

河北省电子认证有限公司

电子认证业务规则

版本 4.6

河北省电子认证有限公司

生效时间：2026 年 10 月 31 日

版权声明

《河北省电子认证有限公司电子认证业务规则》受到完全的版权保护，本文件中所涉及的“河北CA”、“河北CA电子认证业务规则”及其标识等由河北省电子认证有限公司独立享有版权及其他知识产权。

未经河北省电子认证有限公司书面同意，本文件的任何部分不得以任何方式、任何途径（电子的、机械的、影印、录制等）进行复制、存储、调入网络系统检索或传播。

在满足下述条件下，本文件可以被书面授权，在非独占性的、免收版权许可使用费的基础上进行复制及传播：

●前文的版权说明和上段主要内容应标于每个副本开始的显著位置；

●副本应按照河北CA提供的文件准确、完整地复制。

对任何复制及传播本文件的请求，请寄往：河北省电子认证有限公司。

地址：石家庄市桥西区红旗大街88号翰林观天下23号楼27层

邮编：050081

电话：400-707-3355

电子邮件：hebca@hebca.com

修订历史

版本	日期	备注
1.0	2005 年 9 月 8 日	依据 RFC3647 结构进行编写。
2.0	2006 年 1 月 26 日	根据《电子认证业务规则规范（试行）》的各项要求进行修改。
2.1	2006 年 8 月 10 日	根据 RFC3647 标准、《电子认证业务规则规范（试行）》及《电子认证服务机构年检指引（试行）》进行制定。（内部修订）
2.2	2006 年 10 月 25 日	根据信产部电子认证服务管理办公室的审查意见进行修订。
3.0	2011 年 11 月	对证书生命周期中相关业务的内容进行修订完善。更正了不规范名称的文字描述。
3.1	2012 年 5 月	修订、补充身份鉴别方式、证书更新处理方式，在证书生命周期操作中增加证书变更，增加对河北 CA 数字证书载体不得转让他人的说明。
3.2	2014 年 12 月	修订退款策略。
3.3	2016 年 11 月	增加提供 7×24 小时证书状态服务的描述。
4.0	2017 年 12 月	修订用户提交资料内容

4.1	2018 年 9 月	修订退款策略
4.2	2019 年 12 月	修订初始身份确认及证书变更请求的处理
4.3	2021 年 9 月	修订初始身份确认、证书生命周期操作要求等
4.4	2021 年 12 月	增加撤销挂起的流程说明
4.5	2025 年 4 月	完善证书生命周期管理细则；更新用户隐私保护政策；细化赔偿范围、责任等。
4.6	2026 年 7 月	根据《电子认证业务规则规范》要求修订相关内容。

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 4
1.4 电子认证活动参与者 4
1.4.1 电子认证服务机构 4
1.4.2 注册机构 4
1.4.3 订户 4
1.4.4 依赖方 4
1.4.5 其他参与者 5
1.5 证书应用 5
1.5.1 证书应用分类 5
1.5.2 证书应用限制 6
1.6 策略管理 6
1.6.1 策略管理机构 6
1.6.2 策略文档批准程序 8
1.7 定义和缩写 9
1.7.1 术语、定义 9
1.7.2 缩写 12
2 信息发布与信息管理 13
3 身份标识与查验 14
3.1 身份查验通用要求 14
3.1.1 通用要求 14
3.1.2 订户告知 14
3.2 初始身份确认 15
3.2.1 证明拥有私钥的方法 15

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3.2.2 个人身份的查验 15
3.2.3 机构身份的查验 16
3.2.4 设备证书订户身份的查验 18
3.2.5 SSL 证书订户身份的查验 18
3.2.6 时间戳证书订户身份的查验 18
3.3 订户意愿记录 19
3.3.1 订户意愿记录内容 19
3.3.2 个人高等级证书的意愿记录 19
3.3.3 个人基础级证书的意愿记录 19
3.3.4 机构高等级证书的意愿记录 19
3.3.5 机构基础级证书的意愿记录 20
3.4 订户协议 20
3.5 未验证的订户信息 20
3.6 互操作要求 20
3.7 命名 21
3.7.1 命名规则 21
3.7.2 确保命名具有实际意义 21
3.7.3 商标权的处理策略和方式 22
3.7.4 其他内容 22
3.7.5 DN 项结构定义 22
4 证书生命周期操作要求 23
4.1 通用要求 23
4.2 证书申请 23
4.2.1 处理流程 23
4.2.2 处理时限 23
4.3 证书签发 23
4.3.1 签发过程 23
4.3.2 结果通告 24
4.4 证书接受 24

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.4.1 向订户交付证书的方式 24
4.4.2 接受或拒绝接受证书的步骤和条件 24
4.4.3 保存订户接受证书的记录 25
4.5 密钥对和证书的使用 25
4.5.1 交付前的安全保护 25
4.5.2 私钥管理服务要求 26
4.5.3 安全事件反馈 26
4.6 证书续期 26
4.6.1 证书续期的情形 26
4.6.2 证书续期申请人 26
4.6.3 身份查验方式 27
4.6.4 证书签发与接受 27
4.7 证书密钥更新 27
4.7.1 证书密钥更新的情形 27
4.7.2 证书密钥更新申请人 27
4.7.3 身份查验方式 27
4.7.4 证书签发与接受 28
4.8 证书变更 28
4.8.1 证书变更的情形 28
4.8.2 请求证书变更的实体 28
4.8.3 身份查验方式 28
4.8.4 证书签发与接受 28
4.9 证书撤销或冻结 28
4.9.1 证书撤销或冻结的审批流程 29
4.9.2 请求撤销或冻结证书的实体 30
4.9.3 请求处理 30
4.9.4 处理流程记录 30
4.10 证书状态信息服务 30
4.11 停止使用认证服务 31

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.11.1 停止订户服务的情形 31
4.11.2 处理停止服务请求的时限和方式 31
4.11.3 停止使用认证服务后的责任延续 32
4.11.4 停止使用服务的操作记录 32
4.12 密钥托管与恢复 33
4.12.1 根证书私钥保管 33
4.12.2 根证书密钥备份与恢复策略 33
5 认证机构设施、管理和操作控制 34
5.1 物理控制 34
5.1.1 基础设施 34
5.1.2 分区管理与访问控制 34
5.1.3 电力保障 36
5.1.4 门禁与监控 36
5.1.5 灾备 36
5.1.6 环境保障措施 36
5.1.7 消防措施 37
5.1.8 设备管理 37
5.1.9 存储媒体管理 37
5.2 操作过程控制 37
5.2.1 可信角色 37
5.2.2 职责分离 40
5.3 人员控制 40
5.3.1 可信人员资格、经历与背景要求 40
5.3.2 可信人员培训要求 40
5.4 审计日志程序 41
5.4.1 记录范围 41
5.4.2 记录内容 42
5.4.3 保存期限 42
5.4.4 日志审计内容 42

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.4.5 审计周期 42
5.5 记录归档 43
5.5.1 归档范围 43
5.5.2 保存期限 43
5.5.3 保护措施 43
5.5.4 档案管理机构 44
5.6 电子认证服务机构根证书密钥更替 45
5.6.1 密钥更替程序 46
5.6.2 密钥更替的时间 46
5.7 损害与灾难恢复 46
5.7.1 业务连续性目标 46
5.7.2 恢复流程 47
5.7.3 根私钥应急处理 48
5.7.4 事件报告 49
5.7.5 定期验证 49
5.8 电子认证服务机构终止 50
5.9 重大事项报告 50
5.9.1 重大事件类型及判断标准 50
5.9.2 报告的程序、时限与内容 52
6 认证系统技术安全控制 53
6.1 技术安全管理制度要求 53
6.2 密钥对的生成和安装 53
6.2.1 根密钥对的生成和安装 53
6.2.2 订户密钥对的生成和交付 53
6.3 私钥保护和密码模块工程控制 53
6.3.1 CA 私钥保护和密码模块工程控制 54
6.3.2 订户私钥保护和密码模块工程控制 54
6.4 密钥对管理的其他方面 55
6.4.1 公钥归档 55

