黑龙江省数字证书认证有限公司
电子认证业务规则

3.0 版

黑龙江省数字证书认证有限公司

2026 年 7 月

修订记录

版本号	修改状态	修改说明	审批/批准人	生效日期
1.0	发布	形成版本并审核通过	策略管理委员会	2016 年 10 月
2.0	修订	修改部分章节内容描述并增加补充说明	策略管理委员会	2022 年 2 月
3.0	修订	参照 T/CQAE 11034-2025 电子认证业务规则规范修订	策略管理委员会	2026 年 7 月

目 录

1 概括性描述 1
1.1 承诺 1
1.2 基本信息 1
1.3 文档名称与标识 2
1.4 电子认证活动参与者 3
1.4.1 电子认证服务机构（CA） 3
1.4.2 注册机构（RA） 3
1.4.3 订户 3
1.4.4 依赖方 4
1.5 证书应用 4
1.5.1 证书应用分类 4
1.5.2 证书应用限制 5
1.6 策略管理 6
1.6.1 策略管理机构 6
1.6.2 策略文档的批准程序 6
1.7 定义和缩写 6
2 信息发布与信息管理 8
3 身份标识与鉴别 9
3.1 身份查验通用要求 9
3.1.1 订户告知 10
3.2 初始身份确认 11
3.2.1 证明拥有私钥的方法 11
3.2.2 个人身份的查验 11
3.2.3 机构身份的查验 13
3.3 订户意愿记录 14
3.3.1 订户意愿记录内容 14
3.3.2 个人高等级证书的意愿记录 15
3.3.3 个人基础级证书的意愿记录 15

3.3.4 机构高等级证书的意愿记录 15
3.3.5 机构基础级证书的意愿记录 16
3.4 订户协议 16
3.5 未验证的订户信息 16
3.6 互操作要求 16
3.7 命名 17
3.7.1 名称类型 17
3.7.2 对名称意义化的要求 17
3.7.3 订户的匿名或伪名 17
3.7.4 理解不同名称形式的规则 17
3.7.5 名称的唯一性 18
3.7.6 商标的识别、鉴别和角色 18
4 证书生命周期操作要求 18
4.1 通用要求 18
4.2 证书申请 19
4.2.1 证书申请实体 19
4.2.2 执行识别与鉴别功能 19
4.2.3 证书申请批准和拒绝 19
4.2.4 处理证书申请的时间 20
4.2.5 处理证书申请提交人的核查 20
4.3 证书签发 20
4.3.1 证书所含信息的审核验证及获得证书的方式 20
4.3.2 证书签发中电子认证服务机构的行为 21
4.3.3 电子认证服务机构对订户的通告 21
4.4 证书接受 21
4.5 密钥对和证书的使用 22
4.6 证书续期 22
4.7 证书密钥更新 22
4.8 证书变更 23
4.9 证书撤销和冻结 23

4.9.1 证书撤销的情形 23
4.9.2 撤销请求的流程 24
4.9.3 证书冻结的情形 24
4.9.4 请求证书冻结的实体 24
4.9.5 冻结请求的流程 25
4.10 证书状态信息服务 25
4.10.1 操作特征 25
4.10.2 服务可用性 25
4.10.3 可选特征 26
4.11 停止使用认证服务 26
4.12 密钥托管与恢复 27
4.12.1 订购结束 27
4.12.2 密钥生成、备份与恢复的策略和行为 27
4.12.3 会话密钥的封装与恢复的策略和行为 28
5 认证机构设施、管理和操作控制 28
5.1 物理控制 28
5.1.1 场地位置与建筑 28
5.1.2 物理访问 29
5.1.3 电力与空调 30
5.1.4 水患防治 30
5.1.5 火灾防护 30
5.1.6 介质存储 30
5.1.7 废物处理 31
5.1.8 异地备份 31
5.1.9 设备台账 31
5.2 操作过程控制 32
5.2.1 可信角色 32
5.2.2 每个角色的识别与鉴别 32
5.2.3 职责分离 32
5.3 人员控制 33

5.3.1 可信人员资格要求 33
5.3.2 背景审查程序 33
5.3.3 可信人员培训要求 33
5.3.4 再培训周期和要求 34
5.3.5 工作轮换周期和顺序 34
5.3.6 对未授权行为的处罚 34
5.3.7 独立合约人的要求 34
5.3.8 提供给员工的文档 35
5.4 审计日志程序 35
5.4.1 记录事件的类型 35
5.4.2 处理日志的周期 36
5.4.3 审计日志的保存期限 36
5.4.4 审计日志的保护 36
5.4.5 审计日志备份程序 36
5.4.6 审计日志收集系统 36
5.4.7 对导致事件实体的通告 37
5.4.8 脆弱性评估 37
5.4.9 审计事件 37
5.5 记录归档 38
5.5.1 归档记录的类型 38
5.5.2 归档记录的保存期限 38
5.5.3 归档文件的保护 39
5.5.4 归档文件的备份程序 39
5.5.5 归档记录时间要求 39
5.5.6 归档收集系统 39
5.5.7 获得和检验归档信息的程序 39
5.6 电子认证服务机构根密钥更替 40
5.7 损害和灾难恢复 40
5.7.1 事故和损害处理程序 40
5.7.2 计算资源、软件和/或数据被破坏 41

5.7.3 实体私钥损害处理程序 41
5.7.4 灾难后的业务连续性能力 42
5.8 电子认证服务机构的终止 43
5.9 重大事项报告 44
6 认证系统技术安全控制 46
6.1 技术安全管理制度要求 46
6.2 密钥对的生成和安装 46
6.2.1 根证书密钥对的生成和安装 46
6.2.2 订户密钥对的生成和交付 47
6.2.3 私钥传送给订户 47
6.2.4 公钥传送给证书签发机构 47
6.2.5 电子认证服务机构公钥传送给依赖方 47
6.2.6 密钥的长度 47
6.2.7 公钥参数的生成和质量检查 47
6.2.8 密钥使用目的 48
6.3 私钥保护和密码模块工程控制 48
6.3.1 CA 私钥保护和密码模块工程控制 48
6.3.2 订户私钥保护和密码模块工程控制 48
6.3.3 私钥导入或导出密码模块 49
6.3.4 私钥在密码模块中的存储 49
6.3.5 激活私钥的方法 49
6.3.6 解除私钥激活状态的方法 49
6.3.7 销毁密钥的方法 50
6.3.8 密码模块的评估 50
6.4 密钥对管理的其他方面 50
6.4.1 公钥归档 50
6.4.2 证书操作期和密钥对使用期限 51
6.5 激活数据 51
6.5.1 激活数据的产生和安装 51
6.5.2 激活数据的保护 52

6.5.3 激活数据的其他方面 52
6.6 计算机安全控制 52
6.7 生命周期技术控制 54
6.7.1 系统开发控制 54
6.7.2 安全管理控制 54
6.7.3 生命周期安全控制 54
6.8 网络安全控制 54
6.9 时间戳 55
7 证书、证书撤销列表和在线证书状态协议 55
7.1 证书 55
7.1.1 版本号 56
7.1.2 证书扩展项 56
7.1.3 算法对象标识符 57
7.1.4 名称形式 57
7.2 证书撤销列表 58
7.2.1 版本号 58
7.2.2 CRL 和 CRL 条目扩展项 58
7.3 在线证书状态协议 58
7.3.1 版本号 59
7.3.2 OCSP 扩展项 59
8 认证机构审计及相关评估 59
8.1 审计评估制度 59
8.1.1 评估者的资质 59
8.1.2 评估者与被评估者之间的关系 60
8.1.3 评估内容 60
8.1.4 对问题与不足采取的措施 60
8.1.5 评估结果的传达与发布 60
8.2 认证业务审计 60
8.3 全面符合性评估 61
9 法律责任和其他业务条款 62

9.1 费用 62
9.1.1 证书签发和（或）更新费用 62
9.1.2 证书访问费用 62
9.1.3 证书撤销或状态信息的查询费用 62
9.1.4 其他服务的费用 63
9.1.5 退款策略 63
9.2 财务责任 63
9.3 业务信息保密 63
9.3.1 保密信息范围 63
9.3.2 不属于保密的信息 64
9.3.3 保护保密信息的责任 64
9.4 个人隐私保密 65
9.4.1 隐私保密方案 65
9.4.2 作为隐私处理的信息 65
9.4.3 不被视为隐私的信息 65
9.4.4 保护隐私的责任 65
9.4.5 使用隐私信息的告知或同意 65
9.4.6 依法律或行政程序的信息披露 66
9.4.7 其他信息披露情形 66
9.5 知识产权 66
9.6 陈述和担保 66
9.6.1 电子认证服务机构的陈述与担保 66
9.6.2 注册机构的陈述与担保 67
9.6.3 订户的陈述与担保 67
9.6.4 依赖方的陈述与担保 68
9.6.5 其他参与者的陈述与担保 68
9.7 担保免责 68
9.8 偿付责任规则 69
9.8.1 偿付责任范围 69
9.8.2 对最终实体的赔偿担保 69

9.8.3 责任免除 69
9.9 赔偿 70
9.10 有效期限与终止 71
9.10.1 有效期限 71
9.10.2 终止 72
9.10.3 效力的终止与保留 72
9.11 对参与者的个别通告与沟通 72
9.12 修订和发布 72
9.12.1 修订程序 72
9.12.2 通告机制和期限 72
9.12.3 必须修改业务规则的情形 73
9.13 争议处理与举证 73
9.14 管辖法律 73
9.15 适用法律的符合性 73
9.16 一般条款 74
9.16.1 完整协议 74
9.16.2 分割性 74
9.16.3 强制执行 74
9.16.4 不可抗力 74
9.17 其他条款 75

1 概括性描述

1.1 承诺

黑龙江省数字证书认证有限公司（简称HLJCA），成立于2006年12月，是工业和信息化部批准设立的电子认证服务机构和国家密码管理局批准设立的电子政务电子认证服务机构，经省政府授权的独立法人企业，注册资本为3000万元。作为黑龙江省指定的数字证书安全认证体系建设与管理主体，HLJCA是全省唯一具有法定资质的第三方电子认证机构。其业务活动严格遵守相关法律法规，公司拥有《电子认证服务许可证》、《电子认证服务使用密码许可证》、《电子政务电子认证服务许可证》和国家电子政务外网黑龙江省电子认证注册服务中心资质。HLJCA致力于提供数字证书的申请、签发、制作、认证管理以及电子签章业务等电子认证服务。为个人和企事业单位提供身份认证、数字签名、电子签章服务以及密码应用解决方案。

公司始终坚守合规经营底线，所有业务开展全过程严格遵守法律法规，坚持以人民为中心的服务理念，积极承担社会责任。合作前全面开展业务调研与风险评估，落实内部定责机制，坚决杜绝违规业务合作。公司统一使用经国家密码管理局审查认证的系统开展服务，主动接受政府与社会监督，建立长效整改机制，保障业务持续合规。

历经近二十年发展，HLJCA组建了全链条专业团队，已成长为区域创新型高科技企业。未来我们将持续筑牢网络安全信任根基，护航电子政务、电子商务与群众信息安全，携手各界共促全省数字信任体系发展。

1.2 基本信息

【公示信息专区】

机构名称：黑龙江省数字证书认证有限公司

法定代表人：隋承钢

经营地址：黑龙江省哈尔滨市道外区东直路480号

联系方式：0451-55918888

邮箱：zhux@hljca.com

【许可证书信息】

证书名称	编号	有效期
电子认证服务许可证	ECP23011021044	2021年10月27日 至 2026年10月26日
电子认证服务使用密码许可证	0043	2026年4月13日 至 2031年4月13日
电子政务电子认证服务机构资质证书	ZWRZ-2320170038	2025年6月3日 至 2030年6月2日

HLJCA目前有证书链如下：ROOTCA证书（SM2）是国家密码管理局的根证书，密码算法为SM2，根密钥长度为256-bit，证书编号：69e2fec0170ac67b，有效期2012年7月14日-2042年7月7日，下设HLJCA_SM2证书，密钥长度为256-bit，签发采用国密算法SM2，证书编号：2665d34e9b226d43117c6a005bef7621，有效期2016年3月31日-2036年3月26日。

电子认证业务规则（Certification Practice Statement，简称CPS）是关于认证机构（CA，Certification Authority）在全部证书服务生命周期中的业务实践（如签发、管理、更新证书或密钥）所遵循规范的详细描述和声明。本文档的编写遵从《中华人民共和国电子签名法》《电子认证服务管理办法》《电子认证业务规则规范》（T/CQAE 11034-2025）等法律法规。为了规范证书业务的正常开展，黑龙江省数字证书认证有限公司发布了《黑龙江省数字证书认证有限公司电子认证业务规则》。

1.3 文档名称与标识

本文档名称为《黑龙江省数字证书认证有限公司电子认证业务规则》，是HLJCA对所提供的认证及相关业务的全面描述。

扩展项名称	OID
组织机构代码证号	1.2.156.10260.4.1.3
个人的身份证号标识	1.2.156.10260.4.1.1

国密 CRL 发布点	2.5.29.31
签名加密密钥用法	2.5.29.15
用户证书签名密钥用法	2.5.29.15
CA 证书签名密钥用法	2.5.29.15
用户证书加密密钥用法	2.5.29.15
根 CA 基本限制	2.5.29.19
业务 CA 基本限制	2.5.29.19
业务子 CA 基本限制	2.5.29.19

