联系。

主题密钥标识符:

通过主体密钥标识符识别相对应证书的公钥

密钥用法:

密钥加密,数据加密,电子签名,验证证书签名,验证 CRL 签名,只加密,只解密。

基本限制:

用于鉴别证书持有实体身份,如终端用户等。

CRL 分发点:

由辽宁 CA 定义的 CRL 发布点。如:

[1]CRL Distribution Point

Distribution Point Name:

Full Name:

Directory Address:

CN=crl113_0

CN=LNCA

OU=lnca

O=Liaoning Digital Certificate Authority Management Co.Ltd

L=Shenyang

S=Liaoning

C=CN

[2]CRL Distribution Point

Distribution Point Name:

Full Name:

URL=ldap://ldap.ln-ca.com:391/CN=crl113_0,CN=LNCA,OU=lnca,O=Liaoning Digital Certificate Authority Management Co.Ltd,L=Shenyang,ST=Liaoning,C=CN?certificateRevocationList?base?objectclass=cRLDistributionPoint

[3]CRL Distribution Point

Distribution Point Name:

Full Name:

URL=http://www.ln-ca.com/crl.crl

7.1.3 名称形式

采用 X.500 甄别名格式。

一个完整的名称应当符合下面的格式，如:

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	辽宁CA
Organizational Unit（OU） =	“C” +企业机构代码证号	C11054385-2
Organizational Unit（OU） =	“B” +证书应用预留字段，具体定义在证书应用中完成	
Organizational Unit（OU） =	“A” +单位部门	A软件部
State or Province （S） =	省	辽宁省
Locality （L） =	市	沈阳市
Common Name （CN） =	通用名: 域名或IP（设备证书）; 个人名称（个人证书、电子商务证书、代码签名证书）; 单位名称（单位证书、电子商务证书、代码签名证书）。	晓超

7.1.4 名称限制

辽宁 CA 签发的数字证书，利用个人的身份证号码或法人的组织机构代码证号码保障命名的唯一性。

各类证书通用名命名方式不同，但是所有证书用户的通用名都需要严格审查。命名方式如下:

编号	证书类型	通用名
1	个人身份证书	个人姓名及身份证号码（与身份证上标明的一致）
2	单位身份证书	单位名称及组织机构代码证号码（与营业执照等有效证件上标明的一致）
3	个人代码签名证书	个人姓名及身份证号码（与身份证上标明的一致）
4	单位代码签名证书	单位名称及组织机构代码证号码（与营业执照等有效证件上标明的一致）
5	设备证书	域名或者IP地址
6	电子商务证书	个人证书为个人姓名及身份证号码（与身份证上标明的一致）；单位证书为单位名称及组织机构代码证号（与营业执照等有效证件上标明的一致）

7.2 证书吊销列表

辽宁 CA 定期签发 CRL（证书吊销列表），其所签发的 CRL 遵循 RFC3280 标准，采用 X.509 V2 格式。

7.2.1 版本号

X.509: V2。

7.2.2 CRL 和 CRL 条目扩展项

版本: X.509: V2。

颁发者:

CN = LNCA

OU = lnca

O = Liaoning Digital Certificate Authority Management Co.Ltd

L = Shenyang

S = Liaoning

C = CN

生效日期: XXXX 年 XX 月 XX 日 : XX 时 XX 分 XX 秒.

下次更新: XXXX 年 XX 月 XX 日 : XX 时 XX 分 XX 秒.

签名算法: sha1RSA。

7.2.3 CRL 发布

辽宁 CA 每隔 4 小时自动发布最新的 CRL,必要时辽宁 CA 可以随时进行手动发布 CRL。

7.2.4 CRL 下载

辽宁 CA 证书用户可以通过辽宁 CA 网站（www.lnca.org.cn）下载 CRL。

7.3 在线证书状态协议

辽宁 CA 为证书用户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充,方便证书用户及时查询证书状态信息。辽宁 CA 的 OCSP 服务遵循 RFC2560 标准。版本号：OCSP：V1。

8. 认证机构审计和其他评估

8.1 评估的频率或情形

由辽宁 CA 或法律主管部门指定评估者。评估者对辽宁 CA 进行评估。辽宁 CA 本身也需要对辽宁 CA 的关联单位（包含辽宁 CA 授权的注册机构、注册分支机构、受理点等证书体系成员）所有的流程和操作进行审计和评估，检验其是否符合本电子认证业务规则和相应的证书政策的规定，其频率可由辽宁 CA 决定或由法律制定的监管机构决定。

辽宁 CA 对其关联单位实行定期评估（一般为 1 年），评估人员由辽宁 CA 指定。

8.2 评估者的资质

对辽宁 CA 实施规范审计和评估的评估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：

1）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。

2）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。

3）具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

对辽宁 CA 进行评估的评估者必须是一个独立于辽宁 CA 的实体。

8.4 评估内容

对辽宁 CA 规范评估应包括:

1）辽宁 CA 支持的证书认证操作规程是否与本电子认证业务规则表达一致，包括辽宁 CA 的技术、手续和员工的相关管理政策和业务声明。

2）辽宁 CA 是否实施了相关技术、管理、相关政策和业务声明。

3）评估者或辽宁 CA 认为有必要评估的其他方面。

8.5 对问题与不足采取的措施

如果在评估过程中发现执行规范有不足之处，辽宁 CA 将根据评估报告的内容准备一份解决方案，明确对此采取的相应行动。辽宁 CA 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 评估结果的传达与发布

除非法律明确要求，否则辽宁 CA 一般不公开评估结果。在必要

的情况下，向辽宁 CA 关联单位（例如注册机构、受理点）通知审计结果的具体规定将在辽宁 CA 和关联单位的协议中写明。

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

证书持有者以及所有使用辽宁 CA 的各方必需支付辽宁 CA 服务费用（包括证书颁发或更新费用、证书访问费用、 吊销或状态信息访问费用、其他服务的费用）。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。辽宁 CA 也可以通过网站、电子邮件、电话等其他方法通知证书持有者或其他各方费用变化。

9.1.1 证书签发和更新费用

辽宁 CA 采用政府主导，企业运营的运行机制，向社会各界提供服务的同时，按照“有偿服务、不以赢利为目的”的原则，对数字证书的发放、验证和管理实行有偿服务，用户有义务按照规定向辽宁 CA 交纳相关服务费用。

根据辽宁省物价局收费文件及辽宁 CA 的价目表，辽宁 CA 在不高于此价格的前提下可以对证书价格进行适当调整。

9.1.2 证书查询费用

辽宁 CA 目前不收取查询费用，但辽宁 CA 保留对用户证书查询操作进行收费的权利。

9.1.3 证书吊销或状态信息的查询费用

辽宁 CA 目前不收取此类费用，但辽宁 CA 保留对证书吊销或状态信息的查询操作进行收费的权利。

9.1.4 其他服务费用

其他服务费用包括:

1. 密钥更新的费用;

2. 证书恢复的费用;

3. 其他与证书相关的费用。

以上各项费用均根据辽宁省物价局收费标准及辽宁 CA 的价目表收取。

9.1.5 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。

9.2 财务责任

辽宁 CA 授权的发证机关（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用户、接收方以及其他信任其签发的证书和时间戳的组织和个人造成的责任风险。

9.2.1 保险范围

对于操作中涉及的其它用户财务相关信息的保险，例如财务报表、担保合同、信用证明和各种权益证明，目前没有开设相应险种。

对于终端用户由于使用辽宁 CA 证书服务造成的事故的保险和担保，目前没有开设相应险种。

9.2.2 其他资产

辽宁 CA 以其全部资产保障正常运营。

9.2.3 对最终实体的保险或担保

在任何情况下，辽宁 CA 及发证机关将不会对任何间接的、特殊的、结果性的、附带性的损失负责，也不对由于数字证书、数字签名、或其他任何于此提供或考虑的交易或服务引起的，或与之有关的使用、移交、授权、执行、不执行、或无法使用等情况造成的利益损失、数据丢失、或其他间接性的、结果性的、或惩罚性的损失负责。即便是事先被提醒了该损失发生的可能性，辽宁 CA 和发证机关也不需负责。

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 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:

(i) 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;

(ii) 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;

(iii) 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 个人隐私保密

对于个人隐私信息，辽宁 CA 会尽最大的努力进行保护。

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:

(i) 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;

(ii) 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;

(iii) 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:

(i) 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;

(ii) 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;

(iii) 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 关联机构(注册机构、受理机构)知悉并同意辽宁 CA 拥有辽宁 CA、辽宁 CA 的合作方及/或特许权授予方在服务中产生的所有想法、观念、技术、发明、程序或创作成果之知识产权（“知识产权”），该想法、观念、技术、发明、程序或创作成果包含、呈现或运用在辽宁 CA 所提供的产品或服务中。

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 注册机构的陈述与担保

经辽宁 CA 依据认证业务声明指定的地方注册机关应 (a)严格遵守辽宁 CA 认证业务规则、手册及地方注册机关的要求条件中所列明的职责，包括但不限于确认证书申请资料、批准或驳回该证书申请、使用辽宁 CA 指定的软件与硬件、以及发出证书吊销请求等; (b)在地方注册机关批准某证书申请后，辽宁 CA (i) 应有权信赖经批准的证书申请中的信息是正确的，及(ii)向发出该证书申请的申请人签发一张证书; (c)地方注册机关应以称职、专业及熟练的方式履行辽宁 CA 的业务规范;（d）地方注册机关应使接受证书的用户遵守"数字证书申请表"的条款;（e）地方注册机关应依据其选择的证书数量，支付给辽宁 CA 按照协议价格应支付的证书服务费用;（f）地方注册机关不得移动或破坏任何辽宁 CA 产品资料或文件上之所有商标和版权声明;(g)地方注册机关向辽宁 CA 保证: (i) 所有关于签发证书且由地方注册机关鉴证的信息资料，其实质是真实且正确的; (ii)不限于上述之一般原则，地方注册机关对证书申请的批准将不会造成证书的错误签发，其中包括且不限于因冒名顶替而造成的错误签发;及(iii)地方注册机关充分遵行辽宁 CA 认证业务规则及地方注册机关的要求条件中所要求的各项内容。

9.6.3 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“数字证书申请表”并同意本责任书之条款，并承诺提供真实信息;（b）用户交付数字证书申请表，即表示您要求

发证机构签发数字证书予您，亦表示您已同意数字证书申请表中的条款。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此表的约定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。

9.6.4 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.