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6.4.2 证书操作期和密钥对使用期限 55
6.5 激活数据 56
6.5.1 激活数据的生成和传输 56
6.5.2 激活数据的使用和保管 56
6.5.3 激活数据的销毁 57
6.6 计算机安全控制 57
6.7 生存周期安全控制 57
6.8 网络安全控制 57
6.9 时间戳 58
7 证书、证书撤销列表和在线证书状态协议 59
7.1 证书 59
7.2 证书撤销列表 59
7.3 在线证书状态协议 59
8 认证机构审计及相关评估 60
8.1 审计评估制度 60
8.1.1 审计评估的类型 60
8.1.2 执行审计评估的频率，或是引发评估事件的条件 60
8.1.3 参与执行审计评估人员的专业背景 60
8.1.4 审计评估所涵盖的主题和评估的方法 60
8.2 认证业务审计 61
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 退款规定 62
9.2 财务责任 62
9.3 业务信息保密 62
9.3.1 保密信息的范围 62
9.3.2 非保密信息的范围 63
9.4 个人隐私保护 63

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.4.1 隐私保密方案 64
9.4.2 作为隐私处理的信息 64
9.4.3 不被视为隐私的信息 64
9.4.4 用户个人信息的收集 64
9.4.5 个人信息的存储 65
9.4.6 用户个人信息的使用 65
9.4.7 用户个人信息的共享 65
9.4.8 CA 对于用户个人信息的管理 66
9.4.9 个人信息的查阅 66
9.4.10 个人信息的删除和更改 66
9.5 知识产权 67
9.6 陈述与担保 67
9.6.1 CA 的陈述与担保 67
9.6.2 订户的陈述与担保 68
9.6.3 依赖方的陈述与担保 68
9.7 担保免责 69
9.7.1 担保责任的否定描述 69
9.7.2 隐含担保责任的描述 70
9.7.3 担保免责条款的适用规定 70
9.8 偿付责任规则 71
9.8.1 财务赔偿范围 71
9.8.2 赔付计算方式 71
9.8.3 赔付监督机制 72
9.9 赔偿 72
9.10 有效期和终止 72
9.10.1 有效期限 72
9.10.2 终止 73
9.10.3 效力的终止与保留 73
9.11 对参与者个别通告与沟通 73

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.12 修订和发布 73
9.12.1 规则修订的条件 73
9.12.2 通告机制和周期 74
9.13 争议处理与举证 74
9.13.1 争议受理范围 74
9.13.2 争议处理流程 74
9.13.3 协商时限 74
9.13.4 调解规则 75
9.13.5 仲裁与诉讼管辖规则及适用条件 75
9.13.6 举证制度和能力体系 75
9.14 管辖法律 75
9.15 与适用法律的符合性 76
9.16 一般条款 76
9.17 其他条款 76

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

1 概括性描述

1.1 承诺

河北省电子认证有限公司（Hebei Certificate Authority Co., Ltd.，简称河北 CA）是中华人民共和国工业和信息化部批准的第三方电子认证服务机构。河北 CA 编订并发布《河北省电子认证有限公司电子认证业务规则》公示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。

河北 CA 作出如下承诺：

a) 遵守《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》等法律、行政法规，树立以人民为中心的服务理念，承担用户网络可信身份鉴别，维护国家网络安全的社会责任。

b) 与客户建立业务关系前，开展应用业务调研，对应用接入业务进行风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；

c) 使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；

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

1.2 基本信息

河北省电子认证有限公司（Hebei Certificate Authority Co., Ltd.，简称河北 CA）2006 年 11 月 17 日依法取得中华人民共和国工业和信息化部颁发的《电子认证服务许可证》编号：ECP13010821021，当前许可证有效期：2021 年 11 月 17 日至 2026 年 11 月 16 日。法定代表人：罗小津，机构住所：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23-01-2701。

河北 CA 服务网点地址和联系方式如下：

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地市	服务网点地址	联系电话
石家庄	桥西区休门街与四中路交汇处，休门街 3 号滨江优谷大厦 8 楼 811 室（南大厅进入）	0311-80800081
石家庄	桥西区红旗大街与槐安路交口北行 100 米路西，红旗大街 88 号广友大厦（十七中正对面），请绕行至广友大厦西南角，翰林观天下 23 号楼入口进入，到达 27 层。	4007073355
石家庄	新华区石清路 9 号河北航投大厦 16 层 1601 室（省公共资源交易中心楼上，需院外绕行至主楼北大厅进入）	19932119722
石家庄	长安区方北路 18 号中国社会保险 A 区 5 楼 503 室	4007073355
承德	双桥区府前路（市政府对面）华峰中心 A 座 1401 室	18932853700
张家口	桥东区建设东街 27 号富海广场 804 室	13103030947 13231350947
张家口	宣化区市民中心五楼河北 CA 窗口	13231340947
秦皇岛	海港区红旗路 233 号市政务大厦 12 楼 1205 室	13231377228 0335-3377228
秦皇岛	海港区民族路 6 号，市政务服务中心 4 楼公共资源交易中心河北 CA 窗口	13231377228 0335-3377228
唐山	路北区学院路 39 号（路北人社局对面）福地大厦 1588 室	15373526507 15373526739
廊坊	广阳区金光道 16 号万达广场 B 座 1510 室（万达富力嘉华酒店旁）	18932601921
廊坊	广阳区永兴路与艺术大道交口北 100 米 廊坊市市民服务中心 1 号楼 2 层廊坊市公共资源交易中心 CA 认证窗口	0316-2920629

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

地市	服务网点地址	联系电话
廊坊	广阳区广阳道 19 号	17333677003
保定	竞秀区向阳北大街 806 号金沃大厦 A 座 807 室	18630277276
沧州	运河区解放西路颐和国际 B 座 602 室	13231728652 13315703324
沧州	运河区北京路与吉林南大道交汇处，市政务服务中心，一楼北区 A 岛 16 号窗口	13231765232
衡水	桃城区南环西路 128 号市民中心 2 楼 B18 窗口	13373183527
邢台	信都区守敬路与拥军街交汇处西北角，锦鼎国际广场公寓 1817 室	18631901603
邯郸	丛台区人民东路 350 号（邯郸市行政服务中心东侧）嘉华大厦 2105 室	18931099902
邯郸	丛台区人民路 342 号邯郸市行政服务中心 4 楼北侧办公室（CA 受理室）	18931099902
雄安	保定市容城县白洋淀大道如家酒店(白洋淀店)东侧约 50 米雄安新区公共资源交易中心一楼 108 办公室	0312-7208815

河北 CA 根证书 HBSM2CA 为国家根证书 ROOTCA 签发，证书编号：72bb89dcddc44bd363614d41b729cd1a，由国家根 CA 证书 ROOTCA 签发、密码算法 SM2、密钥长度 256 位、有效期自 2012 年 10 月 15 日至 2032 年 10 月 10 日。由河北 CA 中级根证书 HBSM2CA 直接签发用户证书。

河北 CA 计划在根证书 HBSM2CA 到期前二年向国家密码管理局申请 HBSM2CA 证书续期或密钥更新，以保障河北 CA 电子认证服务的持续性。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

1.3 文档名称与标识

本文档名称是“河北省电子认证有限公司电子认证业务规则（简称：河北 CA 电子认证业务规则或河北 CA CPS）”版本号 4.6，发布日期 2026 年 6 月。河北 CA 遵循的证书策略 OID 为 1.2.156.112586.4。

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

本文档所指电子认证服务机构为河北省电子认证有限公司（Hebei Certificate Authority Co.,Ltd.，简称河北 CA）是河北省唯一一家依法取得国家《电子认证服务许可证》《电子认证服务使用密码许可证》的第三方电子认证服务机构，负责数字证书的签发、管理和认证工作。

1.4.2 注册机构

注册机构是受理数字证书申请、更新、恢复和注销等业务的实体。

河北 CA 可以授权下属机构作为注册机构，负责证书业务办理、身份鉴别与审核等服务。

河北 CA 不授权外部机构作为注册机构。

1.4.3 订户

订户是指从电子认证服务机构接收证书的实体。在不同的阶段，也称为证书申请人、证书持有人。在电子签名应用中，订户即为电子签名人。在本文档中订户也被称为用户。

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，依赖方是指基于对

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

电子签名认证证书或者电子签名的信赖从事有关活动的人。河北 CA 的证书体系中，依赖方是信任河北 CA 证书，可以对使用河北 CA 证书进行数字签名验证的实体，或者是使用河北 CA 证书公钥加密信息的实体。