1.4 电子认证活动参与者

1.4.1 电子认证服务机构（CA）

HLJCA是根据《中华人民共和国电子签名法》和《电子认证服务管理办法》等规定，依法设立的第三方电子认证服务机构。

电子认证服务机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.4.2 注册机构（RA）

注册机构作为电子认证服务机构授权委托的下属机构，包括注册管理系统（RA系统）和受理点，负责受理证书申请，并负责在订户和CA之间传递证书管理信息。

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

1.4.3 订户

在电子签名应用中，订户即电子签名人或证书持有人，是获颁证书的证书主体，是HLJCA颁发证书的最终用户，可以是个人、机构或基础设施的组成部件如路由器、防火墙、服务器或用于安全通信的其他设备。

1.4.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是，也可以不是一个订户。

在HLJCA证书服务体系中，是信任HLJCA证书，可以对使用HLJCA证书机制进行的数字签名进行验证，使用其他HLJCA证书的公钥的实体。

HLJCA负责保证数字证书身份的真实性。

1.5 证书应用

1.5.1 证书应用分类

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。HLJCA仅颁发以下四类证书。

1.5.1.1 个人高等级电子签名认证证书

个人高等级电子签名认证证书为符合《中华人民共和国电子签名法》的个人电子签名认证证书（主管部门证书策略OID：2.16.156.339.2.1.1.2）。适用于安全等级高、高风险的业务场景，适用于电子合同签署、生命健康、高价值电子交易、金融业务办理等对身份真实性和电子签名可靠性要求较高的应用场景。申请个人高等级电子签名认证证书时，申请人需提交完整、真实、有效的身份信息及相关证明材料。

1.5.1.2 个人基础级电子签名认证证书

个人基础级电子签名认证证书为符合《中华人民共和国电子签名法》的个人电子签名认证证书（主管部门证书策略OID：2.16.156.339.2.1.1.1）。适用于一般安全需求或低风险业务场景，适用于一般电子政务服务、普通网络身份认证、日常电子业务办理及低风险电子交易等应用场景。申请个人基础级电子签名认证证书时，申请人需提供真实有效的身份信息及相关申请材料。

1.5.1.3 机构高等级电子签名认证证书

机构高等级电子签名认证证书为符合《中华人民共和国电子签名法》的机构电子签名认证证书（主管部门证书策略OID：2.16.156.339.2.1.2.2）。适用于安全要求高、高风险业务的重要机构业务场景，适用于电子公文交换、电子印章、生命健康、重要合同签署、金融及监管业务等高风险应用场景。申请机构高等级电子签名认证证书时，应提交完整的机构身份资料、法定代表人或授权代理人身份证明材料及相关授权文件。

1.5.1.4 机构基础级电子签名认证证书

机构基础级电子签名认证证书为符合《中华人民共和国电子签名法》的机构电子签名认证证书（主管部门证书策略OID：2.16.156.339.2.1.2.1）。适用于一般机构业务及低风险应用场景，适用于普通电子商务、一般业务系统登录、电子业务申报及低风险数据交换等应用场景。申请机构基础级电子签名认证证书时，提交机构相关身份证明材料及申请资料。

1.5.2 证书应用限制

HLJCA签发的数字证书必须在法律法规允许及证书规定的适用范围内使用，禁止在包括但不限于以下场景中使用：

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。订户超出证书适用范围或违反相关规定使用数字证书所产生的法律责任和后果，由订户自行承担。

1.6 策略管理

1.6.1 策略管理机构

本《电子认证业务规则》由HLJCA安全策略管理委员会负责起草、发布、更新等事宜。HLJCA安全策略委员会由来自公司管理层、行政中心、技术中心、客户服务中心等拥有决策权的合适代表组成。

本策略文档的对外咨询服务等日常工作由客户服务中心负责。

本《电子认证业务规则》由黑龙江省数字证书认证有限公司拥有完全版权。

HLJCA设立了安全策略委员会并公示成员名单，明确工作职责并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。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：

a）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；

b）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；

c）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；

d）每年组织运营风险评估并形成报告。

1.6.2 策略文档的批准程序

本《电子认证业务规则》由HLJCA安全策略管理委员会组织CPS的编写，CPS草案完成后，由HLJCA安全策略管理委员会进行CPS草案初步评审。初步评审后，将CPS评审稿提交HLJCA安全策略管理委员会审批。经HLJCA安全策略管理委员会审批通过后，在服务范围内进行发布。

本《电子认证业务规则》经HLJCA安全策略管理委员会审批通过后,三十日内向工业和信息化部备案并对外公布。

1.7 定义和缩写

下列定义适用于本《电子认证业务规则》。

公开密钥基础设施（PKI）Public Key Infrastructure

支持公开密钥的管理并提供真实性、保密性、完整性以及可追究性安全服务的具有普适性的安全基础设施。

证书策略（CP）Certificate Policy

是一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和（或）具体应用类的适用性。

电子认证业务规则（CPS）Certification Practice Statement

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

电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

注册机构（RA）Registration Authority

RA是CA认证体系的一个功能组件，具有下列一项或多项功能的实体：识别和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。

轻量级目录访问协议（LDAP）Lightweight Directory Access Protocol

用于查询、下载数字证书以及证书撤销列表（CRL）。

证书撤销列表（CRL）Certificate Revocation List

标记一系列不再被证书发布者所信任的证书的签名列表，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。

电子签名认证证书（证书）Digital Certificate

是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

证书持有者、订户subscriber

所有拥有任何HLJCA证书的个人或实体，不包括HLJCA管理员证书。

证书使用者、依赖方relying party

使用证书中的数据进行决策的用户或代理。

私钥（电子签名制作数据） private key

指在公钥密码系统中，用户的密钥对中只有用户本身才能持有的密钥，是在电子签名过程中使用的，将电子签名和电子签名人可靠地联系起来的字符、编码等数据。

私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相应的公开密钥加密的文件或信息予以解密。

公钥（电子签名验证数据）public key

指在公钥密码系统中，用户的密钥对中可以被其他用户所持有的密钥。

公钥是经由数字运算产生的密钥，用于解密电子签名确认电子签名人的身份及电子签名的真实性。

公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

HLJCA管理员证书

HLJCA管理员证书的组成情况：超级管理员证书、业务管理员证书、业务操作员证书、审计管理员证书、各系统之间的通讯证书、CA根证书等。

高等级电子签名认证证书 enhanced electronic signature certificate

适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。

基础级电子签名认证证书 qualified electronic signature certificate

适用于除高等级证书规定场景外的其他电子签名场景的证书。

2 信息发布与信息管理

HLJCA通过网站公布以下信息：《电子认证业务规则》修订及其他由HLJCA不定时发出的信息。官网网址：www.ca.com.cn 。

本《电子认证业务规则》按照国家电子认证服务管理平台的要求进行备案并发布在HLJCA网站上，供相关方下载、查阅。

HLJCA通过目录服务器发布订户的证书和CRL，订户或依赖方可以通过HLJCA的LDAP服务器获取证书的信息和证书撤销列表。同时，HLJCA提供在线证书状态及依

赖方协议查询服务。（LDAP查询因证书项可能涉及订户个人敏感信息，按照新的个人信息保护相关法律法规，不应公开发布。CA机构有几种处理方法，一是仅对订户和依赖方提供查询入口，二是精确条件查询，三是获得订户明确授权后公开查询。）

OCSP查询：http://218.7.71.19:9090/certauthquery/certcheck.do

LDAP查询：218.7.71.18:10002

链接：https://pan.baidu.com/s/1bPTcJsJy6TrZ4WTvLC2c0w?pwd=pebv 提取码：pebv

HLJCA建立客户投诉受理和处理机制，负责受理订户、依赖方及其他相关方对电子认证服务过程中产生的投诉、意见和建议。对于收到的投诉事项，HLJCA将按照内部管理制度进行调查、核实和处理，并及时向投诉人反馈处理结果。投诉人可通过电话、电子邮件、书面函件或现场方式向HLJCA的内部监督部门、综合管理部提出投诉。

《电子认证业务规则》一经发布，即时生效。对数字证书的订户及证书申请人均具备约束力。对具体个人不另行通知。

证书的发布：在证书签发时，HLJCA通过LDAP自动将该证书公布。

HLJCA的CRL每24小时自动更新，也可通过人工发布最新CRL。

对于公开发布的CPS、证书、CRL等公开信息，HLJCA允许证书使用者自行通过网站和LDAP进行查询和访问。

HLJCA设置了信息访问及控制权限，保证只有经过授权的CA/RA管理员才能查询电子认证服务机构和注册机构数据库中的其他数据。

3 身份标识与鉴别

3.1 身份查验通用要求

证书类别及安全级别越高，身份鉴别要求越严格，身份核验流程及核验内容越全面，以确保机构订户身份信息的真实性、准确性和有效性。在受理证书申请时，HLJCA会对订户和/或受托人进行告知、身份确认、意愿记录和协议签署。HLJCA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）。

3.1.1 订户告知

3.1.1.1 告知内容

订户在申请证书时，HLJCA 将进行内容告知，内容包含：

a）订户有权依法获取、使用、更新和申请撤销其数字证书；同时订户承担向 HLJCA 如实提供真实、完整、有效的身份申请材料，妥善保管证书存储介质及签名私钥的义务。

b）HLJCA 向订户全面明示所有电子认证服务的收费项目与具体收费标准。相关资费标准均严格遵循按照黑龙江省物价主管部门批准的收费标准执行。

c）证书及电子签名仅限用于国家法律法规允许的且本文档规定的特定应用场景与系统环境。证书在载明的有效期内有效，超出有效期、被吊销或冻结的证书将无法正常使用。

d）HLJCA 向订户说明其所采取的系统性信息安全保障措施，以确保证书服务的连续性与数据安全。保障措施涵盖符合国家密码管理要求的物理场所物理安全、高强度的网络边界防护与系统防侵入机制，以及高可用灾备系统和应急响应机制。

e）因 HLJCA 系统故障、管理疏漏或未尽合理审查义务而造成的直接经济损失，由 HLJCA 承担相应赔偿责任；因订户自身未尽妥善保管义务导致私钥泄露或提供虚假材料而引发的所有损失，由订户承担全部法律责任。

f）订户签名私钥生成并存储在符合国家密码管理局检测认证的安全硬件设备（如智能密码钥匙 USB Key、智能卡）或受保护的移动端安全介质中。订户必须设置强口令（PIN 码），严禁私自拷贝或导出私钥。

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。

3.1.1.2 告知方式

在受理高等级证书申请时，HLJCA 将向订户履行订户告知内容的告知程序。该告知方式须采用面对面、电话、视频通话，或经主管部门认可的其他方式告知。HLJCA 在告知过程中，对告知记录进行完整采集与保留。

在受理基础级证书申请时，HLJCA 会强制向订户履行订户告知内容的告知程

序。其告知方式可以采用与高等级证书相同的面对面、电话、视频或主管部门认可的其他方式，或采用强制阅读并主动勾选同意服务协议、短信、邮件等形式实施告知。HLJCA 在告知过程中，对告知记录进行完整采集与保留。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户密钥对的生成严格按照§6.2（订户密钥对的生成和安装）规定的方式进行。证书申请者必须证明持有与所要注册公钥相对应的私钥，通过数字签名的方式确认订户拥有所要注册公钥相对应的签名私钥。

3.2.2 个人身份的查验

对个人订户，HLJCA 根据个人订户所申请证书的类别、用途及安全等级要求，采取相应的身份鉴别措施。一般情况下随着证书安全等级的提升，身份鉴别的严格程度、核验内容及核验流程要求也相应提高，以确保订户身份认证满足相应安全等级要求。

3.2.2.1 个人身份信息有效性的确认

HLJCA 将采取适当方式对个人身份信息进行确认，具体的方式及内容包含：

a）在受理个人证书申请时，HLJCA 将要求订户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）HLJCA 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，并必须按照本条 b）款规定的机读工具、权威数据库比对等方式，对受托人以及委托人两者的身份证件及身份资料分别进行真实性和有效性查验，确保委托授权关系真实成立。

3.2.2.2 个人高等级证书的实人查验

对于个人高等级证书，HLJCA 将采取适当方式对订户身份信息进行确认，并对确认过程进行记录和保存。

订户身份信息查验采用以下方式之一：

a）现场面对面查验对订户的身份信息进行确认。

b）远程人工面对面查验对订户的身份信息进行确认。

c）生物特征验证（如活体人脸识别、指纹、声纹、掌纹等生物识别技术）对订户的身份信息进行确认。

d）主管部门认可的其他身份鉴别方式对订户的身份信息进行确认。

HLJCA 将完整保存可追溯的身份查验过程和结果的相关证明材料，并为每张数字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

对于个人基础级证书，HLJCA 将采取适当方式对订户身份信息进行确认，并对确认过程进行记录和保存。

订户身份信息查验采用以下方式之一：

a) HLJCA 将采用§3.2.2.2 对订户的身份信息进行确认。

b）电信运营商三要素核验方式，对申请者姓名、有效身份证件号码及手机号码在电信运营商登记信息中的一致性进行验证，并通过对应手机号码接收随机短信验证码进行确认；

c）银行卡四要素核验方式，对申请者姓名、有效身份证件号码、银行卡号及银行预留手机号码在银行登记信息中的一致性进行验证，并通过银行预留手机号码接收随机短信验证码进行确认；

d）主管部门认可的其他身份鉴别方式，包括但不限于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，以及银行、支付机构等依法提供的个人账户与身份信息对应关系验证服务等。