9.6.5 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

辽宁 CA 不对由于不可抗力造成的操作失败或延迟承担任何损失、损坏或赔偿责任。

辽宁 CA 在提供给证书持有者的“数字证书申请表”中都有事先告知证书持有者，辽宁 CA 发放的各类型数字证书只能用于网络上标识身份、加密数据、保证网络安全通讯等相应证书规定的用途，不能作为其他任何用途。若证书持有者将其数字证书用于其他的用途，辽

宁 CA 不承担任何责任。辽宁 CA 在进行申请者身份认证或证书制作时，将充分遵守辽宁 CA 的安全操作流程。如果由于非辽宁 CA 的原因而造成的辽宁 CA 设备故障、线路中断，导致签发数字证书错误、延误、中断或者无法签发，辽宁 CA 不负任何赔偿责任。辽宁 CA 在签发数字证书之前，证书申请实体已同意遵守“数字证书申请表”中的各项规定。如果证书申请实体故意或无意地提供不完整、不可靠或已过期的信息，而又根据正常的流程提供了必须的审核文件，由此得到了辽宁 CA 签发的数字证书，由此引起的法律和经济责任由证书申请实体全部承担，辽宁 CA 不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。辽宁 CA 也不承担任何其他未经授权的人或组织以辽宁 CA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。辽宁 CA 仅仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不表明有对此承担法律责任等方面的约定。

9.8 有限责任

在任何情况下，辽宁 CA 及发证机关将不会对任何间接的、特殊的、结果性的、附带性的损失负责，也不对由于数字证书、数字签名、或其他任何于此提供或考虑的交易或服务引起的，或与之有关的使用、移交、授权、执行、不执行、或无法使用等情况造成的利益损失、数据丢失、或其他间接性的、结果性的、或惩罚性的损失负责。即便是事先被提醒了该损失发生的可能性，辽宁 CA 和发证机关也不需负责。

9.9 赔偿

如辽宁 CA 违反了前款陈述和担保规定的职责，辽宁 CA 承担赔偿责任（法定或约定免责除外）的赔偿限制如下：辽宁 CA 所有的赔偿义务不高于这种证书适用的赔偿责任上限。

赔偿责任上限为证书持有人当年实际缴纳的数字证书年服务费的 5 倍。这种赔偿责任上限可以由辽宁 CA 根据情况重新制定，辽宁 CA 会将重新制定后的情况立刻通知相关当事人。辽宁 CA 只有在用户数字证书有效期限内承担赔偿责任。

注册机构、注册分支机构、受理点等相关机构的责任在各参与方和辽宁 CA 之间签订的协议中表明。

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。

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。

9.11 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管理小组提出修改申请，安全管理小组将会同相关人员在 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，并在得到安全管理小组的认可后，上报辽宁 CA 批准予以公布并通知。

修订流程为:

1. 小组提出修订意见，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. 进行修改并由公司决策层批准;
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

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。

9.14 适用法律

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

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，用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，或政府有关规定、指导方针明确地言明优于本电子认证业务规则。

9.16 一般条款

9.16.1 完整协议

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。

9.16.2 转让

无论是各方明示的或暗示的继任者、执行者、继承者、代表、管理者和受让人，辽宁 CA 均保证其权益，并对其有约束力。各方可根据法律转让（包括合并或转让可控有价证券）辽宁 CA 详述的权利和义务。转让时发证机关操作的终止或暂停或该转让正在发生时，不影

响到转让方对另一方的任何债务或责任的更新。

直接影响辽宁 CA 或发证机关的权利和义务的条款和规定，除非通过受到影响的当事人发出经过鉴定的信息或文件，或者在此另有其他规定，否则不能进行口头上的修正、放弃、补充、修改或终止。

9.16.3 分割性

辽宁 CA 认证服务规则任何条款或其应用，如果因为任何原因或在任何范围内发现无效或不能执行，那么规则其余的部分（以及对它方的无效或不能执行的条款的适用）将会做出合理的解释以反映当事人的原意。相关当事人了解并同意，辽宁 CA 认证服务规则所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，系可独立于其它条款的个别条款，并加以执行。

9.16.4 强制执行

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、翻译和有效性对享有辽宁 CA 认证服务的各参与方具有最高约束力。在合同纠纷中有利的一方有权将代理费作为偿还要求的一部分。

9.16.5 不可抗力

由于不可预见的原因和不可控的原因，视为不可抗力，会导致合同或协议的终止。例如战争、恐怖行动、罢工、自然灾害、供货商或代理商倒闭、互联网或其它基础设施无法使用等。但各方都有义务建立灾难恢复和业务连续性机制。

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。