1.4.5 其他参与者

其他参与者是指为河北 CA 的电子认证活动提供相关服务的其他实体。

1.5 证书应用

1.5.1 证书应用分类

河北 CA 签发的数字证书按申请主体、用途及适用场景的不同，分为电子签名认证证书、身份认证证书、设备证书、SSL 证书、时间戳证书。其中，电子签名认证证书按照证书主体对象、风险等级，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。身份认证证书按照主体的不同，分为个人身份认证证书、机构身份认证证书两类。具体证书分类、证书策略 OID、特点及适用场景细分如下：

证书类型及证书策略 OID

证书类型	证书策略 OID	特点及适用场景
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	适用于低风险业务、符合《电子签名法》的个人电子签名认证证书
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书
个人身份认证证	1.2.156.112586.4.1	适用于个人身份认证、数据完整性

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

书		保护，不适用于电子签名
机构身份认证证书	1.2.156.112586.4.2	适用于机构身份认证、数据完整性保护，不适用于电子签名
设备证书	1.2.156.112586.4.3	适用于设备身份认证、数据完整性保护，不适用于电子签名
SSL 服务器证书	1.2.156.112586.4.4	适用于加密网络传输数据、验证网站真实身份、防止数据被篡改，不适用于电子签名
时间戳证书	1.2.156.112586.4.5	适用于签发可信时间戳、证明时间公信力，不适用于电子签名

1.5.2 证书应用限制

河北 CA 颁发的数字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行承担。河北 CA 颁发的电子签名认证证书禁止应用的场景如下：

a) 涉及人身关系（如婚姻、收养、继承等）；

b) 涉及公共事业服务停止（如停止供水、供热、供气等）；

c) 法律、行政法规规定的其他不适用电子签名的应用场景或类型；

d) 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6 策略管理

1.6.1 策略管理机构

策略管理机构为河北 CA 安全策略委员会，是 CPS 和 CP 的最高管理机构。安全策略委员会由来自于公司管理层、技术中心、CPS 起草小组、合规部、安全运行部等合适代表组成。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

安全策略委员会成员公示如下：

职务	姓名	所在部门/职务
主任	吴志峰	总经理
副主任	陈晓嘉	技术总监
CPS 起草小组组长	李影	客服总监
合规部负责人	王海莉	合规部经理
安全运行部负责人	张喆	安全运行部经理

河北 CA 安全策略委员会负责 CPS 和 CP 以及配套制度的维护，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，建立专项档案台账，长期妥善保存，确保可追溯、可核查。主要工作职责如下：

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，明确起草、评审、审批、发布、备案各环节的职责分工。

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，确保关键操作和变更符合安全合规要求。

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，确保其符合国家法律法规、主管部门要求和业务实际。

d) 每年组织运营风险评估并形成报告，识别潜在风险并制定应对措施。

e) 审批确定 CPS 起草小组成员，明确其工作职责、工作内容及操作流程。

f) 组建并领导应急专项小组，负责重大安全事件的指挥、决策与审批。包括但不限于系统迁移改造、重大安全事故应对、订户信息泄露处置、合规性事件处理以及人力资源类重大事件的决策与审批。

g) 授权并监督根证书密钥的生成、备份、恢复、销毁等操作，确保上述操作在多人控制机制下实施，并全程录音录像记录。

h) 根据风险评估结果或发现的服务风险，随时安排认证业务审计或全面符合性评估，并审批审计计划、审计范围和审计结论。

i) 对 CPS 修订版本进行最终审批，并监督批准后发布以及向主管部门备案的流程。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

j） 负责制定和审批技术安全管理制度，确保覆盖密钥管理、系统开发、网络防护等领域，并定期（不低于每年一次）评审制度的有效性。

k） 负责 CPS 的对外咨询、内部培训与日常管理。

安全策略委员会成员工作职责分工如下：

安全策略委员会主任：为安全策略委员会第一责任人，统筹负责委员会重大人事、制度、密钥、审计、应急事件的最终决策与审批，全面把控电子认证业务合规安全风险。

安全策略委员会副主任：协助主任统筹安全策略委员会日常工作，负责策略流程搭建、年度评审、风险评估、审计督办及工作协调，保障各项合规工作落地执行。

CPS 起草小组组长：负责在安全策略委员会统筹下完成 CPS、CP 的起草、修订、迭代更新，并配合完成评审、备案、培训支撑等专项工作。

合规部负责人：承担安全策略委员会合规监督职能，负责全流程合规校验、风险核查、审计监督、制度有效性检查及重大事件合规处置，筑牢整体合规防线。

安全运行部负责人：在安全策略委员会中负责各类安全策略、密钥管控、制度规范的落地运维与实操保障，统筹系统安全、日常运维、技术风险落地防控，支撑委员会各项合规及安全策略有效落地。

1.6.2 策略文档批准程序

CPS 起草小组成员由负责 CA 运营、安全管理的各部门经理选举产生，由安全策略委员会成员审议通过，负责 CPS 的起草、问题收集、修订、发布、工作。

本 CPS 根据国家的政策法规、技术要求、业务发展情况每年修订。CPS 起草小组根据相关情况拟定 CPS 修订内容，由合规部、法务人员对 CPS 修订内容进行初步评审，初审通过后，将 CPS 评审稿提交河北 CA 安全策略委员会审批。经河北 CA 安全策略委员会审批通过后，递增版本号、更新发布时间/生效时间及修订记录，并由 CPS 起草小组在河北 CA 网站上发布，合规部于对外发布之日起三十日之内向工业和信息化部备案。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

1.7 定义和缩写

1.7.1 术语、定义

- 加密 encipherment encryption

  对数据进行密码变换以产生密文的过程。

- 密码模块 cryptographic module

  实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。

- 密码算法 cryptographic algorithm

  描述密码处理过程的算法。

- 密钥 key

  控制密码变换操作的符号序列。

  注：在非对称密码算法中，密钥包括私钥和公钥。

- 私钥 private key

  非对称密码算法中只能由拥有者使用的不公开密钥。

  注：属于《中华人民共和国电子签名法》中电子签名制作数据的一种实现形式。

- 公钥 public key

  非对称密码算法中可公开的密钥。

  注：属于《中华人民共和国电子签名法》中电子签名验证数据的一种实现形式。

- RSA 算法 RSA algorithm

  一种基于大整数因子分解问题的公钥密码算法。

- SM2 算法 SM2 algorithm

  由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

- SM3 算法 SM3 algorithm

  由 GB/T 32905 定义的一种密码杂凑算法。

- 公钥基础设施 public key infrastructure (PKI)

  基于公钥密码技术，具有普适性，可用于提供机密性、完整性、真实性

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

及抗抵赖性等安全服务的基础设施。

- 数字签名 digital signature

  签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

- 电子认证服务机构 certification service provider

  取得电子认证服务许可证，为需要第三方认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体。

  注：本文中也称为认证机构，简称 CA。

- 数字证书 digital certificate

  也称公钥证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

- 电子签名认证证书 electronic signature certificate

  由依据《中华人民共和国电子签名法》设立的电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。

  注 1：如无具体限定，本规范中的“证书”均指“电子签名认证证书”，本规范中的“密钥”“私钥”，均指电子签名认证证书对应的“密钥”“私钥”。

  注 2:可证实电子认证服务机构与电子签名制作数据有关系的数字证书，称为根证书。

- 电子签名依赖方 electronic signature relying party

  是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

  注：本文中简称依赖方。

- 订户 subscriber

  被颁发给一张证书的证书主体。

  注：在不同的阶段，也称为证书申请人、证书持有人。属于《中华人民共和国电子签名法》中电子签名人的一种类型。

- 对象标识符 object identifier (OID)

  用于无歧义地标识对象的全局唯一值。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

- 证书策略 certificate policy(CP)

  指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。

- 证书链 certificate chain

  证书链是一个用于证书验证的证书序列。

- 身份查验 entity authentication

  证实某个实体就是所声称身份的过程。

- 激活数据 activation data

  用于使密码模块进入可操作状态的数据。可为口令、生物特征等。

- 时间戳 time stamp (TS)