HLJCA 将完整保存可追溯的身份查验过程和结果的相关证明材料，并为每张数字证书建立独立的身份验证记录

3.2.3 机构身份的查验

对组织机构订户，HLJCA根据机构订户申请证书的类别及相应安全等级要求，采取相应的身份鉴别措施。一般情况下，证书类别及安全级别越高，身份鉴别要求越严格，身份核验流程及核验内容越全面，以确保机构订户身份信息的真实性、准确性和有效性。

3.2.3.1 机构身份信息有效性的确认

HLJCA 对在受理机构证书申请时身份信息查验的方式及内容包含：

a）机构有效证件的查验方式及证件类型要求：HLJCA 在受理机构证书申请时，可接受的有效证件类型仅限于法律法规和国家有关文件规定的证件，包括在有效期内的统一社会信用代码证、营业执照、事业单位法人证书或社会团体法人登记证书等法定身份证件。HLJCA 通过法定权威数据库进行在线比对，对机构登记状态及证件信息的真实性和有效性进行严格查验。

b）法定代表人或受托人的身份及授权查验方式：代表机构办理证书申请的人员必须通过严格的身份和授权核验。若由法定代表人亲自办理或由受托人代办，相关人员身份证件信息的真实性与有效性查验方式均参见本§3.2.2.1 的规定；当由受托人代为办理时，受托人除需提供其个人有效身份证件外，还必须提交加盖机构公章的有效书面授权证明，HLJCA 对授权书、公章及授权范围进行查验。

3.2.3.2 机构高等级证书的实人查验

对于机构高等级证书，HLJCA 将采取适当方式对订户身份信息进行确认，并对确认过程进行记录和保存。

订户身份信息查验采用以下方式之一：

a）由机构法定代表人申请办理机构高等级证书时，HLJCA 通过§3.2.2.2 的方式对机构法定代表人的身份信息进行确认。

b）由受托人代理申请办理机构高等级证书时，HLJCA 通过§3.2.2.2 的方式对机构受托人的身份信息进行确认，并通过机构对公账户随机金额打款验证或主管部门认可的其他方式，确保受托人得到申请机构的授权。

HLJCA 将完整保存可追溯的身份查验过程和结果的相关证明材料，并为每张数字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

对于机构基础级证书，HLJCA 将采取适当方式对订户身份信息进行确认，并对确认过程进行记录和保存。

订户身份信息查验采用以下方式之一：

a）由机构法定代表人申请办理机构基础级证书时，HLJCA 通过§3.2.2.3 的方式对机构法定代表人的身份信息进行确认。

b）由受托人代理申请办理机构基础级证书时，HLJCA 通过§3.2.2.3 的方式对机构受托人的身份信息进行确认。

HLJCA 将完整保存可追溯的身份查验过程和结果的相关证明材料，并为每张数字证书建立独立的身份验证记录。

3.3 订户意愿记录

3.3.1 订户意愿记录内容

HLJCA 将对订户申请数字证书过程中的真实意愿进行确认，并对相关确认过程和结果进行记录和保存。订户意愿记录内容包括但不限于：

a）订户身份信息，包括订户姓名、有效身份证件号码、联系方式及其他相关身份信息；

b）HLJCA 及相关注册机构信息；

c）签名私钥的保存方式、保存主体及其相应安全保护义务；

d）订户对数字证书及电子签名使用所承担的法律责任和义务；

e）订户已充分知晓并同意本 CPS、订户协议及上述相关内容的明确意愿表示；

f）订户申请数字证书的时间、方式及相关确认记录；

g）其他与订户意愿确认相关的信息。

HLJCA 将完整记录并妥善保存订户意愿确认过程及相关资料，确保相关记录具有真实性、完整性、可审计性和可追溯性。

3.3.2 个人高等级证书的意愿记录

对于个人高等级证书，HLJCA 将采取适当方式对订户真实意愿进行确认，并对确认过程进行记录和保存。订户意愿确认采用以下方式之一：

a）现场办理时，通过面对面确认、手抄提示语或其他合理方式确认订户意愿，并通过录音录像或主管部门认可的其他方式对确认过程进行记录；

b）远程办理时，通过音频、视频、实时视频交互或主管部门认可的其他方式，对订户意愿进行确认和记录。

HLJCA 将完整保存订户意愿确认过程中的音视频资料、确认记录、日志信息及相关证明材料，并为每张数字证书建立独立的意愿确认记录。

3.3.3 个人基础级证书的意愿记录

HLJCA 将采取适当方式确认个人基础级证书申请人的真实申请意愿，并对相关确认过程进行记录。订户意愿确认采用以下方式之一：

a）个人基础级证书的意愿确认采用同§3.3.2 相同的方式对个人意愿进行确认。

b）个人基础级证书的意愿采用协议强制阅读确认、短信验证码确认、电子邮件确认等方式。

HLJCA 会对订户意愿确认过程、确认结果及相关操作信息进行记录和保存，确保相关记录完整、真实并具备可追溯性。

3.3.4 机构高等级证书的意愿记录

HLJCA 将对机构高等级证书申请过程中的真实申请意愿进行确认。订户意愿确认采用以下方式之一：

a）由机构法定代表人申请的，通过§3.3.2 的方式确认机构法定代表人的意愿；

b）由授权代理人办理的，提交加盖机构有效公章的授权文件，并通过§3.3.2 对代理人的申请意愿进行确认。

HLJCA 对机构高等级证书申请过程中的身份核验、授权关系、意愿确认及相关操作过程进行记录，并采用录音录像或主管部门认可的其他方式保存相关记录。

3.3.5 机构基础级证书的意愿记录

HLJCA 将对机构基础级证书申请人的真实申请意愿进行确认。订户意愿确认采用以下方式之一：

a）由机构法定代表人申请的，通过§3.3.3 的方式确认机构法定代表人的意愿；

b）由授权代理人办理的，提交加盖机构有效公章的授权文件，并通过§3.3.3 对代理人的申请意愿进行确认。

HLJCA 对机构基础级证书申请过程中的授权材料、确认记录及相关操作信息进行保存，确保相关记录完整、真实并可追溯。

3.4 订户协议

详见§3.1.1.1 中规定的内容。

3.5 未验证的订户信息

HLJCA 对拟写入数字证书的所有订户信息实施严格的审核机制，具体查验方法与流程参照§3.2。证书中的信息必须经过验证，未经验证的信息不得写入证书。

3.6 互操作要求

对于非 HLJCA 的其他机构，如果双方之间有协议，那么 HLJCA 将依据协议的内容，接收该机构鉴别过的信息，并为之签发相应的证书。如果双方没有任何类似的协议，HLJCA 要求该机构要严格按照本《电子认证业务规则》的规定鉴别身份信息。HLJCA 会根据情况决定是否接受这些被鉴定审核过的材料，并作出是否接受受理的决定。

如果国家法律法规对此有规定，HLJCA 将严格予以执行。

3.7 命名

3.7.1 名称类型

每个订户对应一个甄别名（Distinguished Name，简称DN），DN包含于每张证书的主题中，唯一标识证书用户的身份。

数字证书中的主体的X.500DN应是C=CN命名空间下的X.500目录唯一名字。

3.7.2 对名称意义化的要求

订户的甄别名必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中绑定的实体信息。

3.7.3 订户的匿名或伪名

在HLJCA证书服务体系中，不允许订户（证书申请人）使用匿名或伪名。

3.7.4 理解不同名称形式的规则

DN的具体内容由以下部分组成：

C，国家

S，省份

L，城市

O，订户所在机构信息

OU，订户所在机构部门信息

CN，订户名称

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）；

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。

3.7.5 名称的唯一性

在HLJCA证书服务体系中，证书主体名称必须是唯一的。

3.7.6 商标的识别、鉴别和角色

本《电子认证业务规则》受到完全的版权保护，本文件中涉及的“HLJCA”及其图标等是由黑龙江省数字证书认证有限公司独立持有的专有商标。其他参与者的商标为其拥有方所有。

HLJCA签发的证书主体甄别名中将不包含商标名。

4 证书生命周期操作要求

HLJCA 提供数字证书授权、申请、发放、变更、查询和管理等服务，提供网络信息安全及身份认证、电子签名、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的要求。

4.1 通用要求

证书申请人按照本《电子认证业务规则》所规定的要求，填写《数字证书申请表》，并准备相关的身份证明材料。HLJCA 依据身份鉴别规范对证书申请人的身份进行审核，并决定是否受理申请。申请过程中各方责任为：订户按要求准备并如实填写证书申请材料，HLJCA 负责接收证书申请人的请求材料，对订户所提供的证书申请信息与身份证明资料的一致性进行审核。

a）HLJCA 负责建立、运营和维护证书注册通道，确保申请受理、身份鉴别、申请信息传输及相关业务处理过程安全、可靠和有效运行。

b）HLJCA 按照相关规定与订户签订电子认证服务协议，明确双方权利、义务及责任。

c）订户需要提供§3.2 初始身份确认所述的有效身份证明材料，并确保材

料真实准确。配合 HLJCA 或授权注册机构完成对身份信息的采集、记录和审核。HLJCA 须按§3.2 初始身份确认的要求和流程对申请人身份材料信息进行审查。如证书申请人未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 HLJCA 或电子签名依赖方造成损失的，由证书申请人承担赔偿责任。

d）HLJCA 参照§3.2 初始身份确认的要求对订户的身份信息进行采集、记录，审核。通过查验后，HLJCA 向订户签发证书。HLJCA 负责对证书申请信息、身份鉴别记录、审核记录及其他相关业务资料进行记录、保存和管理，并按照相关规定妥善保存相关信息。

4.2 证书申请

4.2.1 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。

4.2.2 执行识别与鉴别功能

HLJCA 按照本《电子认证业务规则》所规定的身份鉴别流程对证书申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2.3 组织机构身份的鉴别、§3.2.2 个人身份的鉴别。

4.2.3 证书申请批准和拒绝

HLJCA 根据本《电子认证业务规则》所规定的流程对证书申请人进行协议告知、身份确认、意愿记录、协议签署等动作，根据既定准则决定批准或拒绝证书申请。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴别结果为合格，HLJCA 将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴别，HLJCA 将拒绝申请人的证书申请，并通知申

请人，同时向申请人提供失败的原因（法律禁止的除外）。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.4 处理证书申请的时间

HLJCA 在对订户进行身份鉴别后，并根据数字证书的受理及制作流程开展工作。HLJCA 在处理证书申请材料时，由双人控制，即录入人员对订户信息进行录入操作，审核人员对所录入信息正确性进行确认（录入人员与审核人员不兼任），最后制证人员完成证书的写入工作。

HLJCA 在处理证书申请时通常情况下将在受理之日起三个工作日内完成，因特殊情况确需超时的，HLJCA 将与订户协商确定处理时限。

4.2.5 处理证书申请提交人的核查

HLJCA 对申请提交人的授权文件进行核查，只有通过审查才能受理数字证书申请材料，审核内容一般包括以下内容：

数字证书申请表；

营业执照原件及复印件；

法人及经办人身份证原件及复印件；

申请材料的复印件均需加盖单位公章；

申请人签字。

4.3 证书签发

4.3.1 证书所含信息的审核验证及获得证书的方式

数字证书中至少包括以下内容：

电子认证服务提供者名称；

证书持有人姓名；

证书序列号；

证书有效期；

证书持有人的电子签名验证数据；

电子认证服务提供者提供的电子签名。

制作数字证书及证书中所包含的信息都经过了审核，只有审核通过的用户才能制作数字证书。在订户提供证书制作资料并通过身份真实性确认后一般在 3 个工作日内可以接受数字证书。

4.3.2 证书签发中电子认证服务机构的行为

HLJCA 批准证书申请后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

通常，HLJCA 所签发的证书在 24 小时后生效（与 CRL 列表发布时间一致）。

4.3.3 电子认证服务机构对订户的通告

电子认证服务机构，对订户的通告有以下几种方式：

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

数字证书签发完成后，HLJCA 将数字证书当面或者寄送给证书申请者，证书申请者从获得数字证书起，就被视为同意接收证书。

如订户在接受证书后发现证书信息存在错误、申请信息与实际情况不符或存在其他异常情况，应及时向 HLJCA 提出拒绝接受申请。

HLJCA 根据相关流程对证书进行处理。HLJCA 对订户证书接受过程相关信息进行记录和保存，包括但不限于证书接受时间、方式、操作人员、确认记录及其他相关操作信息，并按照相关规定妥善保存。

4.5 密钥对和证书的使用

在将密钥对交付订户保管之前，HLJCA 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）HLJCA 将拒绝颁发证书。

HLJCA 不提供订户签名私钥管理服务，订户只能在指定的应用范围内使用私钥和证书，订户只有在接收了相关证书之后才能使用对应的私钥，并且在证书到期或被吊销之后，订户必须停止使用该证书对应的私钥。

HLJCA 建立了便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书盗用等异常情况。

4.6 证书续期

证书续期是指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。证书中有明确的证书有效期，表明该证书的起始日期与截止日期。订户应当在证书有效期到期前，到 HLJCA 申请更新证书。

