

辽宁数字证书认证管理有限公司

证书策略

v1.0

辽宁数字证书认证管理有限公司

2024 年 10 月

目录

1.概括性描述	1
1.1 概述	1
1.2 电子认证活动参与者	1
1.2.1 电子认证服务机构	1
1.2.2 注册机构	1
1.2.3 订户及证书类型	2
1.2.4 依赖方	2
1.2.5 其它参与者	2
1.3 证书应用	2
1.3.1 适合的证书应用	2
1.3.2 禁止的证书应用	3
1.4 策略管理	3
1.4.1 策略文档管理机构	3
1.4.2CP 制定程序	3
1.4.3 联系方式	3
1.4.4 定义和缩写	4
2.信息发布与信息管理的	7
2.1 信息库	7
2.2 认证信息的发布	7
2.3 发布的时间或频率	7
2.4 信息库访问控制	7
3.身份标识与鉴别	8
3.1 命名	8
3.1.1 名称类型	8
3.1.2 对名称意义化的要求	8
3.1.3 用户的匿名或伪名	8
3.1.4 理解不同名称形式的规则	8

3.1.5 名称的唯一性	9
3.1.6 商标的识别、鉴别和角色	9
3.2 初始身份确认	9
3.2.1 证明拥有私钥的方法	9
3.2.2 证书订户信息鉴别	10
3.2.3 互操作准则	10
3.3 密钥更新请求的标识与鉴别	11
3.3.1 更新申请情况	11
3.3.2 更新操作	11
3.3.3 更新申请的确认	11
3.3.4 废止后密钥更新的标识与鉴别	11
3.4 撤销请求的标识与鉴别	12
3.4.1 证书废止（撤销）情况	12
3.4.2 废止操作	12
3.4.3 废止申请的确认	12
4. 数字证书服务操作要求	12
4.1 证书申请	13
4.1.1 证书申请实体	13
4.1.2 注册过程与责任	13
4.2 证书申请处理	13
4.2.1 执行识别与鉴别功能	13
4.2.2 证书申请批准和拒绝	13
4.2.3 处理证书申请的时间	14
4.3 证书签发	14
4.3.1 证书签发中注册机构和电子认证服务机构的行为	14
4.3.2 电子认证服务机构和注册机构对用户的通告	14
4.4 证书接受	15
4.4.1 构成接受证书的行为	15
4.4.2 电子认证服务机构对证书的发布	15

4.5 密钥对和证书的使用	15
4.5.1 订户私钥和证书的使用	15
4.5.2 信赖方公钥和证书的使用	15
4.6 证书更新	16
4.6.1 证书更新的情形	16
4.6.2 请求证书更新的实体	16
4.6.3 证书更新请求的处理	16
4.6.4 颁发更新证书时对用户的通告	17
4.6.5 构成接受更新证书的行为	17
4.6.6 电子认证服务机构对更新证书的发布	17
4.6.7 电子认证服务机构对其他实体的通告	17
4.7 证书密钥更新	18
4.7.1 证书密钥更新的情形	18
4.7.2 请求证书密钥更新的实体	18
4.7.3 证书密钥更新请求的处理	18
4.7.4 颁发更新证书时对用户的通告	18
4.7.5 构成接受密钥更新证书的行为	19
4.7.6 电子认证服务机构对密钥更新证书的发布	19
4.7.7 电子认证服务机构对其他实体的通告	19
4.8 证书变更	19
4.8.1 证书变更的情形	19
4.8.2 请求证书变更的实体	20
4.8.3 证书变更请求的处理	20
4.8.4 颁发新证书时对用户的通告	20
4.8.5 构成接受变更证书的行为	20
4.8.6 电子认证服务机构对变更证书的发布	21
4.8.7 电子认证服务机构对其他实体的通告	21
4.9 证书吊销和挂起	21
4.9.1 证书吊销的情形	21