  对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

- 证书续期 certificate renewal

  指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。

- 密钥更新 key re-key

  用新密钥替换旧密钥的过程。

  注：通常指证书于密钥同时更新。

- 密钥恢复 key recovery

  将归档或备份的密钥恢复到可用状态的过程。

- 证书撤销列表 certificate revocation list (CRL)

  由电子认证服务机构签发并发布的被撤销证书的列表。

- 证书认证系统 CA system

  对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生存周期进行管理和服务的系统。

  注：也称电子认证服务系统，包括证书签发子系统、证书注册子系统等。

- 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

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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。

1.7.2 缩写

下列缩写适用于本文件。

- CA：电子认证服务机构(Certification Authority)
- CPS：电子认证业务规则(Certification Practice Statement)
- CP：证书策略(Certification Policy)
- CRL：证书撤销列表(Certificate Revocation List)
- ARL：权威撤销列表（Authority Revocation List）
- DN：甄别名称 (Distinguished Name)
- LDAP：轻量级目录访问协议(Lightweight Directory Access Protocol)
- OCSP：在线证书状态协议 (Online Certificate Status Protocol)
- OID：对象标识符(Object Identifier)
- RTO：恢复时间目标(Recovery Time Objective)
- RPO：恢复点目标(Recovery Point Objective)

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

2 信息发布与信息管理

a) 河北 CA 已在网站 http://www.hebca.com 发布以下内容：

1) CPS、CP 的所有版本；

2) 证书链：国家自签根 ROOTCA、河北 CA 中级根 HBSM2CA；

3) 证书信息、状态信息等查询服务；

河北 CA 通过网站（http://www.hebca.com）和目录服务器（LDAP）发布订户的证书、证书撤销列表（CRL），并提供 7×24 小时的证书状态服务，订户或依赖方可以通过访问河北 CA 的网站和目录服务器（LDAP）获取证书的信息和证书撤销列表（CRL）。同时，河北 CA 提供在线证书状态服务（OCSP）。

LDAP 发布地址：ldap.hebca.com 端口号：389

OCSP 发布地址：ocsp.hebca.com 端口号：3018

4) 详细的业务办理指南，包括：服务网点地址、营业时间、联系电话；

5) 依赖方协议；

6) 投诉处理政策及投诉方式，包括投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。

b) 信息更新：信息发布内容如有变化，将在变化生效后 1 个工作日内更新。

c) 监管备案：河北 CA 声明按照国家电子认证服务管理平台的要求进行了备案。

d) 证书信息对接：河北 CA 完成与国家电子认证服务管理平台的技术对接，实现根证书唯一编码、订户身份信息等维度查询河北 CA 已签发证书列表的功能。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3 身份标识与查验

3.1 身份查验通用要求

3.1.1 通用要求

a) 河北 CA 在受理订户证书申请时，均对订户和/或受托人进行告知、身份确认、意愿记录和协议签署；
b) 身份查验义务由河北 CA 履行，不会委托给外部机构或个人。

3.1.2 订户告知

3.1.2.1 告知内容

在订户申请证书时，河北 CA 明确告知以下内容：
a) 订户的权利和义务；
b) 服务收费的项目和标准；
c) 电子签名认证证书、电子签名的使用条件；
d) 信息安全保障措施；
e) CA 和订户的责任划分；
f) 订户签名私钥的存储方式及安全要求；
g) 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.1.2.2 告知方式

a) 高等级证书采用面对面、电话、视频或主管部门认可的其他方式告知，并保留告知的记录；
b) 基础级证书采用高等级证书的告知方式，或采用强制阅读、短信、邮件等方式告知，并保留告知的记录。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

a) 按照§6.2.2规定的方式生成订户密钥对；

b) 通过数字签名的方式来确认证书订户拥有某个公钥对应的签名私钥。

3.2.2 个人身份的查验

3.2.2.1 个人身份信息有效性的确认

a) 受理个人证书申请时，订户需出示有效身份证件或有效身份证件信息，个人订户有效身份证件包括：中国居民身份证、港澳居民来往内地通行证、台湾居民来往大陆通行证、护照以及法律法规和国家有关文件规定的其他有效身份证件。

b) 通过证件机读工具、权威数据库或主管部门认可的其他方式查验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，受托人出示其有效身份证件或有效身份证件信息，并按照b)款方式查验订户和受托人的身份证件或身份资料。

3.2.2.2 个人高等级证书的实人查验

对于申请个人高等级证书的订户开展实人查验，具体方式如下：

a) 面对面查验；

b) 远程人工面对面查验；

c) 生物特征验证：如活体人脸生物识别技术；

d) 通过主管部门认可的其他方式。

鉴别审核批准后，河北CA将按照相关法律法规的要求完整记录并保存身份查验过程和结果，并妥善保存订户申请材料，河北CA保存订户申请材料可以是

地址：河北省石家庄市桥西区红旗大街88号翰林观天下23号楼27层
客服热线：400-707-3355
网址：http://www.hebca.com

纸质或电子数据形式。每张证书有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

对于申请个人基础级证书的订户开展实人查验，具体方式如下：

a) 通过§3.2.2.2节规定的方式；

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

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

d) 由申请人持有的有效电子签名认证证书签名验证；

e) 通过国家网络身份认证系统对应关系验证。

鉴别审核批准后，河北CA将按照相关法律法规的要求完整记录并保存身份查验过程和结果，并妥善保存订户申请材料，河北CA保存订户申请材料可以是纸质或电子数据形式。每张证书有独立的身份验证记录。

3.2.2.4 个人身份认证证书的实人查验

同§3.2.2.3个人基础级证书的实人查验。

3.2.3 机构身份的查验

3.2.3.1 机构身份信息有效性的确认

河北 CA 受理机构证书申请时的身份信息查验方式及内容：

a) 机构有效的身份证件先通过权威数据库进行查验，权威数据库没有基础数据无法查验的，通过人工查验证件及证件信息。机构有效的身份证件包括但不限于：营业执照、统一社会信用代码证、事业单位登记证、社会团体登记证、民办非企业单位登记证、组织机构代码证、政府主管部门的批文或登记证书、法律法规和国家有关文件规定的其他有效证

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

件。

b) 法定代表人或受托人的身份，查验方式：

1) 法定代表人或受托人身份证件信息查验方式参见§3.2.2.1；

2) 受托人办理时，还需查验机构加盖公章的有效书面授权证明。

3.2.3.2 机构高等级证书的实人查验

对于申请机构高等级证书的订户开展实人查验采用下列方法之一：

a) 法定代表人实人查验，方法参见§3.2.2.2。

b) 受托人实人查验，方法参见§3.2.2.2，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。

鉴别审核批准后，河北CA将按照相关法律法规的要求完整记录并保存身份查验过程和结果，并妥善保存订户申请材料，河北CA保存订户申请材料可以是纸质或电子数据形式。每张证书有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

对于申请机构基础级证书的订户开展实人查验采用下列方法之一：

a) 法定代表人实人查验，方法参见§3.2.2.3。

b) 受托人实人查验，方法参见§3.2.2.3。

c) 由订户持有的同等或者更高级的有效机构证书签名验证。

鉴别审核批准后，河北CA将按照相关法律法规的要求完整记录并保存身份查验过程和结果，并妥善保存订户申请材料，河北CA保存订户申请材料可以是纸质或电子数据形式。每张证书有独立的身份验证记录。

3.2.3.4 机构身份认证证书的实人查验

同§3.2.3.3机构基础级证书的实人查验。

地址：河北省石家庄市桥西区红旗大街88号翰林观天下23号楼27层
客服热线：400-707-3355
网址：http://www.hebca.com

3.2.4 设备证书订户身份的查验

订户申请设备证书，可向河北 CA 注册机构提交申请。

机构订户需提交设备证书申请表（含授权内容）、加盖公章的机构有效身份证件复印件、加盖公章的受托人有效身份证件复印件。

个人订户需提交设备证书申请表、个人有效身份证件复印件。

河北 CA 将通过权威数据库确认订户身份信息的真实性，并确认订户对设备的所有权。

3.2.5 SSL 证书订户身份的查验

订户申请 SSL 证书，可向河北 CA 注册机构提交申请。

机构订户需提交 SSL 证书申请表（含授权内容）、加盖公章的机构有效身份证件复印件、加盖公章的受托人有效身份证件复印件。

个人订户需提交 SSL 证书申请表、个人有效身份证件复印件。

河北 CA 将通过权威数据库确认订户身份信息的真实性。河北 CA 还需通过可信第三方网站查询、验证指定目录设置随机数文件等方式进行域名所有权或 IP 所有权的查验。