证书续期的具体情形如下：

a）证书的有效期将要到期；

b）密钥对的使用期将要到期；

当申请人为订户或其受托人处理续期请求时的身份查验方式：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，按照§3.2 的规定重新进行身份查验；证书签发与接受的流程符合§4.3 与§4.4 的规定。

4.7 证书密钥更新

证书密钥更新指为订户生成新的密钥对并为其新公钥签发新证书。证书密钥更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户

甄别名、证书序列号、原证书对应的私钥对证书密钥更新请求签名等，并上送新的公钥申请签发新证书。

证书密钥更新的具体情形如下：

a）证书的有效期将要到期，证书更新；

b）因私钥泄漏而撤销证书；

c）其他。

当申请人为订户或其受托人处理密钥更新请求时的身份查验方式：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，否则按照§3.2 的规定重新进行身份查验；证书签发与接受的流程符合§4.3 与§4.4 的规定。

4.8 证书变更

证书变更指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。

当订户实体身份信息发生改变（如订户更名等），订户需向 HLJCA 报告并申请证书变更，HLJCA 将原证书吊销后重新签发新证书。当申请人为订户或其受托人处理证书变更时，HLJCA 按照§3.2 的规定进行查验，若发起方不是证书订户，HLJCA 会采用必要方式取得订户同意；证书签发与接受的流程符合§4.3 与§4.4 的规定。

4.9 证书撤销和冻结

HLJCA 提供热线电话等便捷渠道接受不同的情况，订户、受托人及依赖方或 CA 机构的申请。过程中会记录影响证书或私钥安全的事件（如密钥遗失、泄露）等。办理业务时会按要求验证申请人的身份与权限，并做出是否受理的决定。

4.9.1 证书撤销的情形

发生下列情形之一的，订户应当申请撤销数字证书：

1）数字证书私钥泄露；

2）数字证书中的信息发生重大变更；

3）认为本人不能实际履行数字证书认证业务规则。

发生下列情形之一的，HLJCA 可以吊销其签发的数字证书：

1）订户申请撤销数字证书；

2）订户提供的信息不真实；

3）订户没有履行双方合同规定的义务；

4）数字证书的安全性得不到保证；

5）法律、行政法规规定的其他情形。

4.9.2 撤销请求的流程

证书撤销请求的处理采用与原始证书签发相同的过程。

订户到 HLJCA 书面填写《证书吊销申请表》，并注明撤销原因；HLJCA 根据要求对订户提交的撤销请求，身份信息以及权限进行审核；HLJCA 撤销订户证书后，将当面通知订户证书被撤销，订户证书在 24 小时内进入 CRL，向外界公布。

强制撤销是指 HLJCA 确认用户违反本《电子认证业务规则》的情况发生时，对订户证书进行强制撤销，撤销后将立即通知该订户。

HLJCA 将完整保存处理过程的相关材料。

4.9.3 证书冻结的情形

证书用户暂停使用证书。

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。

4.9.4 请求证书冻结的实体

由 HLJCA 颁发的证书有效期限未到的个人、机构等各种实体，以及其他凡是持有 HLJCA 各类证书而有效期限未到的证书持有者。

4.9.5 冻结请求的流程

订户到 HLJCA 书面填写《证书冻结申请表》，并注明冻结原因；HLJCA 根据 3.2 节的要求对订户提交的证书冻结请求进行审核，审核通过后对证书进行冻结操作。HLJCA 可以依法对订户证书进行强制冻结，冻结后将立即通知该订户。保存期限届满后，相关数据将按照信息安全管理制度进行销毁；法律法规另有规定的，从其规定。因业务承接或监管要求需要转移相关数据的，HLJCA 将在确保数据安全和合法合规的前提下实施转移。停止服务不影响停止服务前已经产生的权利义务和法律责任。订户、依赖方及 HLJCA 在停止服务前依据证书产生的责任，仍按照相关法律法规、协议约定及本 CPS 规定执行。HLJCA 对停止服务申请受理、审核、证书处理、密钥销毁、数据保存或转移等全过程进行记录，并确保相关记录真实、完整、可追溯。

证书被冻结后，订户必须在证书有效期前恢复证书。HLJCA 将通过电话提醒订户，若证书到期订户还没有提交恢复申请，HLJCA 有权自行撤销证书。对此造成的任何后果，HLJCA 不负任何责任。

HLJCA 将完整保存处理过程的相关材料。

4.10 证书状态信息服务

4.10.1 操作特征

HLJCA 通过 CRL、LDAP、OCSP 为用户提供证书状态服务，上述方式的证书状态服务应该对查询请求有合理的响应时间和并发处理能力。

4.10.2 服务可用性

HLJCA 提供 7×24 小时的证书状态查询服务，查询服务为连续不间断服务，服务可用率不低于 99%。即在网络允许的情况下，订户能够实时获得证书状态查询服务。且响应时间不超过 10 秒。HLJCA 提供备用查询机制进行查询。

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。（提供付费服务）。

4.11 停止使用认证服务

当订户发生以下情形之一时，将停止使用全部或部分认证服务：

a）订户主动申请停止使用认证服务；

b）订户不再需要使用电子认证服务，或者相关业务已经终止；

c）订户的身份信息、主体资格或注册信息发生变化，导致原认证信息不再真实、准确或完整；

d）订户的签名私钥发生泄露、丢失、被盗用或存在其他安全风险；

e）订户发现或有合理理由怀疑签名私钥可能已被未经授权的人员使用；

f）订户发生注销、解散、破产、死亡或其他导致其主体资格终止的情形；

g）订户违反电子认证服务协议、认证业务规则或相关法律法规，认证机构要求其停止使用认证服务；

h）订户使用证书或认证服务从事违法违规活动，或者存在危害认证服务安全的行为；

i）认证机构依法或依据相关认证业务规则要求订户停止使用认证服务的其他情形。

对于由订户持有和控制的签名私钥，订户应立即停止使用并按照相关安全要求进行销毁；对于由 HLJCA 或其授权机构管理的密钥材料，需按照密钥管理制度进行安全销毁，并保留相应记录。

停止服务后，HLJCA 将按照法律法规、监管要求及本 CPS 规定保存相关业务数据、日志记录和身份验证资料。保存期限届满后，相关数据将按照信息安全管理制度进行销毁；法律法规另有规定的，从其规定。因业务承接或监管要求需要转移相关数据的，HLJCA 将在确保数据安全和合法合规的前提下实施转移。

停止服务不影响停止服务前已经产生的权利义务和法律责任。订户、依赖方及 HLJCA 在停止服务前依据证书产生的责任，仍按照相关法律法规、协议约定及本 CPS 规定执行。

HLJCA 对停止服务申请受理、审核、证书处理、密钥销毁、数据保存或转移等全过程进行记录，并确保相关记录真实、完整、可追溯。

4.12 密钥托管与恢复

4.12.1 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

a）证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

b）在证书有效期内，证书被撤销后，即订购结束。

4.12.2 密钥生成、备份与恢复的策略和行为

订户的签名密钥对由订户的密码设备（如智能 USB KEY）生成，加密密钥对由密钥管理中心生成。

签名密钥对由订户的密码设备保管。

密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为三类：订户密钥恢复、司法取证密钥恢复和根证书密钥恢复。

a）订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在 HLJCA 申请，经审核后，通过 HLJCA 向 KMC 请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

b）司法取证密钥恢复：司法取证人员在 KMC 申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

c）根证书密钥恢复：HLJCA 根证书私钥由 HLJCA 自行管理，不委托任何第三方机构或个人进行托管、保管或控制。根证书私钥存放于经国家密码主管部门认可的密码设备中，并在 HLJCA 控制的安全环境下使用和管理。HLJCA 建立根证书密钥备份与恢复机制，对根证书私钥进行安全备份。根证书私钥备份采用安全的密码技术和管理措施进行保护，并保存在具备相应物理安全和访问控制措施的

安全场所。根证书私钥的备份、恢复和使用操作须按照密钥管理制度执行，由经授权的可信人员共同完成，并保留完整的操作记录和审计日志，确保操作过程可追溯。仅在密码设备故障、灾难恢复、业务连续性保障等经授权批准的特殊情况下，方可启动根证书私钥恢复程序。恢复过程遵循密钥管理制度要求，在安全受控环境中实施，并采取必要措施保障根证书私钥的机密性、完整性和可用性。

4.12.3 会话密钥的封装与恢复的策略和行为

非对称算法组成数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

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

HLJCA 中心机房坐落于哈尔滨市道外区，为独立单体建筑，建筑本体配套防震、防火、防水、防雷等全项安防防护设施；机房院区仅设置单一出入口及通行道路。机房依据业务功能划分为核心区、服务区、管理区、公共区四大功能分区。机房实行分级准入管控，仅限经审批授权人员进入对应权限区域，所有区域通行统一执行双人核验准入制度。

HLJCA 的建筑物和机房建设按照下列标准实施：

1. GM/T 0034-2014：《基于 SM2 密码算法证书认证系统密码及其相关安全技术规范》；

2. GB50174－93：《电子计算机机房设计规范》；

3. GB2887-89：《计算机站场地技术条件》；

4. GB/T-2887-2000：《电子计算机场地通用规范》；

5. GB6650-86：《计算机机房用活动地板技术条件》；

6. SJ/T30003—93：《电子计算机机房施工及验收规范》；

7. GB9361-88：《计算站场地安全要求》；

8.GBJ114-88：《采暖通风与空气调节规范》。

5.1.1.1 公共区

公共区包括入口、大堂、保安室，部署各配套设施和监控设备。

5.1.1.2 管理区

管理区安装签发、审计控制台，网络管理、监控控制台，是 RA 和 CA 管理员、审计员和网络安全员的工作区，只允许管理区规定的管理人员进入，需要两个管理员同时使用双因素身份认证才可以进入。

5.1.1.3 服务区

服务区主要安装 RA 管理控制台、LDAP 服务器、OCSP 服务器、RA 注册服务器等设备；只允许服务区规定的管理人员进入。

5.1.1.4 核心区

核心区为屏蔽区，加装高强度的钢制防盗门，主要安装 CA 应用服务器、CA 数据库服务器、防火墙、数据备份服务器等核心设备，只允许核心区规定的管理人员进入，而且需要两个管理员同时使用双因素身份认证才可以进入。密码柜也安放在核心区，存放保密资料。

5.1.2 物理访问

为了保证本系统的安全，采取了一定的隔离、控制手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

1.门禁系统：控制各层门的进出，工作人员需使用身份识别卡和指纹识别才能进出，进出每一道门都有时间记录。

2.报警系统：任何非法闯入、非正常手段的开门以及长时间不关门，都会触发报警系统。

3.监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对

安全区域和操作区域进行 7×24 小时不间断录像。所有录像资料至少保留 6 个月，以备查询。

5.1.3 电力与空调

机房供电系统包括整个机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备专用配电柜和辅助设备配电柜独立设置，分开计算机设备电源与动力线。

使用 UPS 不间断电源，最大限度满足机房计算机设备对供电电源质量的要求。市电电源供电与备用发电机供电在机房配电室进行切换，再经过 UPS 不间断电源对计算机设备供电。

按《电子计算机机房设计规范》（GB50174-93）规定和功能需要，采用机房精密空调，保持机房在恒温 22±3℃、恒湿 45%±5%RH 的状态下运行。

5.1.4 水患防治

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

根据国家有关消防规范，对 HLJCA 机房区域采用火灾自动报警系统及气体灭火进行保护，同时配备消防自救呼吸器。

5.1.6 介质存储

介质必须指定专人管理，并存储在专用的介质柜中，保证物理安全，注意防磁、防静电干扰、防火、防水。并采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。制定存储介质全生命周期管理制度，明确介质使用权限、领用和归还要求、报废标准、销毁方式及审批流程，并对介质领用、使用、归还、转移、报废和销毁等全过程进行记录和管理，确保相关操作可审计、可追溯。

5.1.7 废物处理

当 HLJCA 存档的敏感数据或密钥已不再需要或存档的期限已满时，会将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

HLJCA 对关键系统数据、审计日志数据和其他敏感信息进行异地备份，异地备份地点为牡丹江市，距离本部机房直线距离约三百公里以上，遇到灾难情况发生时保证数据安全。

5.1.9 设备台账

HLJCA 建立设备全生命周期管理制度，对认证服务相关设备进行统一管理，并建立完整、准确的设备台账。设备台账应记录设备名称、型号、编号、安装位置、责任人、投入使用时间、使用状态、维护周期、维护记录、报废标准及报废情况等信息，确保设备信息可查询、可追溯。

HLJCA 明确设备管理责任人，负责设备的日常使用、运行维护、安全管理和状态监测。设备发生配置变更、维修、更换、停用或报废时，应及时更新设备台账信息。HLJCA 按照内部管理制度定期开展设备巡检、维护保养和安全检查，并依据设备维护周期实施预防性维护，确保设备持续满足电子认证服务运行要求。

HLJCA 定期组织设备盘点和核对工作，对设备实际情况与设备台账进行一致性检查，确保账实相符。发现设备遗失、损坏、状态异常或台账信息不一致的，应及时调查处理并形成记录。对于达到报废条件或无法继续满足安全运行要求的设备，HLJCA 按照设备报废管理流程进行审批、登记和处置。涉及敏感数据、密钥信息或认证业务数据的设备，在报废、转移或销毁前，按照相关安全管理制度进行数据清除或安全销毁，并保留完整记录。