4.9.2 请求证书吊销的实体	22
4.9.3 吊销请求的流程	22
4.9.4 吊销请求宽限期	22
4.9.5 电子认证服务机构处理吊销请求的时限	23
4.9.6 依赖方检查证书吊销的要求	23
4.9.7CRL 发布频率	23
4.9.8CRL 发布的最大滞后时间	23
4.9.9 在线状态查询的可用性	23
4.9.10 在线状态查询要求	24
4.9.11 吊销信息的其他发布形式	24
4.9.12 密钥损害的特别要求	24
4.9.13 证书挂起的情形	24
4.9.14 请求证书挂起的实体	25
4.9.15 挂起请求的流程	25
4.9.16 证书挂起请求的处理时间	25
4.9.17 挂起的期限限制	26
4.10 证书状态服务	26
4.10.1 操作特征	26
4.10.2 服务可用性	26
4.11 订购结束	27
4.11.1 证书废止情况	27
4.11.2 废止操作	27
4.12 密钥生成、备份与恢复	27
5.认证机构设施、管理和操作控制	28
6.认证系统技术安全控制	28
7.证书、证书吊销列表和在线证书状态协议	28
7.1 证书	28
7.1.1 版本号	28
7.1.2 证书扩展项	28

7.1.3 名称形式	29
7.1.4 名称限制	29
7.2 证书吊销列表	30
7.2.1 版本号	30
7.2.2CRL 和 CRL 条目扩展项	30
7.2.3CRL 发布	30
7.2.4CRL 下载	30
7.3 在线证书状态协议	30
8.认证机构审计和其它评估	31
8.1 评估的频率或情形	31
8.2 评估者的资质	31
8.3 评估者与被评估者之间的关系	31
8.4 评估内容	32
8.5 对问题与不足采取的措施	32
9.法律责任和其他业务条款	32

1. 概括性描述

1.1 概述

证书策略（CP，CertificatePolicy）是认证机构（CA, CertificationAuthority）制订的一组策略，表明辽宁 CAPKI 体系中的各个参与者的划分与其义务，并包含辽宁 CA 证书基本策略。

本证书策略的适用范围为辽宁 CA 发放的证书。

1.2 电子认证活动参与者

本文中所包含的电子认证活动参与者有：电子认证服务机构、注册机构、订户、依赖方以及其它参与者，下面将分别进行描述。

1.2.1 电子认证服务机构

电子认证服务机构 CA（CertificationAuthority）承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或 CRL）发布、政策制定等工作。

1.2.2 注册机构

注册机构 RA (RegistrationAuthority) 负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

辽宁 CA 与合作机构签署协议，合作机构可成为辽宁 CA 的注册机构，并遵照辽宁 CA 的《注册机构运营管理办法》开展数字证书业务。

辽宁 CA 本身承担 RA 职责，不委托其它机构行使此职责。

1.2.3 订户及证书类型

订户是指向辽宁 CA 申请证书的实体。

需要明确的是，证书订户与证书主体是两个不同的概念。“证书订户”是指向辽宁 CA 申请证书的实体，通常为个人或机构；“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。

1.2.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.2.5 其它参与者

除电子认证服务机构（辽宁 CA）、订户和依赖方以外的参与者称为其它参与者。

1.3 证书应用

1.3.1 适合的证书应用

辽宁 CA 证书支持相应的合法应用，具体应用场景和配套软件（如

浏览器) 在相应 CPS 中说明。

1.3.2 禁止的证书应用

辽宁 CA 签发的证书不能在任何与国家或地方法律、法规规定相违背的应用系统中使用。

1.4 策略管理

1.4.1 策略文档管理机构

本 CP 由辽宁 CA “安全管理小组” 负责起草和管理。

1.4.2 CP 制定程序

经“安全管理小组”共同讨论后, 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。最终确定 CP 文本格式和版本号, 形成最终的定稿, 之后在 15 个工作日内报国家密码管理局进行备案。

备案完成后, 在公司网站上发布。

“安全管理小组”会定期对存在的业务风险进行评估, 并及时对本 CP 进行修订。

1.4.3 联系方式

本 CP 的发布地址: <https://www.lnca.org.cn>

如对本 CP 有任何疑问, 可联系:

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

1.4.4 定义和缩写

- ANSI

美国国家标准协会(TheAmericanNationalStandardsInstitute)

- CA

电子认证服务机构(CertificateAuthority)

- RA

注册机构(RegistrationAuthority)

- CRL

证书吊销列表(CertificateRevocationList)

- OCSP

在线证书状态协议(OnlineCertificateStatusProtocal)

- CP

证书策略(CertificatePolicy)

- CPS

电子认证业务规则(CertificatepracticeStatement)

- CSR

证书签名请求 (CertificateSignatureRequest)

- IETF

互联网工程任务组 (TheInternetEngineeringTaskForce)

- 电子认证服务机构

受订户信任的，负责创建和签发、管理公钥证书的权威机构，有时也可订户创建密钥。

- 注册机构

面向证书订户，负责订户证书的申请、审批和证书管理工作。

- 数字证书

经 CA 数字签名包含数字证书使用者身份公开信息和公开密钥的电子文件。

- 证书吊销列表

一个严格要求进行周期性发布的列表，被 CA 签名，用于标记一系列不再被证书发布者所信任的证书列表。

- 在线证书状态协议

IETF 颁布的用于检查数字证书状态的协议。

- 证书策略

一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。例如，一个特定的 CP 可以指明某类证书适用于鉴别从事企业到企业 (B-to-B) 交易活动的参与方，针对给定价格范围内的产品和服务。

- 电子认证业务规则

关于电子认证服务机构在签发、管理、吊销或更新证书（或更新证书中的密钥）过程中所采纳的业务实践的声明。

- 订户

申请证书的实体。

- 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构。

- 私钥

经由数学运算产生的密钥（由持有者保管），用于制作数字签名，亦可依据运算方式，就相对应的公开密钥加密的文件或信息（以确保资料的机密性）予以解密。

- 公钥

经由数学运算产生的密钥，可公开取得、并可用于验证由其对应的私钥所产生的数字签名。公开密钥亦可依据其运算方式，将信息或档案加密，再以对应的私钥进行解密。

- 唯一甄别名

在数字证书的主体名称域中，用于唯一标识证书主体的 X.500 名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

2. 信息发布与信息管理

2.1 信息库

辽宁 CA 信息库面向订户及证书应用依赖方提供信息服务。辽宁 CA 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、辽宁 CA 网站信息以及辽宁 CA 不定期发布的信息。

2.2 认证信息的发布

辽宁 CA 的 CPS、CP 以及相关的技术支持信息等辽宁 CA 网站上发布。用户证书可通过辽宁 CA 证书下载平台获取，已被吊销了的证书的信息可从 CRL 站点查获，证书的状态（有效、吊销、挂起）可通过 OCSP 服务获得。

2.3 发布的时间或频率

CPS、CP 以及相关业务规则在完成 1.5.4 所述的批准流程后的 15 个工作日内发布到辽宁 CA 网站上，并可确保 7*24 小时可访问；订户有特殊要求的，将根据订户的需求，适当提高 CRL 发布的频率。辽宁 CA 签发的 CRL 信息，根据需要，也可以人工方式实时发布。

2.4 信息库访问控制

辽宁 CA 的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

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

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) =	个人证书和设备证书：单位名称； 单位证书：上级主管单位	辽宁 CA
OrganizationalUnit (OU) =	个人证书：“@”+身份识别码 单位证书：“@”企业代码证号	@01212345-2
OrganizationalUnit (OU) =	“!”+证书应用预留字段，具体定义在证书应用中完成	
OrganizationalUnit (OU) =	单位部门	软件部
StateorProvince (S) =	省	辽宁省
Locality (L) =	市	沈阳市

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(与身份证上标明的一致)
2	单位身份证书	单位名称(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(与身份证上标明的一致)
4	单位代码签名证书	单位名称(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(与身份证上标明的一致) 单位证书为单位名称(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，且不承担任何相关的任何责任