3.2.6 时间戳证书订户身份的查验

订户申请时间戳证书，可向河北 CA 注册机构提交申请。

机构订户需提交时间戳证书申请表（含授权内容）、加盖公章的机构有效身份证件复印件、加盖公章的受托人有效身份证件复印件。

个人订户需提交时间戳证书申请表、个人有效身份证件复印件。

河北 CA 将通过权威数据库确认订户身份信息的真实性。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

3.3 订户意愿记录

3.3.1 订户意愿记录内容

订户意愿记录内容，包括但不限于：

a) 订户身份信息；

b) CA 的信息；

c) 签名私钥保存方及其保存义务；

d) 订户对电子签名的法律责任；

e) 订户对上述 a)至 d)项内容已充分知晓并同意的明确意愿表示。

3.3.2 个人高等级证书的意愿记录

对于申请个人高等级证书的订户意愿的确认采用下列方式之一：

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

b) 远程办理时，通过音视频或通过权威机构安全性评估的其他方式确认并记录订户意愿。

3.3.3 个人基础级证书的意愿记录

对于申请个人基础级证书的订户意愿的确认采用下列方式之一：

a) 与高等级证书相同的方式，参见§3.3.2。

b) 采用强制阅读、短信等电子方式。

河北 CA 将保留完整、可追溯的订户意愿记录。

3.3.4 机构高等级证书的意愿记录

对于申请机构高等级证书的订户意愿的确认采用下列方式之一：

a) 法定代表人申请时，按照§3.3.2 的方式确认机构法定代表人的意愿；

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

b） 受托人申请时，查验加盖机构公章的授权文件，并按照§3.3.2的方式确认受托人的意愿。

河北CA采用录音录像或通过主管部门认可的其他方式记录订户意愿。

3.3.5 机构基础级证书的意愿记录

对于申请机构基础级证书的订户意愿的确认采用下列方式之一：

a） 法定代表人申请时，按照§3.3.3的方式确认机构法定代表人的意愿。

b） 受托人申请时，查验加盖机构公章的授权文件，并按照§3.3.3的方式确认受托人的意愿。

河北CA采用保留完整、可追溯的订户意愿记录。

3.4 订户协议

河北CA订户协议中已明确包含§3.1.2.1中规定的内容。

3.5 未验证的订户信息

a） 河北CA会对证书中载明的所有信息进行合理查验。如证书中需要载明订户证件号码、应用系统唯一标识、单位、部门、电话号等附加信息。河北CA将采用以下方式对证书中载明的信息进行核查。常用的验证方式包括但不限于：

1） 证书申请人所在单位提供加盖公章的证书申请资料，其中包括单位、部门、手机号等需要写入证书的附加信息；

2） 河北CA在证书将使用的应用系统中获得的系统中用户唯一识别号，通过第三方维护的用户数据库查询需要写入证书的附加信息，并由数据提供方对提供的用户信息进行盖章确认。

b） 证书中不包含未经验证的订户信息。

3.6 互操作要求

河北CA支持交叉互认。根据业务需要，河北CA可以与其他经过国家主管机

地址：河北省石家庄市桥西区红旗大街88号翰林观天下23号楼27层
客服热线：400-707-3355
网址：http://www.hebca.com

构批准的 CA 机构签订互操作协议，在不同 CA 机构或不同信任域之间在证书策略一致或基本相同基础之上，互相签发交叉 CA 证书或签发单向交叉 CA 证书，建立相互信任关系，从而使双方的订户可以实现互相认证。但交叉认证并不表示河北 CA 批准了或赋予了其他 CA 中心或电子认证服务机构以河北 CA 名义开展电子认证服务的权限。

3.7 命名

3.7.1 命名规则

在河北 CA 证书服务体系中，原则上订户不使用匿名或者伪名。具体命名规则如下：

a) 个人证书命名为个人真实姓名。

b) 机构证书命名为机构全称。

c) 设备证书命名为机构名称+设备名称，同一机构多个设备申请设备证书的，为区分设备，在前述名称后增加设备编号。

d) SSL 服务器证书命名为域名或 IP 地址。

e) 时间戳证书命名为机构名称+时间戳。

3.7.2 确保命名具有实际意义

订户的甄别名（DN）必须具有实际意义，且能追溯到唯一实体。

a) 个人证书的甄别名通常可包含订户姓名，在 DN 项或扩展项中包含有效证件类型及其编号（或这些信息的某种映射，包括但不限于编号的散列值、掩码等），作为标识订户的关键信息被认证。

b) 机构证书的甄别名通常包含机构名称，在 DN 项或扩展项中包含机构的有效证件类型及其编号，作为标识订户的关键信息被认证。

c) 设备证书的甄别名通常包含设备所属机构名称或设备编码。

d) SSL 服务器证书的甄别名通常包含订户所拥有的域名、IP 地址，结合订户的其他信息一起被鉴别和认证。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

e） 时间戳证书的甄别名通常包含订户机构名称及设备编码。

在不影响证书通用性的前提下，可在证书中增加自定义的其他信息。

3.7.3 商标权的处理策略和方式

河北 CA 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.7.4 其他内容

河北 CA 签发的证书可在证书主题项或扩展项中增加其他经过验证的订户信息，如手机号、电子邮箱等。

3.7.5 DN 项结构定义

河北 CA 证书 DN 项结构定义符合 GB/T 16264.8 的要求，证书主体 DN 项编码规则如下表。

证书主体 DN 项代码

代码	说明	示例
C	国家	CN
S	省份（可选）	河北
L	城市（可选）	石家庄
O	订户所在机构信息（可选）	XX 公司
OU	订户所在机构部门信息（可选）	XX 部门
CN	订户名称（个人姓名或机构法定名称）	张三/XX 公司

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4 证书生命周期操作要求

4.1 通用要求

河北 CA 的责任，包括但不限于：

a) 河北 CA 承担建立、运营和维护注册通道的责任；

b) 河北 CA 承担与订户签订电子认证服务协议的责任；

c) 河北 CA 承担妥善记录并保存相关信息的责任。

订户的责任，包括但不限于：

a) 订户承担证书申请真实意愿的责任；

b) 订户承担提供准确信息的责任。

4.2 证书申请

4.2.1 处理流程

河北 CA 按照 §3 身份标识与鉴别，完成对订户的告知、身份确认、意愿记录、协议签署等动作，并依据既定准则批准或拒绝该申请。

4.2.2 处理时限

河北 CA 自受理之日起完成证书申请处理的最长期限为 3 个工作日。因特殊情况确需超期的，将与订户协商确定处理时限。

4.3 证书签发

4.3.1 签发过程

a) 申请信息的验证

在按照 §3.2 初始身份确认流程完成申请信息和订户身份的验证。

b) 证书的生成与签发

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

河北 CA 为审核通过的申请人签发数字证书。RA 与 CA 建立安全通道，CA 接收 RA 机构的证书申请请求，对 RA 的权限、数据格式、RA 的签名等进行验证，验证通过后，按照本 CPS 要求签发数字证书并发布证书信息。

河北 CA 提供与国家电子认证服务平台交互的数据接口，实现根据证书、订户名称、证件号码等维度从河北 CA 获取已签发证书相关信息的功能。

4.3.2 结果通告

河北 CA 通过注册机构对证书订户的通告有以下几种方式：

a) 通过认证应用工具或进行信息提示；

b) 通过信函、站内信或电子邮件发送；

c) 通过短信通知；

d) 通过电话通知；

e) 当面通知或通过实时视频等相当于面对面的方式通知；

f) 通过主管部门认可的其他方式。

4.4 证书接受

4.4.1 向订户交付证书的方式

河北 CA 向订户交付证书的方式包括：交付已下载证书的载体、订户自行下载证书、订户控制 CA 密钥托管服务下载证书。

4.4.2 接受或拒绝接受证书的步骤和条件

a) 订户接受证书的步骤和条件：订户在收到证书后，应仔细核对证书内容与申请信息是否一致，确认无误后方可启用。构成接受河北 CA 证书的行为包括：

1) 订户自收到证书起，或订户在收到证书签发成功的系统提示、短信、邮件等提示信息后，24 小时内无异议的，视为已确认证书无误并接

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

受证书。

2） 证书一经使用，即视为订户已确认证书无误并接受证书。

b） 订户拒绝接受证书的步骤和条件：订户发现证书内容有误时，可拒绝接受该证书，并向河北 CA 注册机构说明拒绝理由。河北 CA 注册机构将协助该订户撤销原证书并重新签发新证书。