5.2 操作过程控制

5.2.1 可信角色

HLJCA、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：

a）系统管理员：负责系统策略配置、用户与权限管理等；

b）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；

c）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；

d）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；

e）密钥管理员：负责根证书密钥材料管理、根证书密钥生存周期管理等；

f）业务操作员：负责证书申请的受理、审核，订户的身份与意愿鉴证；

g）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；

h）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审计等；

i）其他人员：对公司运营有重要影响的其他管理人员。

5.2.2 每个角色的识别与鉴别

按照所担任角色的不同，分别进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。HLJCA 将独立完整地记录其所有的操作行为。

5.2.3 职责分离

为保证系统安全，遵循可信角色分离的原则，即 HLJCA 的可信角色由不同的人担任。

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，来进行任何密钥恢复的操作。

5.3 人员控制

5.3.1 可信人员资格要求

HLJCA 工作人员必须与公司签订劳动合同并无同行业重大错误记录、无违法犯罪记录，经过保密教育，签订保密协议后，方能取得可信人员的资质。

5.3.2 背景审查程序

所有目前的可信人员和申请调入的可信人员都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

a）人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

b）人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进行鉴定。

c）用人部门通过现场考核、日常观察、情景考验等方式对其考察。

d）经考核，人事部门和用人部门联合填写《可信人员调查表》，报主管领导批准后准予上岗。

5.3.3 可信人员培训要求

HLJCA 对运营人员按照其岗位和角色安排不同的培训。培训有：系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 HLJCA 组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人

员进行培训并考核。

HLJCA 根据可信角色的职位需求，给予相应大于 20 学时岗前培训，综合培训内容如下：HLJCA 运营体系；HLJCA 技术体系；HLJCA 安全管理策略和机制；岗位职责统一要求；PKI 基础知识；身份验证和审核策略和程序；灾难恢复和业务连续性管理；CP、CPS 政策及相关标准和程序；HLJCA 管理政策、制度及办法等；电子认证服务运营体系构成；电子认证服务技术体系构成；国家关于电子认证服务的法律法规及标准、程序；其他需要进行的培训等。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 HLJCA 组织的大于 20 学时培训一次。

认证策略调整、系统更新时，HLJCA 将对全体人员进行再培训，以适应新的变化。

5.3.5 工作轮换周期和顺序

对于可替换角色，HLJCA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

5.3.6 对未授权行为的处罚

当 HLJCA 员工被怀疑，或者已进行了未授权的操作，例如滥用权力或超出权限使用 HLJCA 系统或进行越权操作，HLJCA 得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

对不属于 HLJCA 内部的工作人员，但从事 HLJCA 有关业务的人员等独立签约者（如注册机构的工作人员），HLJCA 的统一要求如下：

a）对人员档案进行备案管理；

b）具有相关业务的工作经验；

c）必须接受 HLJCA 组织的为期一周的岗前培训。

5.3.8 提供给员工的文档

为使得系统正常运行，HLJCA 提供给具有权限的相关人员所需文档。

5.4 审计日志程序

5.4.1 记录事件的类型

HLJCA 记录所有与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的类型、事件的内容、事件的作用对象、事件的结果和事件相关的实体等。HLJCA 还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。关键操作由操作人员 UKey 操作签名完成。

这些事件包括但不限于：

1. 密钥生命周期内的管理事件，包括密钥生成、备份、存储、恢复、使用、撤销、归档、销毁、私钥泄露等；

2. 证书生命周期内的管理事件，包括证书的申请、批准、更新、撤销等；

3. 系统、网络安全事件，包括：成功或失败的访问 CA 系统的活动，系统日常运行产生的日志文件，系统变更等；

4. 信息安全设备记录的安全事件：路由器和防火墙活动的日志记录至少包括以下内容：1）记录所有成功和失败的路由器及防火墙登录尝试；2）记录所有在路由器和防火墙上执行的管理操作，包括配置更改、固件更新以及访问控制修改；3）记录所有防火墙规则的更改，包括新增、修改和删除；4）记录所有系统事件和错误，包括硬件故障、软件崩溃以及系统重启；

5. 系统操作事件，包括系统权限的创建、删除，设置或修改密码；

6. CA 设施的访问，包括授权人员进出 CA 设施、非授权人员进出 CA 设施等相关记录；

7. 可信人员管理记录，包括系统权限的创建、删除及变更等。

5.4.2 处理日志的周期

HLJCA 每季度对发证系统进行日志分析。所有的审计日志定期由专人进行检查和审阅，以便发现重要的安全和操作事件，及时采取相应的措施进行处理并对审查日志的行为进行备案。

5.4.3 审计日志的保存期限

HLJCA 审计日志至少保存证书失效后五年。

5.4.4 审计日志的保护

HLJCA 执行严格的管理，确保只有 HLJCA 授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志要进行异地备份。审计日志的制作和访问进行岗位分离。

5.4.5 审计日志备份程序

HLJCA 所有的审查日志都进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，采用在线和离线两种方式的备份工具。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

证书签发管理系统；

证书注册管理系统；

密钥管理系统；

证书目录系统；

其他需要审计的系统。

5.4.7 对导致事件实体的通告

HLJCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

HLJCA 有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

HLJCA 每年对系统进行漏洞扫描和渗透测试等脆弱性评估，并根据日志的日常审计和监督实施，随时调整和系统运行密切相关的安全控制措施，以降低系统运行的风险。

5.4.9 审计事件

HLJCA 系统具有完善的日志审计系统，记录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。只有 HLJCA 授权的人员才能接近这些审查记录。审计日志处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。HLJCA 对以下事件进行了审计：

1）电子认证服务系统的操作事件

审计日志记载了以下内容：系统操作事件的日期、内容、发生的时间及事件相关的实体信息。

2）证书生命周期事件

详细记录了证书生命周期的申请、签发、更新、变更、吊销、挂起等操作。

3）可信人员的操作事件

审计日志记载了可信人员在证书整个生命周期内的操作记录。

4）不符合规定的事件

HLJCA 审计人员对不符合规定的事件操作进行了及时处理。

5）HLJCA 审计记录至少保存证书失效后五年。

6）HLJCA 制定了确保审计日志不被未授权询问、复制、修改和删除的制度，

对审计日志进行了严格的通道管理，确保只有 HLJCA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。

7）HLJCA 保证所有的审查记录和审查总结都按照 HLJCA 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。

5.5 记录归档

5.5.1 归档记录的类型

HLJCA 对以下几类事件进行归档记录，包括但不限于：

1）证书申请材料、身份证明材料、订户意愿记录，以及证书服务申请、批准和拒绝相关记录；

2）与订户签订的协议文件及电子认证服务相关文档；

3）证书及证书撤销列表（CRL）相关记录；

4）所有审计日志及电子认证服务过程中的其他操作记录；

5）证书认证系统运行日志、关键操作日志以及系统安全事件识别、分析和处置记录；

6）证书系统建设、升级、变更及维护相关文档；

7）密码设备全生命周期管理记录，以及密码设备日常操作和使用记录；

8）根证书、CA 密钥及相关密钥生命周期管理的全部记录；

9）各类内部评估、外部审计、合规检查及安全评估相关文档；

10）电子认证服务过程中产生的其他需要保存的重要记录和资料。

5.5.2 归档记录的保存期限

CA 数据库的保存期至少保存证书失效后五年。

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查询。HLJCA 保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在 HLJCA 的存储库，还在异地保存其备份。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。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。HLJCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 归档记录时间要求

所有记录都要在存档时加具体准确时间标识以表明存档时间。系统产生的记录，也要有时间标识。

5.5.6 归档收集系统

档案收集系统由人工操作和自动操作两部分组成。HLJCA 设立专门的档案管理机构，统一负责电子认证服务相关档案和记录的归档管理工作。档案管理机构负责归档资料的接收、整理、分类、保管、查询等工作，并建立相应的档案管理制度和操作规范。档案管理机构应明确各岗位职责和权限，严格控制档案访问范围，确保归档记录的真实性、完整性、准确性。任何单位和个人未经授权不得查阅、复制、修改、删除或销毁归档资料。

档案管理机构采取安全保护措施，保障档案存储环境和档案数据安全，防止档案发生丢失、损毁或未经授权访问等情况。

5.5.7 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，只有被授权的可信人员才能获得

归档信息，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。HLJCA 每年会验证归档信息的完整性。

5.6 电子认证服务机构根密钥更替

电子认证服务机构密钥更替指 HLJCA 根证书到期和电子认证服务机构证书到期时，需要更换密钥对而采取的措施。HLJCA 将在密钥到期前两年完成密钥更替。

在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期。生成和管理 CA 密钥对时，严格遵守密钥规范。及时发布新的 CA 证书。确保整个过渡过程安全、顺利，不出现信任真空期。

HLJCA 根密钥由加密机产生，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 张证书达到密钥更换的目的，使新旧证书之间互相信任。

电子认证服务机构证书到期时，更替办法同根密钥的更替一样。

5.7 损害和灾难恢复

5.7.1 事故和损害处理程序

HLJCA 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，HLJCA 将按照灾难恢复计划实施恢复。为了及时响应和处理事故和损害发生的情况，HLJCA 建立了一系列应急处理预案和事故处理方案。相关岗位的工作人员将按照方案和相关制度的规定，积极实施抢修恢复计划和措施，每年进行一次重大事故应急演练。

5.7.2 计算资源、软件和/或数据被破坏

HLJCA 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，HLJCA 将按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

当 HLJCA 根证书被作废时，HLJCA 通知订户。

当 HLJCA 的私钥被攻破或需要作废时，HLJCA 根据 HLJCA 灾难恢复计划规定的灾难恢复步骤进行操作。

1、当证书库因系统故障、设备损坏、网络攻击、自然灾害或其他突发事件导致数据丢失、损坏或无法正常提供服务时，HLJCA 将按照业务连续性和灾难恢复预案启动证书库恢复程序。首先，HLJCA 根据灾难恢复预案重建安全运行环境，包括恢复服务器、数据库、网络设备、密码设备及相关安全配置，确保恢复后的系统满足电子认证服务安全运行要求。完成运行环境恢复后，HLJCA 利用备份数据恢复证书库信息，并对恢复结果进行完整性、一致性和可用性验证。

对于无法确认状态、存在异常或可能受到影响的证书，HLJCA 将根据实际情况生成受影响证书清单，并依法采取证书撤销、冻结或重新签发等措施。对于订户签名私钥由订户自行持有和管理的，HLJCA 不保存、不恢复订户签名私钥；如因灾难事件导致证书无法继续使用，订户应重新申请证书。对于由密钥管理中心管理的加密密钥，按照密钥管理制度和灾难恢复预案实施恢复操作。对于需要重新签发证书的订户，HLJCA 将通过公告、电话、短信、电子邮件或其他适当方式通知订户，并按照证书申请、身份鉴别和证书签发流程重新向订户提供有效的数字证书。恢复期间的相关操作、处理过程及结果均形成完整记录并归档保存，确保全过程可追溯。

2、当 HLJCA 的根密钥出现损害时，HLJCA 将立即向电子认证服务管理办公室和其他相关主管部门汇报，通过网站或其他方式对订户进行通告，采取必要措施避免订户利益遭受更大损失。立即通知相关依赖方关闭与证书认证服务相关的系统。立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和

依赖方查询。同时 HLJCA 立即生成新的密钥对。HLJCA 新的证书签发后，将及时通过 HLJCA 门户网站或其他方式发布。

5.7.4 灾难后的业务连续性能力

为满足《中华人民共和国电子签名法》和《电子认证服务管理办法》对电子认证服务机构的业务连续性要求，确定并减少因自然灾害等不可抗力以及其他人为因素带来的损失，有效地保障业务的连续性，HLJCA 制定业务连续性计划。主要内容有：故障恢复处理、设备与数据的备份、故障应急处理。

针对证书系统的核心业务系统，证书签发管理系统和证书注册管理系统采用双机热备方式；对核心数据库，采用光盘和备份磁盘阵列的方式来确保证书系统的高可靠性和可用性。对于一般故障，HLJCA 将在 2 小时内解决；对于紧急事件，HLJCA 在 24 小时内解决。

发生自然或其他不可抗力性灾难后，采取的安全措施按照 HLJCA 灾难恢复计划实施。

CA 系统的数据备份是在发生事故时，保证业务可恢复性的关键。HLJCA 系统备份主要包括数据库备份、应用系统备份、加密机备份、设备硬件备份。

根私钥是 HLJCA 的核心数据，一旦被攻破将给 HLJCA 带来巨大损失。所以，HLJCA 制定了应急机制：

1）立即停止使用和发放与根私钥相关的一切证书业务；

2）立即上报有关主管部门；

3）通过各种方式通知证书应用方及依赖方；

4）更换根私钥重新签发证书。

HLJCA 需要定期备份的数据包括：认证系统数据、用户数据、系统配置数据。为保障系统的业务连续性，我们为重要系统配备了备用设备，HLJCA 员工不定期对设备进行检查，发现问题及时处理。