电子政务数字证书命名符合国家密码管理局颁布的《电子政务数字证书格式规范》要求，不允许使用匿名或假名。

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 证书订户信息鉴别

订户在申请辽宁 CA 签发的证书前应指定并书面授权证书的申请代表，提供有效身份证明文件、证书申请文件或以辽宁 CA 认可的安全方式提交订户真实有效信息，并接受证书申请的有关条款，同意承担相应的责任。

辽宁 CA 或者辽宁 CA 的注册机构接受订户的证书申请后，应对订户的身份真实性进行审核，并按照双方的约定妥善保管订户申请材料。具体鉴别内容参见 CPS 相应章节。

3.2.3 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

具体操作内容参见 CPS 相应章节。

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 撤销请求的标识与鉴别

3.4.1 证书废止（撤销）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

具体操作内容参见 CPS 相应章节。

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。

4. 数字证书服务操作要求

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》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

具体鉴别内容参见 CPS 相应章节。

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在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，以及其他凡是辽宁 CA 各类证书的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，携带证书《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，以及其他凡是辽宁 CA 各类证书的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，也可以是由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，以及其他凡是辽宁 CA 各类证书的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 24 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 CACRL 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 吊销信息的其他发布形式

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

如果有以下情况，辽宁 CA 将会考虑挂起证书：

1. 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，可以申请证书挂起等情形。

2. 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；

3. 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挂起请求并获得批准。

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，以及其他凡是辽宁 CA 各类证书的有效期限未到的证书持有者或其授权的代理人、证书注册机构、受理点、政府主管部门或国家司法机关。

4.9.15 挂起请求的流程

1. 挂起申请人需向辽宁 CA 提交挂起申请表和身份证明材料，同时说明挂起的理由，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）提交挂起申请，同样需要填写申请表并加盖公章；

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

3. 证书服务机构审核挂起申请后，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；

4. 电子认证服务机构在处理挂起申请后，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挂起。

4.9.16 证书挂起请求的处理时间

证书用户提出挂起请求并经辽宁 CA 审核通过后，进行挂起操作，挂起操作根据用户情况，可立即完成或在三个工作日内受理完成。

4.9.17 挂起的期限限制

证书挂起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。

4.10 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.lnca.org.cn>。

4.10.1 操作特征

用户可根据所要查找用户的相关信息查询，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 24 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。

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

本章节参见相关 CPS 内容

6. 认证系统技术安全控制

本章节参见相关 CPS 内容

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《公钥和属性证书框架（GB/T16264.8-2005）》中声明的证书格式。

7.1.1 版本号

V3

7.1.2 证书扩展项

辽宁 CA 颁发的证书除支持 IETF RFC3280 中定义的扩展项外，还支持私有扩展项。

辽宁 CA 采用的 IETF RFC3280 中定义的扩展项有：

- 颁发机构密钥标识符 AuthorityKeyIdentifier
- 主题密钥标识符 SubjectKeyIdentifier
- 密钥用法 KeyUsage
- 基本限制 BasicConstraints
- CRL 分发点 CRLDistributionPoints

私有扩展项有：

- ” 1.2.86.11.7.1” 个人身份标识码
- ” 1.2.86.11.7.2” 个人社会保险号
- ” 1.2.86.11.7.3” 企业组织机构代码
- ” 1.2.86.11.7.4” 企业工商注册号
- ” 1.2.86.11.7.5” 企业国税号
- ” 1.2.86.77.1” 企业地税号

7.1.3 名称形式

采用 X.500 甄别名格式。

完整的名称应当符合的格式，参见本 CP3.1.2 章节。

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。命名方式参见本 CP3.1.4 章节。

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《公钥和属性证书框架（GB/T16264.8-2005）》中声明的格式。

7.2.1 版本号

V2。

7.2.2 CRL 和 CRL 条目扩展项

不使用 CRL 扩展项，也没有使用 CRL 条目扩展项。

7.2.3 CRL 发布

辽宁 CA 每隔 24 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. 认证机构审计和其它评估

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。

9. 法律责任和其他业务条款

本章节参见相关 CPS 内容