4.4.3 保存订户接受证书的记录

河北 CA 将保存订户接受证书的记录，包括接受时间、方式、操作人等信息。根据不同的证书交付方式，保存订户接受证书的时间、方式、操作人信息规则如下：

a） 河北 CA 向订户交付已下载证书的载体的，证书接受时间即订户接收证书载体的时间、方式为现场领取或邮寄、操作人为实际证书载体接收人。

b） 订户自行下载证书至本地存储介质的，证书接受时间即证书下载时间、方式为自行下载证书、操作人即订户。

c） 订户控制 CA 密钥托管服务下载证书的，证书接受时间即托管服务接收到证书的时间、方式为密钥托管、操作人即订户。

4.5 密钥对和证书的使用

4.5.1 交付前的安全保护

在将密钥交付订户保管前，河北 CA 采取有效措施保障其安全性，包括但不限于以下措施：

a） 签名私钥在符合国家安全标准的密码模块内生成，私钥明文全程不出加密芯片，且无法从硬件中复制或导出，保障签名私钥生成和传输过程的安全。

b） 审核订户密钥是否符合国家或行业相关安全标准要求，拒绝为不符合要求的密钥颁发证书，包括密钥长度不足(如 RSA 小于 2048 位)、使用 MD5、SHA-1 等不安全算法。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.5.2 私钥管理服务要求

河北 CA 提供订户签名私钥管理服务，对密钥托管服务采用下列管理与技术措施，保障签名私钥的安全性：

a) 未经订户书面授权，不保存或委托他人保存其签名私钥；

b) 机构证书签名私钥的使用，可设置法定代表人或委托人作为授权主体；

c) 仅在获得订户明确授权的情况下使用其签名私钥；

d) 签名私钥以加密形式存储，保存条件符合相关安全标准；

e) 所有涉及签名私钥的操作均有完整、可追溯的记录。

4.5.3 安全事件反馈

河北 CA 建立了多种外部安全事件反馈渠道，包括 400 服务热线、投诉电话、服务网点现场受理、在线即时通讯、电子邮箱等，可以及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

4.6 证书续期

证书续期是指在不改变证书中订户主体信息的情况下，在原证书到期前，为订户签发一张新证书。

4.6.1 证书续期的情形

每张数字证书都有明确的证书有效期，表明该证书的起始日期与截至日期。如证书主体信息不变，需要继续使用证书，订户或其受托人在证书有效期到期前，应按要求向河北 CA 提出证书续期申请。

4.6.2 证书续期申请人

证书续期申请人为订户或其受托人。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.6.3 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。

4.6.4 证书签发与接受

续期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。

4.7.1 证书密钥更新的情形

证书密钥更新的情形如下（以下的情形并不代表必须执行证书密钥更新）：

a) 证书的有效期将要到期或已经到期；

b) 订户证书密钥遭到损坏；

c) 订户证实或怀疑其证书密钥不安全；

d) 河北CA的策略要求或相关法律法规引致的其他可能导致密钥更新的情形。

4.7.2 证书密钥更新申请人

证书密钥更新申请人为订户或其受托人。

4.7.3 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

地址：河北省石家庄市桥西区红旗大街88号翰林观天下23号楼27层
客服热线：400-707-3355
网址：http://www.hebca.com

行身份查验。

4.7.4 证书签发与接受

续期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）。

4.8.1 证书变更的情形

在证书有效期内，改变证书中除订户公钥之外的信息而签发新证书，对原证书进行吊销处理的情形，例如：订户名称改变等。

4.8.2 请求证书变更的实体

证书变更申请人为订户或其受托人。

4.8.3 身份查验方式

按照§3.2 的规定查验，若发起方不是证书订户，河北 CA 将取得订户同意。

4.8.4 证书签发与接受

证书签发与接受的流程符合§4.3 与§4.4 的规定。

4.9 证书撤销或冻结

证书撤销指使证书永远失效且无法恢复使用的操作。

证书冻结指使证书在有效期内暂停其使用效力的操作，需要时可申请恢复继

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

续使用原证书。

4.9.1 证书撤销或冻结的审批流程

发生下列情况之一的，订户或受托人应当向河北 CA 注册机构申请撤销或冻结证书：

a) 数字证书私钥泄露；

b) 数字证书中的信息有误或发生重大变更；

c) 认为本人不能实际履行本 CPS；

d) 认为当前密钥的安全性得不到保证。

订户或受托人申请证书撤销或冻结的审批流程：

a) 订户或受托人持机构有效证件、加盖公章的授权委托书、办理人身份证件到河北 CA 注册机构服务网点申请撤销或冻结证书。

b) 河北 CA 按照 § 3.2 进行身份确认。

c) 身份查验通过后执行证书撤销或冻结操作。

发生下列情况之一的，依赖方可以向河北 CA 注册机构申请撤销或冻结订户证书：

a) 数字证书私钥泄露；

b) 数字证书中的信息有误或发生重大变更；

c) 订户数字证书超范围使用；

d) 数字证书主体消亡。

依赖方申请订户证书撤销或冻结的审批流程：

a) 依赖方持办理人身份证件及撤销或冻结申请到河北 CA 注册机构服务网点申请撤销或冻结证书。

b) 河北 CA 注册机构核实撤销或冻结申请原因及办理人身份。

c) 核验通过后，河北 CA 注册机构执行证书撤销或冻结操作。

发生下列情况之一的，河北 CA 可以强制吊销订户证书：

a) 订户证书信息有误或发生重大变更；

b) 订户提供的信息或材料造假；

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

c) 订户未支付服务费；

d) 订户主体消亡；

e) 订户超范围使用证书；

f) 订户证书私钥泄露或数字证书的安全性得不到保证；

g) 订户没有履行双方合同规定的义务，或违反本 CPS；

h) 法律、行政法规规定的其他情形。

河北 CA 强制吊销订户证书的审批流程：

a) 河北 CA 整理应予以吊销的风险证书名单。

b) 业务负责人复核，安全策略委员会负责终审。

c) 审批通过后，执行证书吊销或冻结操作。

4.9.2 请求撤销或冻结证书的实体

可请求撤销或冻结证书的实体，包括但不限于订户、受托人、依赖方或河北 CA。

4.9.3 请求处理

a) 河北 CA 提供 400 服务热线、投诉电话、服务网点现场受理、在线即时通讯、电子邮箱等便捷渠道，并记录影响证书或私钥安全的事件（如密钥遗失、泄密）。

b) 河北 CA 按照 §3.2 初始身份确认的要求，验证申请人的身份与权限，并做出是否受理的决定。

4.9.4 处理流程记录

河北 CA 保留证书撤销或冻结全部处理流程的相关信息。

4.10 证书状态信息服务

a) 证书状态信息服务方式：OCSP。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

b) 证书状态信息服务响应时间不超过 1 分钟。

c) 河北 CA 提供 7×24 小时连续不间断的证书状态信息查询服务，服务可用率不低于 99%。

d) 河北 CA 提供电话查询或邮件查询等备用查询机制。

4.11 停止使用认证服务

4.11.1 停止订户服务的情形

发生下列情形之一的，河北 CA 有权停止向订户提供电子认证服务，并终止相应的电子认证服务合同：

a) 订户主动申请：订户因证书到期不再续期、业务变更、私钥丢失或泄露、主体消亡（如企业注销）等原因，向 CA 机构正式提交停止服务申请的；

b) 订户违反义务：订户在证书使用过程中存在违反《电子认证服务协议》或相关法律法规的行为，包括但不限于提供虚假注册信息、违规使用证书、危及 CA 机构系统安全等；

c) 证书状态异常：经核实，订户的证书私钥发生泄露、被破解，或证书所含信息存在重大错误，继续使用将带来安全风险的；

d) 法律或监管要求：依据有权机关（如法院、工业和信息化部、公安部门）的正式文书要求，需停止对特定订户的服务；

4.11.2 处理停止服务请求的时限和方式

河北 CA 将在 24 小时内撤销证书，并将相关证书列入证书撤销列表（CRL），并确保 CRL 在下一个发布周期（不超过 24 小时）内更新，同时通过在线证书状态协议（OCSP）实时反映证书的“已撤销”状态。涉及订户私钥托管的，安全销毁订户签名私钥。