证书数据是以数据库的形式表现出来，所以 HLJCA 对数据库进行了备份。

在电源方面采用一路市电加一路 UPS 电源和备用发电机，UPS 供电能力为 6 小时。

通信线路方面由中国联通公司提供。

5.8 电子认证服务机构的终止

因各种情况，HLJCA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

HLJCA 在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于订户等。在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。HLJCA 将选择具备相应电子认证服务资质的业务承接机构，并与承接机构签署业务承接协议，明确双方在业务承接、运行维护、数据管理、安全保障及责任划分等方面的职责和义务。HLJCA 按照相关规定向业务承接方移交电子认证服务相关资料和关键数据，包括但不限于证书办理资料、证书信息库、证书状态信息、审计日志、系统运行记录、相关密钥资料及其他必要信息，并协调承接机构开展后续运营工作。若 HLJCA 未能就业务承接事项与其他电子认证服务机构达成协议，将依法申请行业主管部门协调其他具备资质的电子认证服务机构承接相关业务。

HLJCA 采用以下措施终止业务：

在电子认证服务暂停或者终止后，HLJCA 会停止证书状态查询服务及其他电子认证相关服务，并按照相关规定对证书数据、日志记录、业务档案及其他相关资料进行整理、归档和封存。

HLJCA 停止相关密码设备运行，并对密码设备、密钥数据及相关安全管理资料进行归档和封存。涉及敏感数据、密钥信息及安全参数的，并按照国家有关规定采取安全处理措施。

HLJCA 将及时撤销或冻结业务管理员、系统管理员及业务操作人员的相关权限，防止未经授权的访问和操作。HLJCA 会对所有档案记录、敏感文档及重要数据进行安全整理、封存和管理，并采取必要措施清除主机系统、密码设备及相关存储介质中的敏感数据，确保数据及密钥信息安全。HLJCA 会根据电子认证服务暂停或者终止的实际情况，采取其他必要的数据安全、密钥安全及系统安全保护措施。

若存在与订户电子认证证书签发、管理相关的外部合作机构，HLJCA 会明确合作机构终止服务时的业务处理流程、通知机制及相关责任要求，并确保相关业务安全、有序完成交接或终止。

行业主管部门对此另有要求的，HLJCA 将严格按照相关要求执行。

5.9 重大事项报告

HLJCA 建立重大事项报告机制，对可能影响电子认证服务连续性、安全性、合规性及用户权益的重大事项进行识别、处置和报告。重大事项发生后，相关部门应立即启动内部报告流程，并按照规定及时向公司管理层、上级机构及行业主管部门报告。

重大事项报告包括但不限于以下内容：

a）事件发生时间、地点及基本情况；

b）事件影响范围、影响对象及严重程度；

c）已采取的应急处置措施及当前处置进展；

d）可能产生的风险及后续影响分析；

e）后续整改方案、恢复计划及防范措施；

f）其他需要说明的重要事项。

HLJCA 根据重大事项性质和影响程度，采取电话、邮件、书面报告或其他有效方式进行报告。对于影响电子认证服务安全运行、订户信息安全或系统连续性的重大事项，应在事件发生后及时逐级上报，并持续跟踪处置进展。

a）重大事项包括但不限于以下情形：

证书认证系统迁移或改造包括系统软件、网络架构、部署环境及证书签发逻辑等重大变更，符合以下任意情形之一的，将纳入重大事项管理：

1）机房迁移，或机房内服务区、管理区、核心区划分范围发生重大变化；

2）电子签名认证证书签发逻辑发生变更；

3）新增远程证书注册子系统；

4）新增、更改或删除用于签发电子签名认证证书的证书链；

5）其他可能对电子认证服务安全、用户资料安全或业务连续性产生影响的重大变更。

包括电子认证服务系统遭受网络攻击、病毒入侵、恶意破坏、数据泄漏或其他安全事件，导致系统无法正常运行或数据安全受到严重威胁的情形。符合以下任意情形之一的，将纳入重大安全事件管理：

1）证书签发服务或证书验证服务连续中断超过 24 小时；

2）根证书密钥、CA 私钥或其他关键密钥数据发生泄露；

3）发生持续性或大范围未经授权的私钥访问行为或其他异常安全活动；

4）系统日志持续或大范围出现异常操作记录，包括但不限于非授权时间、非授权网络地址访问敏感功能等情况；

5）其他严重影响电子认证服务安全运行的事件。

b)订户信息泄露事件

包括订户身份信息、证书申请资料、业务数据等敏感信息泄露、丢失或损毁等情形。符合以下任意情形之一的，将纳入重大信息安全事件管理：

1）个人信息泄露影响范围较大，并造成经济损失、社会影响或客户投诉；

2）数据丢失导致证书状态信息无法恢复；

3）其他对订户合法权益造成重大影响的信息安全事件。

c)合规性事件

包括违反法律法规、行业标准、监管要求或合同约定等情形。符合以下任意情形之一的，将纳入重大合规事件管理：

1）涉及电子认证服务的司法判决、仲裁或其他法律程序；

2）收到行业主管部门、监管机构或行政机关出具的违规通知、整改通知或行政处罚决定；

3）其他可能对 HLJCA 合规运营造成重大影响的事件。

d)人力资源类事件

包括核心岗位人员异常流动、大规模劳动纠纷或重大职场安全事件等。符合以下任意情形之一的，将纳入重大人力资源事件管理：

1）一个月内涉及 2 名及以上管理层人员或 10%以上可信岗位人员离职；

2）劳动纠纷参与人数超过员工总数 10%，且经法院、仲裁机构等生效裁决确认由 HLJCA 承担法律责任；

3）其他可能影响电子认证服务正常运行或安全管理的人力资源事件。

HLJCA 会对重大事项处置全过程进行记录和归档，并保存相关报告、日志、处置记录及整改材料，以满足审计、监管和追溯要求。

6 认证系统技术安全控制

6.1 技术安全管理制度要求

HLJCA 建立并实施覆盖电子认证服务全过程的技术安全管理制度，对密钥管理、密码设备管理、系统开发与维护、变更管理、漏洞管理、网络安全防护、主机与终端安全、恶意代码防范、数据安全保护、备份与恢复、日志审计以及业务连续性管理等方面制定相应的管理规范和操作流程，并在日常运营过程中严格执行。

HLJCA 按照国家有关法律法规、密码管理规定、行业标准以及内部安全管理要求，持续完善技术安全管理制度，确保电子认证服务系统安全、稳定、可靠运行。设立安全策略委员会，负责技术安全管理制度的审议、监督和持续改进。安全策略委员会每年至少组织一次对技术安全管理制度及其执行情况的评审，并根据法律法规、技术发展、业务变化、安全风险及审计评估结果，对相关制度进行修订和完善。评审过程及结果形成记录并归档保存。

6.2 密钥对的生成和安装

6.2.1 根证书密钥对的生成和安装

CA 密钥生成工作在物理隔离的安全环境内开展，统一使用经国家密码管理部门认可、检测认证的硬件密码设备及密码模块。密钥的生成、备份、恢复、销毁等操作执行 M 选 N 多人控制机制，其中 M 不少于 5，N 不低于 M/2；所有操作必须经安全策略委员会授权，全程进行录音录像，相关记录保存期限自操作完成之日起不少于十年。

CA 密钥由多名可信人员依规开展管理，其生成、存储、使用、备份、恢复、归档、销毁等全生命周期环节，均需严格遵守国家密码管理相关法律法规、标准规范及安全管理要求，保障密钥全程安全可控。

6.2.2 订户密钥对的生成和交付

订户的签名密钥对由订户持有的符合国家安全标准的密码设备（如智能密码钥匙、密码设备、密码模块）产生和存储，加密密钥对由密钥管理中心生成。完整留存签名私钥相关操作日志，记录操作时间、方式、人员等信息，日志保存期限自证书失效之日起不少于五年。

6.2.3 私钥传送给订户

订户的签名密钥对由自己的密码设备生成并保管。

加密密钥对由 KMC 产生，通过安全通道传到订户手中的密码设备中。

6.2.4 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 HLJCA。

订户的加密证书公钥，由 KMC 通过安全通道传递到 CA 中心。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.2.5 电子认证服务机构公钥传送给依赖方

依赖方可以从 HLJCA 的网站上下载根证书和 CA 证书，从而得到 CA 的公钥。

6.2.6 密钥的长度

HLJCA 用于加密和签名的 SM2 密钥对的模长为 256 位，对称密钥的长度是 128 位。

6.2.7 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的硬件产生。

6.2.8 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

6.3 私钥保护和密码模块工程控制

6.3.1 CA 私钥保护和密码模块工程控制

HLJCA 所用的密码设备都是经国家密码管理局认可的产品，其安全性达到以下要求：

接口安全：不执行规定命令以外的任何命令和操作；

协议安全：所有命令的任意组合，不能得到私钥的明文；

密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

根 CA 系统的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 个管理员 USB KEY 中，只有其中三至五人在场并许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过密码设备控制。

6.3.2 订户私钥保护和密码模块工程控制

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

KMC 严格保证用户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

订户的签名密钥 HLJCA 和 KMC 都不备份。加密私钥由 KMC 备份，备份数据以密文形式存在，保存在有防盗措施的安全场所。

订户密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询或恢复。

HLJCA 提供过期的托管加密密钥的归档服务。

6.3.3 私钥导入或导出密码模块

使用 HLJCA 软件可以把私钥安全导入密码模块中，私钥无法从硬件密码模块中导出。

6.3.4 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。密码设备采用国家密码管理局批准和许可的服务器密码机，硬件密码模块至少符合国家标准，私钥的数据存储在服务器密码机硬件中，在整个生命周期都不会明文出现在硬件密码机之外。订户的私钥存储在符合国家密码管理规定的设备或文件证书中，所有在设备中存储的私钥，都以密文的形式保存。

6.3.5 激活私钥的方法

具有激活私钥权限的管理员使用含有自己身份的 USB KEY 登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员同时在场。

6.3.6 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己身份的 USB KEY 登录，启动密钥管理程序，进行解除私钥的操作，需要三名管理员同时在场。

当订户使用硬件密码模块产生、保存私钥时，订户使用硬件密码模块口令（或 pin 码）保护私钥，硬件加密模块被加载，密码模块验证口令完成后，私钥被激活。

6.3.7 销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己身份的 USB KEY 登录，启动密钥管理程序，进行销毁密钥的操作，需要三名管理员同时在场。

当订户私钥过期或发现不安全时，应按照存储私钥的密码模块的说明完成私钥销毁。订户在销毁私钥前，须自行确认是否还有信息需要加密私钥进行解密。由于订户销毁私钥导致的原有信息无法解密的后果，需由订户自行承担，HLJCA 不承担任何责任。

6.3.8 密码模块的评估

HLJCA 使用普华诚信信息技术有限公司的 SJJ1011 服务器密码机，该密码机已通过国家密码管理局的审批，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。主要技术指标如下：

a）通信接口：符合国际 ITU Ethernet RJ45 标准；

b）带宽控制：10M/100M/1000M 自适应，充分满足突发业务需要；

c）密钥管理：密钥不以明文形式出现在服务器密码机以外；

d）身份鉴别：采用 USB KEY 对用户进行身份鉴别管理，以控制对加密系统的使用；

e）处理速度：SM2 签名速度：350 次/秒

SM2 加密速度：180 次/秒

SM1 算法加密/解密速度：90Mbps

6.4 密钥对管理的其他方面

6.4.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥，由 HLJCA 和密钥管理中心定期归档。HLJCA 每五年定期完成归档操作。

6.4.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。特殊情况下，对于签名类证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。为了验证在证书有效期内签名的信息，与之对应的公钥可以在证书的有效期限以外使用，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。

对于加密类证书，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

另外需注意的是无论是订户证书还是根证书，证书到期后，在保证安全的情况下，允许使用原密钥对证书进行更新。但是密钥对不能无限期使用。订户证书其密钥对的最长允许使用年限是 5 年，根证书其密钥对的最长允许使用年限是 20 年。

6.5 激活数据

6.5.1 激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质（如：智能密码钥匙）出厂时设置了缺省的 PIN 值，证书制作时激活证书存储介质的 PIN。

HLJCA 产生的激活数据，包括用于下载证书的口令、USBKey、IC 卡的登录口令等，都是在安全可靠的环境下产生。这些激活数据，都是通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。为了保护私钥的安全，证书订户生产和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改，或者被非法授权的披露。CA 私钥的激活数据，必须按照有关密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。订户私钥的激活数据，激活数据是保护私钥的密码，HLJCA 推荐订户使用强口令来保证私钥的安全性，该口令需要：

- 至少为 8 位数字
- 建议至少包含一个小写字母以及一个大写字母

●建议订户不要使用生日、简单重复的数字等容易被人猜中或破解的信息做为口令

6.5.2 激活数据的保护

HLJCA 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。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。同时为了配合业务系统的安全需要，应该经常对激活数据进行修改。

6.5.3 激活数据的其他方面

只有在拥有证书介质并知道证书介质的 PIN 值时才能激活证书存储介质，进而使用私钥。考虑到安全因素，对于订户激活数据的生命周期，规定如下：用于保存私钥的密码模块的 PIN 码（口令），建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后需要进行修改。

6.6 计算机安全控制

HLJCA 按照国家有关信息安全、密码管理及电子认证服务相关法律法规和标准要求，依据《信息安全技术证书认证系统密码及其相关安全技术规范》《电子认证服务管理办法》以及其他相关信息安全标准规范，建立并实施符合 GB/T25056—2018 相关要求的计算机安全控制体系，制定全面、完善的信息安全管理制度、安全技术规范及运行维护流程，并在运营过程中持续实施、检查、审计和记录。

建立覆盖认证系统、网络系统、主机系统、数据库系统及安全设备的安全管理机制，主要安全控制措施包括身份识别与认证、逻辑访问控制、物理访问控制、权限分离管理、网络边界防护、安全审计、恶意代码防护及系统运行监控等。

实行严格的身份认证与权限控制机制，为所有具有系统访问权限的人员（包

括 CA 系统、RA 系统及相关管理系统操作人员）分配唯一身份账户，并按照最小权限原则授予访问权限。系统访问采用双因素身份认证机制，包括用户名、口令及数字证书等认证方式。

通过严格的安全控制措施，保障 CA 软件、业务系统及数据文件运行环境的安全性和可信性，防止未经授权的访问、使用、泄露、篡改或破坏。核心业务系统应与其他系统实施物理隔离，生产环境应与办公环境、测试环境进行逻辑隔离，以限制未经授权的网络访问行为。通过防火墙、访问控制设备、安全隔离设备及其他安全防护措施，对内外网络访问进行控制和防护，限制对生产系统的非授权访问。仅具有业务需要并经过授权的可信人员，方可访问 CA 系统及相关数据库。相关访问和操作行为应进行日志记录和安全审计。

电子认证系统通过国家有关主管部门的安全性检查或评估，并定期接受认证系统、计算机系统及网络安全相关检查和评估。根据安全管理要求、风险情况及技术发展需要，HLJCA 对认证系统及安全防护措施进行升级、优化和完善。

HLJCA 至少每半年对操作系统、中间件、数据库及相关应用系统的安全补丁和升级情况进行检查，并对系统升级、补丁安装、变更审批及实施过程进行记录和管理。

对于已停止官方补丁支持或不再提供安全更新的系统，HLJCA 采取网络隔离、访问限制、功能限制等加强防护措施，并制定系统升级、更换或迁移计划。

在所有服务器、业务终端及管理终端部署防病毒软件或恶意代码防护软件，并保持恶意代码防护机制持续有效。

病毒库应定期更新，更新周期原则上不超过 30 日；对于重要系统、高风险环境或出现重大安全风险时，会及时更新病毒特征库。

定期对服务器、终端设备及相关存储介质进行恶意代码扫描，病毒扫描周期原则上不超过 30 日；对于关键业务系统，可根据安全风险情况提高扫描频率。

HLJCA 电子认证服务系统已通过国家密码管理局组织的安全性审查。

6.7 生命周期技术控制

6.7.1 系统开发控制

系统开发采用先进的安全控制理念，同时兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.7.2 安全管理控制

HLJCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才能进行安全使用，任何修改和升级会记录在案。

6.7.3 生命周期安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计符合 GB/T25056—2018 中第 10、11、12 章要求的生存周期安全控制体系中的相关要求。使用的算法和密码设备均通过了国家密码管理局审批，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。HLJCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括对软、硬件生命周期的安排。

6.8 网络安全控制

HLJCA 建立并实施符合 GB/T25056—2018 相关要求的网络安全控制体系，对认证系统网络环境实施统一安全管理和安全防护，确保电子认证服务系统、网络设备及相关数据安全、稳定运行。

认证系统采用符合安全要求的网络架构，并通过防火墙、安全隔离设备及网络安全控制系统实施网络边界防护。核心业务网络、生产网络、管理网络、办公

网络及外部接入网络之间实施物理隔离或逻辑隔离，防止未经授权的网络访问及数据交互。仅开放证书申请、证书查询、证书状态查询等电子认证服务相关功能供用户访问，并对相关访问行为实施安全控制。未经授权的人员不得访问 CA 系统、RA 系统、证书目录系统、数据库系统及相关核心设备。

对 Web 服务部署防火墙、Web 应用防火墙、入侵检测或入侵防御系统、内容过滤等安全防护措施，并根据安全管理要求及时更新安全策略和相关系统版本，降低网络安全风险。

建立并维护完整、准确的网络拓扑结构文档。网络拓扑图包括网络设备、连接关系、网络区域划分及安全边界等信息，并根据网络结构调整或设备变更情况及时更新，确保与实际网络环境保持一致。

针对证书签发子系统、证书注册子系统及相关数据库建立访问控制和白名单机制，仅允许经授权的业务模块、管理设备及可信主机进行访问，并对访问来源、访问协议、访问端口及访问权限实施严格控制。

部署了入侵检测、安全审计、恶意代码防护及网络管理系统，并持续监测认证系统及网络运行状态。HLJCA 定期对系统日志、网络日志及安全审计记录进行分析，分析内容包括系统异常、未经授权的访问尝试、资源使用异常、配置变更及其他安全事件，并根据分析结果及时采取相应处置措施。

对网络安全相关操作、配置变更、安全事件及安全审计活动进行记录，并按照相关规定妥善保存相关日志和记录，以满足安全审计和事件追溯要求。

6.9 时间戳

HLJCA 目前未部署且不对外提供可信时间戳服务，本条规则在现行 CPS 中不适用。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

HLJCA 签发的证书符合 GB/T20518 要求。遵循 X.509 v3 证书模板，序列号、

签发者、主体、有效期、公钥、签名算法、签名值字段编码、ASN.1 DER 编码格式完全匹配标准定义。证书包含支持的数字证书格式版本号、密码算法对象标识符、CA 和订户的名称、证书序列号、证书有效期、订户的电子签名验证数据、CA 的电子签名、证书策略对象标识符，包含主管部门制定的相应等级证书策略 OID（§1.5.1）等。

7.1.1 版本号

X.509 V3。

7.1.2 证书扩展项

HLJCA 定义的证书扩展项可使用 IETF RFC 3280 中定义的如下证书扩展项：

机构密钥标识符 AuthorityKeyIdentifier

主体密钥标识符 SubjectKeyIdentifier

密钥用法 KeyUsage

扩展密钥用途 ExtendedKeyUsage

私有密钥使用期 PrivateKeyUsagePeriod

证书策略 CertificatePolicies

策略映射 PolicyMappings

主体替换名称 SubjectAlternativeName

颁发者替换名称 IssuerAlternativeName

主体目录属性 SubjectDirectoryAttributes

基本限制 BasicConstraints

名称限制 NameConstraints

策略限制 PolicyConstraints

证书撤销列表分发点 CRLDistributionPoints

限制任意策略 InhibitAnyPolicy

最新证书撤销列表 FreshestCRL

机构信息访问 AuthorityInformationAccess

主体信息访问 SubjectInformationAccess

私有扩展项支持以下类型

个人身份标识码 IdentifyCode

个人社会保险号 InsuranceNumber

企业工商注册号 ICRegistrationNumber

企业组织机构代码 OrganizationCode

企业税号 TaxationNumber

7.1.3 算法对象标识符

使用 SM2 算法，算法 OID 为 1.2.156.10197.1.502。

7.1.4 名称形式

HLJCA 数字证书中的主体的 X.500DN 是 C=CN 命名空间下的 X.500 目录唯一名字。DN_C（Country）属性的编码使用 PrintableString，其他属性的编码一律使用 UTF8String。

主体的 X.500 DN 为：

C= CN

S= XXXX

L= XXXX

O= XXXX

OU= XXXX

CN= XXXX

C（Country）为 CN，表示国家；

S（StateOrProvinceName）表示省份；

L（LocalityName）表示城市；

O（Organization）中的内容分为 2 种：

a）证书主体或者证书主体所属单位具有明确的上一级单位，则为其上一级单位的名称全称；

b）不存在 a）中所述的上一级单位，则为证书主体或者证书主体所属单位的所在省、自治区、直辖市名称全称；

OU（Organization Unit）为证书主体或者证书主体所属单位的名称全称；

CN（Common Name）中的内容分为 4 种：

a）个人证书中为证书主体的姓名；

b）单位机构证书中为证书主体单位的标准简称；

c）服务器证书为证书主体设备的域名或者 IP 地址或者设备编码；

d）代码签名证书为负责人的姓名，或者是所属单位的标准简称。

7.2 证书撤销列表

HLJCA 签发的证书吊销列表遵循 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

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用 CRL 条目扩展项。

采用 GB/T16262.1-2006 的特定编码规则（DER）对下列证书撤销列表项中的各项信息进行编码，组成特定的证书撤销列表数据结构。ASN.1DER 编码是关于每个元素的标记、长度和值的编码系统，格式符合 GB/T20518—2018 中 5.3 的相关要求。

7.3 在线证书状态协议

OCSP 服务采用符合国家密码管理要求的密码算法和数据编码方式，实现证书状态的在线查询与验证。OCSP 响应中包含证书状态、响应者信息等内容，依赖方可对响应结果的真实性和完整性进行验证。

7.3.1 版本号

OCSP：v1。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8 认证机构审计及相关评估

8.1 审计评估制度

审计是为了检查、确认 HLJCA 是否按照《电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分为内部审计和外部审计。

内部审计是由 HLJCA 自己组织内部人员进行的审计，审计的结果可供 HLJCA 改进、完善业务，内部审计结果不需要公开。

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

8.1.1 评估者的资质

内部审计人员的选择一般包括：

HLJCA 的安全负责人及安全管理人员；

HLJCA 业务负责人；

认证系统及信息系统负责人；

人事负责人；

其他需要的人员。

外部审计的审计人员的资质由第三方确定。

8.1.2 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

8.1.3 评估内容

对 HLJCA 规范评估包括：

安全策略是否得到充分实施；

运营工作流程和制度是否严格遵守；

电子认证业务规范是否符合证书策略的要求；

是否严格按照本 CPS、业务规范和安全要求开展业务；

各种日志、记录是否完整，是否存在问题；

HLJCA 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 HLJCA 的技术、手续和员工的相关管理政策和业务声明；

HLJCA 是否实施了相关技术、管理、相关政策和业务声明；

评估者或 HLJCA 认为有必要评估的其他方面。

8.1.4 对问题与不足采取的措施

对审计中发现的问题，HLJCA 将根据审计报告的内容准备一份解决方案，明确对此采取的行动。HLJCA 将根据国际惯例和相关法律法规迅速解决问题。

8.1.5 评估结果的传达与发布

除非法律明确要求，HLJCA 一般不公开评估结果。

对 HLJCA 关联方，HLJCA 将依据签署的协议来公布评估结果。

8.2 认证业务审计

HLJCA 落地执行认证业务审计与全面符合性评估两项制度，持续对电子认证服务的合规性、运行有效性及整体安全水平开展监督与评价。

认证评估分为认证业务审计、全面符合性评估两类。其中，认证业务审计聚焦证书全生命周期内的各项业务开展检查；全面符合性评估围绕电子认证服务许可条件、认证规则落地情况及整体运营管理工作实施综合考评。

认证业务审计常规情况下每年至少开展一次。若出现重大安全事件、重大业务调整、监管部门指令、集中投诉举报，或是其他可能影响电子认证服务安全与合规运营的情形，将及时启动专项审计或临时评估工作。

参与审计、评估工作的人员，须具备电子认证、信息安全、密码应用、信息系统审计、法律合规等相关专业能力，且熟知行业法律法规、标准规范与业务流程。若委托第三方机构开展相关工作，合作机构须具备对应专业资质、保持工作独立性并拥有良好从业信誉，同时需与 HLJCA 签订保密协议。

审计与评估的核查范围包含电子认证业务规则执行、证书全生命周期管理、密钥管理、信息安全管理、人员管理、物理环境安全、系统运行、业务连续性管理，以及法律法规和监管要求的落实情况等。工作开展可结合文件审阅、资料核对、现场核查、人员访谈、系统核验、抽样检查等多种方式进行。

HLJCA 常态化组织开展认证业务审计，对电子认证服务各项业务实施监督检查，保障所有认证业务严格遵守国家法律法规、监管规定、证书策略（CP）及电子认证业务规则（CPS）。认证业务审计每年至少开展一次，结合实际业务运行状况，可另行组织专项审计。

审计工作重点核查证书申请、签发、更新、续期、密钥变更、撤销、冻结、恢复等全流程业务，检查各环节中订户告知、身份核验、实人查验、意愿确认、协议签订、资料留存、业务审批及操作记录的合规性。同时对安全策略落地、业务流程执行、日志完整度、档案管理及潜在安全风险开展全面排查。审计可采取全面审计或抽样审计形式，若采用抽样方式，抽样占比不低于当期业务总量的 10%，保证样本具备代表性与有效性。

针对审计查出的问题，我方将及时向相关部门及责任人下达整改通知，明确整改标准与完成时限，并持续跟踪核验整改成效，确保问题彻底处置。审计全过程资料与审计结果均形成书面材料，按规定归档留存。

8.3 全面符合性评估

HLJCA 建立常态化全面符合性评估机制，针对电子认证服务全流程开展合规

核查，重点检验各项业务是否严格遵循国家法律法规、监管规定、经营许可条件、证书策略（CP）及电子认证业务规则（CPS）。该评估工作原则上每年至少组织一次。

评估范围涵盖年度电子认证服务运营状况、电子认证服务许可条件保持情况、证书策略与认证规则落地执行情况、信息安全管理体系运转状态、密码应用合规性、业务连续性管理、风险管控成效，以及监管部门明确的其他核查事项。若采取抽样检查方式，抽样比例需严格满足认证业务审计的相关标准。