河北 CA 对证书申请、审核、签发、吊销等电子认证业务数据及合规审计日志予以归档留存，服务停止后至少保存五年。归档数据转移至离线、加密的归档存储介质中，实施严格的物理隔离与访问控制，确保数据安全。对超出保存期限

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

的归档数据，将采取多次覆写、物理粉碎等不可逆方式彻底销毁。用户证书对应的私钥在证书废止后立即安全销毁并留存审计记录，河北 CA 不保留任何用户私钥副本，且相关数据不得向第三方转移，仅法律法规强制要求的情形除外。

4.11.3 停止使用认证服务后的责任延续

停止使用认证服务后，河北 CA 与订户之间的部分权利义务关系并不立即终止，具体延续如下：

a) 证书使用责任延续：订户对其在证书撤销生效前使用证书所产生的一切法律后果承担全部责任。河北 CA 对撤销生效前基于有效证书所开展的认证服务承担相应法律责任。

b) 河北 CA 声明与保证的延续：对于证书撤销前已签发的、且订户在证书有效期内完成的电子签名，河北 CA 仍应按照原 CPS 的规定承担相应的证明责任和举证义务，包括在涉及相关签名有效性争议时提供必要的技术支持和审计记录。

c) 责任免除：证书撤销自 CRL 发布之时起生效，撤销生效后订户继续使用该证书所产生的一切后果，由订户自行承担，河北 CA 不承担任何责任。

d) 数据保存义务：尽管服务已停止，河北 CA 仍需按照法律法规要求，继续保存与订户相关的认证业务记录、审计日志和证书状态信息，保存期限不因服务停止而缩短。

4.11.4 停止使用服务的操作记录

河北 CA 对每一次停止使用服务的过程进行完整、真实、不可篡改的记录，确保可追溯、可审计。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

4.12 密钥托管与恢复

4.12.1 根证书私钥保管

河北 CA 根证书私钥不会托管给任何第三方机构或个人，并在自建的屏蔽机房中保管。

4.12.2 根证书密钥备份与恢复策略

河北 CA 根证书密钥的备份恢复策略采用五选三模式，根密钥在 HSM 内生成后分割为五个密钥分量，由不同密钥管理员分别存储于智能密码钥匙中，任何单一分量无法恢复根证书密钥。恢复时必须由至少三名密钥管理员同时到场，在 HSM 内完成密钥重构，全程遵循多人控制、职责分离与审计监督原则。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 基础设施

河北CA电子认证服务的技术设施位于河北省石家庄市桥西区红旗大街88号翰林观天下23号楼28层河北CA机房。物理建筑、机房环境和网络通信设施的建设标准包括：

a) GB/T 25056-2018《信息安全技术证书认证系统密码及其相关安全技术规范》

b) GB 9361-88《计算站场地安全要求》

c) GB 2887-89《计算站场地技术条件》

d) GB 6650-86《计算机机房用活动地板技术条件》

e) GB 50174-93《电子计算机机房设计规范》

f) GB 12190-2000《加密屏蔽机房安装设计规范》

g) GB/T 2887-2000《电子计算机场地通用规范》

h) GB 7450-1987《电子设备雷击保护导则》

i) GBJ 45-1982《高层民用建筑设计防火规范》

j) GBJ 79-85《工业企业通信接地设计规范》

5.1.2 分区管理与访问控制

5.1.2.1 技术设施内部的安全区域划分

河北CA机房场所实行分层访问的安全管理策略，按功能区域划分为四个区域：公共区、服务区、管理区和核心区。

a) 公共区

功能定位：网络最外侧边界，对接互联网，承载外网访问入口、入侵检测、

地址：河北省石家庄市桥西区红旗大街88号翰林观天下23号楼27层
客服热线：400-707-3355
网址：http://www.hebca.com

防火墙设备，供外部订户、公众发起证书查询、业务访问请求，是内外网第一道隔离边界。

安全防护：部署防火墙、入侵检测/防御、防病毒网关；仅开放业务必需端口，严格黑白名单；全程流量审计，阻断异常攻击；禁止内网设备直连，与服务区硬隔离。

b）服务区

功能定位：对外服务中间缓冲层，部署 OCSP、证书目录、Web 业务服务器，对外提供证书状态查询、业务受理接口，隔离外网与内部运维、核心密钥系统。

安全防护：独立安全域，双防火墙前后隔离；服务器最小权限运行，定期漏洞扫描；外网请求不得穿透至管理、核心区；所有对外接口国密加密传输，操作日志留存。

c）管理区

功能定位：CA 内部运维操作区域，部署注册、证书签发审计、业务管理终端，工作人员办理证书受理、业务审核、运维监控，仅内部授权人员接入。

安全防护：终端禁用外网、USB 外设管控；操作全程审计留痕；与核心区间单向访问控制。

d）核心区

功能定位：最高安全等级屏蔽机房，部署加密机、KMC 密钥管理、根签发服务器，存储、生成、保管 CA 根私钥、签名私钥，是密钥与证书签发核心资产区。

安全防护：独立电磁屏蔽机房，防拆自毁硬件；防尾随互锁门；7×24 小时高清视频监控；断外网物理隔离；禁止携带电子设备进入；密钥操作多人在场，全流程不可篡改审计，配套专用气体消防、恒温恒湿环境管控。

5.1.2.2 核心区和管理区的物理访问控制

机房核心区和管理区的物理访问实施“双人共管”与“双因素认证”的强制访问控制策略，并记录访问信息。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.1.3 电力保障

河北 CA 机房采用双路市电保障，同时机房部署在线式 UPS 不间断电源，市电断电时可无缝切换供电。UPS 搭配蓄电池组保障核心设备短时持续运行，持续供电时间不低于 8 小时，预留充足断电处置缓冲时间。配备 UPS 远程监控系统，实时监测电压、负载、电池状态，异常自动告警。定期开展 UPS 放电、切换演练，维护蓄电池，保障断电应急功能可靠有效。

5.1.4 门禁与监控

为了保证本系统的安全，河北 CA 采取了严密的隔离、控制、监控手段。机房部署门禁、侵入检测、视频监控、红外监控等安防系统。

服务区、管理区、核心区的视频监控记录和门禁访问记录保存期为 6 个月，并于销毁前进行审计，形成的审计报告存档备查。

5.1.5 灾备

河北 CA 对离线根密钥、证书申请记录、用户身份查验记录、证书数据、黑名单数据、系统配置文件、应用安装包、系统运行日志等重要数据实施异地备份，备份数据保存于河北省石家庄市桥西区休门街 3 号滨江优谷 1706 室机房内。该异地机房与主机房分属不同变电所电网、不同通信网络节点，两地直线距离约 5km。该距离选址经技术评估，可在满足业务连续性恢复时效要求的前提下，有效规避同区域重大灾害导致的单点故障风险。

5.1.6 环境保障措施

机房配备温湿度控制和防水措施，保持相对湿度在 40%-60%范围内，保持温度在 18-28° C 范围内。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.1.7 消防措施