针对评估排查出的问题，HLJCA 将第一时间告知责任部门，督促制定整改方案、逐项落实整改举措，并全程跟踪整改进度与实际成效。

HLJCA 按年度编制符合性评估报告，须在每年 1 月底前完成上一年度报告编制并按监管要求上报。评估报告、工作记录等相关资料，均依照单位档案管理规定统一归档留存。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和（或）更新费用

HLJCA 的数字证书的收费标准经过了严格的服务成本核算并制定价格策略。按照国家和黑龙江省物价主管部门批准的收费标准执行。

根据证书实际应用的需要，HLJCA 在不高于收费标准的前提下可以对证书价格进行适当调整。

9.1.2 证书访问费用

在证书有效期内，对该证书信息进行查询，HLJCA 不收取查询费用。

9.1.3 证书撤销或状态信息的查询费用

查询证书是否吊销，HLJCA 不收取信息访问费用。

对于在线证书状态查询（OCSP），由 HLJCA 与订制者在协议中约定。

9.1.4 其他服务的费用

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

9.1.5 退款策略

在实施证书操作和签发证书的过程中，HLJCA 遵守并保持严格的操作程序和策略。一旦订户接受数字证书，HLJCA 将不办理退证、退款手续。

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

9.2 财务责任

HLJCA 保证其具有维持其运作和履行其责任的财务能力。有能力承担对订户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

HLJCA 具备维持电子认证服务持续运营及履行相应责任的财务能力，并建立与电子认证服务规模和风险相适应的财务保障机制。设立赔付专项备用资金或采取其他有效的资金保障方式，用于电子认证服务过程中可能产生的赔偿责任。相关资金保障额度不低于上一年度营业收入的 1.5%，并根据业务发展情况、风险情况及监管要求进行动态调整。

赔付专项备用资金来源包括但不限于公司自有资金、风险准备金、专项保障资金或其他合法资金来源。相关资金由 HLJCA 按照内部财务管理制度进行管理和使用，确保资金安全、独立和可用于电子认证服务相关赔付责任。

9.3 业务信息保密

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

a）在双方披露时标明为保密（或有类似标记）的；

b）在保密情况下由双方披露的或知悉的；

c）双方根据合理的商业判断应理解为保密数据和信息的；

d）以其他书面或有形形式确认为保密信息的；

e）或从上述信息中衍生出的信息。

对于 HLJCA 来说，保密信息包括但不限于以下方面：

a）最终用户的私人签名密钥都是保密的；

b）保存在审计记录中的信息；

c）年度审计结果也同样视为保密；

d）除非有法律要求，由 HLJCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

HLJCA 不保存任何证书应用系统的交易信息。除非法律明文规定，HLJCA 没有义务公布或透露订户数字证书以外的信息。

9.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。HLJCA 在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书的相关信息可以通过 HLJCA 目录服务等方式向外公布。

HLJCA 在其目录服务器中公布证书的吊销信息，供网上查询。

9.3.3 保护保密信息的责任

各方有保护自己和其他人员或单位的机密信息并保证不泄露给第三方的责任。不将机密数据和信息（也不会促使或允许他人将机密数据和信息）用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

当 HLJCA 在任何法律法规或规章的要求下，或在法院的要求下必须提供本《电子认证业务规则》中具有保密性质的信息时，HLJCA 按照要求，向执法部门

公布相关的保密信息，HLJCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

除非证书申请人主动提供，HLJCA 保证不会收集任何证书申请人的资料。HLJCA 按照国家有关法律法规及相关标准要求，对订户个人信息和隐私信息进行保护，并采取必要的管理措施和技术措施，防止信息泄露、篡改、损毁、丢失或被非法获取、非法使用。HLJCA 通过身份鉴别、访问控制、权限管理、安全审计、安全传输、备份恢复等措施，对订户个人信息进行安全保护。

9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。

数字证书是公开的，通过 HLJCA 目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄露、使用或发布给第三方。

9.4.5 使用隐私信息的告知或同意

使用隐私信息，须获得本人同意。

9.4.6 依法律或行政程序的信息披露

当 HLJCA 在任何法律法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，HLJCA 按照法律法规或规章的要求或法院的要求，向执法部门公布相关信息，HLJCA 无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

除非额外声明，HLJCA 享有并保留对证书以及 HLJCA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。HLJCA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本《电子认证业务规则》的规定，所有由 HLJCA 签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于 HLJCA 所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得 HLJCA 的同意使用相关的文件和手册，并有责任和义务提出修改意见。

9.6 陈述和担保

9.6.1 电子认证服务机构的陈述与担保

HLJCA 在提供电子认证服务活动过程中的承诺如下：

a）遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的法律责任。

b）保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

c)除非已通过HLJCA证书库发出了HLJCA的私钥被破坏或被盗的通知,HLJCA保证其私钥是安全的。

d）签发给订户的证书符合 HLJCA 的 CPS 的所有实质性要求。

e）HLJCA 将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。

f）HLJCA 将及时吊销证书。

g）拒绝签发证书后，将立即向证书申请人归还所支付的全部费用。

h）证书公开发布后，HLJCA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构的陈述与担保

注册机构在参与电子认证服务过程中的承诺如下：

a）提供给证书订户的注册过程完全符合 HLJCA 的《电子认证业务规则》的所有实质性要求。

b）在 HLJCA 生成证书时，不会因为失误而导致证书中的信息与证书申请人的信息不一致。

c）在 HLJCA 将按 CPS 的规定，及时提交证书申请、吊销、更新等服务请求。

9.6.3 订户的陈述与担保

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

a）订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书持有人在证书使用方面的有关限制。

b）订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供 HLJCA 检查和核实。

c）订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄漏和被篡改等事件的发生。

d）私钥为订户本身访问和使用，订户对使用私钥的行为负责。

e）一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以

及其他情况，订户应立刻通知 HLJCA，申请采取吊销等处理措施。

f）订户已知其证书被冒用、破解或被他人非法使用时，应及时通知 HLJCA 吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《电子认证业务规则》的有关条款。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同§9.6.4。

9.7 担保免责

有下列情况之一的，免除 HLJCA 之责任：

a)如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必需的审核文件，得到了 HLJCA 签发的证书，由此引起的经济纠纷应由证书申请人全部承担，HLJCA 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。

b）HLJCA 不承担任何其他未经授权的人或组织以 HLJCA 名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

c）HLJCA 不承担在法律许可的范围内，根据受害者或法律的要求如实提供网 上业务中“不可抵赖”的数字签名依据所引起的法律责任。

d）HLJCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损 失承担责任。

e)由于客观意外或其他不可抗力事件原因而导致证书签发错误、延迟、中 断、

无法签发，或暂停、终止全部或部分证书服务的。

f）因 HLJCA 的设备或网络故障等技术故障而导致证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。本项所规定之“技术故障”引起原因包括但不限于：不可抗力；关联单位如电力、电信、通讯部门而致；黑客攻击；设备或网络故障。

g）HLJCA 已谨慎地遵循了国家法律法规规定的证书认证业务规则，而仍有损失产生的。

9.8 偿付责任规则

9.8.1 偿付责任范围

HLJCA 只在证书有效期限内承担有限损失赔偿责任。在证书有效期内产生的损失，订户或依赖方应在知道或应当知道损失发生之日起一年内向 HLJCA 书面提出赔偿申请，其间届满未提出的，视为放弃赔偿申请权利。期满后提出的，HLJCA 有权拒绝申请。HLJCA 建立了赔付审核与监督机制，对赔偿申请受理、调查、审核、处理及结果反馈全过程进行记录和管理。赔偿处理过程中，相关部门应对赔偿事项进行审核、复核和监督，确保赔偿处理过程规范、完整和可追溯。

9.8.2 对最终实体的赔偿担保

在任何情况下，HLJCA 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，HLJCA 和发证机关也不需负责。

9.8.3 责任免除

有下列情况之一的，将免除 HLJCA 之责任。

a）如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，

又根据正常的流程提供了必需的审核文件，得到了 HLJCA 签发的数字证书，由此引起的经济纠纷应由证书申请人全部承担，HLJCA 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。

b）HLJCA 不承担任何其他未经授权的人或组织以 HLJCA 名义编撰、发布或散布的不可信赖的信息所引起的法律责任。

c）HLJCA 不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。

d）HLJCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

e）HLJCA 不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。HLJCA 和证书持有人间的关系以及 HLJCA 和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方法让 HLJCA 承担信托责任。

f）由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。

g）因 HLJCA 的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障。

h）HLJCA 已谨慎地遵循了国家法律法规规定的数字证书认证业务规则，而仍有损失产生的。

HLJCA 根据与订户的合同承担相应的有限责任。

HLJCA 在与订户和依赖方签订的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

HLJCA 按照本《电子认证业务规则》具有担保免责和承担有限赔偿的责任，赔偿责任上限为该订户实际缴纳数字证书当年注册开户费或年度服务费的十倍。订户或依赖方认为因 HLJCA 原因导致其合法权益受到损害的，可以向 HLJCA 提出

赔偿申请，并提交相关证明材料，包括但不限于身份证明、证书信息、损失证明及相关情况说明等材料。HLJCA 在收到赔偿申请后会在 5 个工作日内对申请材料进行初步审查。对于申请材料不完整的，会及时通知申请人补充相关材料。

HLJCA 受理赔偿申请后，将对事件原因、责任归属、损失情况及相关证据材料进行调查和审核。审核工作原则上在 30 个工作日内完成；对于情况复杂或存在特殊情形的，可适当延长审核期限，并将相关情况告知申请人。赔偿事项经审核确认后，由 HLJCA 按照内部审批流程进行审批。审批通过后，HLJCA 按照相关约定向申请人支付相应赔偿款项原则上在 15 个工作日内完成。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致 HLJCA 产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

a）未向 HLJCA 提供真实、完整和准确的信息，而导致 HLJCA 或有关各方损失。

b）未能保护订户的私钥，或者没有采取必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

c）在知悉证书密钥已经失密或者可能失密时，未及时告知 HLJCA，并终止使用该证书从而导致 HLJCA 或有关各方损失。

d）订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

e）证书的非法使用，即违反 HLJCA 对证书使用的规定，造成了 HLJCA 或有关各方的利益受到损失。

9.10 有效期限与终止

9.10.1 有效期限

本《电子认证业务规则》自发布之日起正式生效。

本《电子认证业务规则》中将详细注明版本号及发布日期。

9.10.2终止

当新版本的《电子认证业务规则》正式发布生效时，旧版本的《电子认证业务规则》自动终止。

9.10.3效力的终止与保留

《电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

9.11 对参与者的个别通告与沟通

认证活动的某一参与方与另一参与方进行通信时可通过适当方式（如电话、电邮、信函、传真等）以使其通信过程在法律上有效。

9.12 修订和发布

9.12.1修订程序

当本《电子认证业务规则》不适用时，由 HLJCA 安全策略管理委员会组织 CPS 编写小组进行修订。

修订完成后，由 HLJCA 安全策略管理委员会进行审批，审批通过后将在 HLJCA 网站（www.ca.com.cn）发布新版本的《HLJCA 电子认证业务规则》。

9.12.2通告机制和期限

本《电子认证业务规则》在 HLJCA 的网站（www.ca.com.cn）上发布。

版本更新时，最新版本的《电子认证业务规则》在 HLJCA 的网站发布，对具体个人不作另行通知。

9.12.3 必须修改业务规则的情形

当管辖相关法律、适用标准及操作规范等有重大改变时，必须修改《黑龙江省数字证书认证有限公司电子认证业务规则》

9.13 争议处理与举证

证书订户、依赖方等实体在电子认证活动中产生争议可按照以下方面解决：

1、当事人首先通知 HLJCA，根据《黑龙江省数字证书认证有限公司电子认证业务规则》中的规定，明确责任方；

2、由 HLJCA 相关部门负责与当事人协调，一般情况下，自受理争议之日起 30 个工作日内完成初步协商处理；情况复杂的，可根据实际情况适当延长处理期限，并通知相关当事人；

3、若协商不成，可以通过仲裁或司法途径解决；

4、举证制度和能力体系覆盖证书全生命周期；

5、任何因与 HLJCA 就《黑龙江省数字证书认证有限公司电子认证业务规则》所产生的任何争议而提起诉讼的，受 HLJCA 工商注册所在地的人民法院管辖。

9.14 管辖法律

本《电子认证业务规则》在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15 适用法律的符合性

在任何情况下，《黑龙江省数字证书认证有限公司电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国的法律。

在任何情况下，《黑龙江省数字证书认证有限公司电子认证业务规则》的执行、解释、翻译和有效性及相关参与者均适用中华人民共和国的法律。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

9.16.1 完整协议

本《黑龙江省数字证书认证有限公司电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.16.2 分割性

当司法机关或仲裁机构判定本《黑龙江省数字证书认证有限公司电子认证业务规则》中的某一条款由于某种原因无效或不具执行力时，不会导致整个协议无效。

9.16.3 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.16.4 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，HLJCA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.17 其他条款

HLJCA 对《黑龙江省数字证书认证有限公司电子认证业务规则》拥有最终解释权。