机房配备联动的火灾自动报警系统和配备自动气体灭火系统，包含温度和烟雾检测功能，同时配备 2 台专用空气呼吸器，每年一次进行消防安全检测。

5.1.8 设备管理

河北 CA 建立设备台账，设备台账包含每台设备的责任人、使用状态、维护周期和报废标准；每年进行设备盘点和核对，保证设备实际情况与设备台账相符。

5.1.9 存储媒体管理

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

5.2 操作过程控制

5.2.1 可信角色

所有涉及证书认证系统操作、维护与管理的都是可信角色，必须由可信人员担任。

各可信角色职责、任职要求、身份验证机制及最小人员配置如下：

a） 系统管理员

岗位职责：负责系统策略配置、用户与权限管理等工作。

任职要求：熟悉 CA 系统架构与安全配置规范，具备系统策略、账号权限管控能力，可保障系统合规安全运行。

身份验证机制：采用基于数字证书的双因素认证方式。针对系统策略配置、密钥操作、系统变更等高风险关键操作增设二次身份核验及双人复核机制。

最小人员配置：不少于 3 人。

b） 技术运维员

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

岗位职责：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工作。

任职要求：掌握机房、网络、服务器运维专业技能，可完成日常监控、故障排查，保障基础设施稳定运行。

身份验证机制：机房门禁访问采用双因素身份验证机制，服务器及系统软件登录采用具有一定复杂度的账号密码进行身份验证。

最小人员配置：不少于 3 人。

c）数据库管理员

岗位职责：负责数据库进行日常运维、性能优化及数据备份等工作。

任职要求：精通数据库运维、优化及备份恢复技术，可落实数据安全管控，保障业务数据完整安全、可恢复。

身份验证机制：采用具有一定复杂度的账号密码进行身份验证。

最小人员配置：不少于 1 人。

d）系统审计员

岗位职责：负责系统和网络日志的审计、管理、审计报告生成等工作。

任职要求：熟悉系统、网络日志审计规范，具备风险排查与审计报告编制能力，可落实全流程审计管控。

身份验证机制：采用基于数字证书的双因素认证方式，并使用多人操作机制。

最小人员配置：不少于 2 人。

e）密钥管理员

岗位职责：负责根证书密钥材料管理、根证书密钥生存周期管理等工作。

任职要求：熟知根证书密钥管理规范，掌握密钥全生命周期管控流程，具备极强的安全保密与合规操作意识。

身份验证机制：采用基于数字证书的双因素认证方式，并使用多人操作机制。

最小人员配置：不少于 5 人，严禁单人独立操作密钥。

f）业务操作员

岗位职责：负责证书申请的受理、审核，订户的身份与意愿鉴证工作。

任职要求：熟悉证书业务流程与订户核验标准，具备严谨的合规审核能力，可有效规避证书违规签发风险。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

身份验证机制：采用基于数字证书的双因素认证方式，并使用双人复核机制。

最小人员配置：不少于 3 人。

g）客户档案管理员

岗位职责：负责客户证书相关档案资料的归档与保密等工作。

任职要求：掌握档案归档与保密管理制度，可规范完成档案全流程管理，保障档案完整、保密、可追溯。

身份验证机制：系统数据访问采用基于数字证书的双因素认证方式。

最小人员配置：不少于 1 人。

h）运营审计员

岗位职责：负责对签发证书、客户服务等核心业务进行独立审计等工作。

任职要求：熟悉 CA 核心业务流程，具备独立审计与风险研判能力，可精准排查业务运营与操作风险。

身份验证方式：采用基于数字证书的双因素认证方式，并使用双人复核机制。

最小人员配置：不少于 2 人。

i）安全策略委员会

岗位职责：规范及策略文档管理、组织制度年度评审，审批重要操作、流程及安全相关变更，开展年度运营风险评估，并妥善保管会议及决议资料，保障电子认证服务合规安全、可追溯。

任职要求：熟悉电子认证、信息安全及商用密码管控规范，具备制度建设、风险评估、合规评审及安全事项审批统筹能力。

身份验证机制：安全事项审批采用电子签名方式验证。

最小人员配置：不少于 5 人。

j）CPS 起草小组

岗位职责：依照国家及行业规范编制、修订、管控 CPS 文件，完成审核报备与年度评审优化，紧跟政策标准动态，保障文件合规适配业务。

任职要求：熟练掌握电子认证、商用密码法规标准，可独立完成 CPS 编制、备案、迭代优化及政策合规适配工作。

身份验证机制：CPS 更新、发布申请采用电子签名方式验证。

最小人员配置：不少于 3 人。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.2.2 职责分离

河北 CA 遵循职责分离的原则，所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色实现双人操作或复核机制；涉及业务连续性相关操作（运维、鉴证、审计等）的角色按工作量设置冗余，确保任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止互相兼任：

a) 系统管理员、技术运维员、数据库管理员、系统审计员的角色不相互兼任。

b) 同一证书业务的录入与审核环节由不同业务操作员完成。

c) 业务操作员、客户档案管理员、运营审计员不相互兼任。

d) 密钥管理员与系统管理员、技术运维员不相互兼任。

e) 密钥管理员与安全策略委员会成员外的其他可信角色不互相兼任。

5.3 人员控制

5.3.1 可信人员资格、经历与背景要求

所有可信角色的资格、经历与背景要求包括但不限于：

a) 从业经历调查要求和无犯罪记录；

b) 具备履行岗位职责所必需的专业技能要求；

c) 签署具有法律约束力的保密协议，承诺不得私自保存、复制或泄露电子认证服务的所有秘密或敏感信息；

d) 签署劳动合同。

5.3.2 可信人员培训要求

河北 CA 建立覆盖所有可信角色的持续培训体系，并规定：

a) 岗前培训：所有可信人员上岗前需完成不少于 20 学时培训并通过考核；

b) 持续培训：每年至少接受一次培训，每人每年培训时长不少于 20 学时，

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

并通过考核；

c) 培训内容至少包括：

1) 国家关于电子认证服务的法律、法规、标准及程序；

2) 岗位职责统一要求及各角色工作要求；

3) CA 管理政策、制度及办法等；

4) PKI 和密码技术基础知识；

5) CP、CPS 政策及相关标准和程序；

6) CA 安全管理策略和机制；

7) 身份查验和审核策略和程序；

8) CA 运营体系；

9) CA 技术体系；

10) 灾难恢复和业务连续性管理。

5.4 审计日志程序

5.4.1 记录范围

河北 CA 在运行系统中，记录所有与物理环境安全、网络安全、密码安全、证书处理系统应用与数据安全、人员操作行为、操作系统和数据库运行安全等相关事件，以备审查。

河北 CA 持续、完整地记录关键操作与事件，包括但不限于：

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

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

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

d) 网络安全的事件：包括防火墙、路由器、入侵检测安全设备记录的告警

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

信息，以及针对被攻击事件识别与相应处理过程、结果等。

e) 证书生命周期关键过程：记录证书申请、审核、签发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均明确记录。

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

5.4.2 记录内容

每个事件记录都包含时间、类型、内容、操作人、作用对象实体（如密钥、系统或证书等）及结果。对系统的关键操作由操作人进行电子签名。

5.4.3 保存期限

系统日志至少保存至相关证书失效后五年，并实施严格的访问控制以防篡改或删除。

5.4.4 日志审计内容

核实系统和操作人员的合规性包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

5.4.5 审计周期

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

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.5 记录归档

5.5.1 归档范围

河北 CA 归档记录范围包括：

a) 证书申请材料和订户意愿记录；

b) 所有审计日志；

c) 密码设备全生存周期管理记录；

d) 密码设备的日常操作与使用记录；

e) 根证书或密钥生存周期管理相关的全部记录；

f) 证书认证系统运行日志；

g) 已识别的安全事件及处置记录；

h) 证书认证系统关键操作日志；

i) 电子认证服务过程中其他操作记录。

5.5.2 保存期限

订户相关档案、系统日志和审计记录至少保存至证书失效后五年。

5.5.3 保护措施

河北 CA 对各种电子、磁带、纸质形式的归档文件，都有安全保护措施和严格的管理程序，确保归档文件不会被损坏，防止非授权的访问、修改、删除或其他的篡改行为。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。对电子归档文档进行电子签名，保证数据的完整性，防止被修改或置换。

河北 CA 对电子归档记录进行备份管理，在安全机制上保证禁止对电子归档文件及其备份进行删除、修改等操作，并由审计人员对归档记录的管理情况进行检查，确保各项规定严格落实执行。

纸质资料保存于专用档案室，由档案管理员按照《河北 CA 客户档案管理规

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

范》进行管理，防止非授权访问、档案资料修改、未经审批销毁等行为的发生。

5.5.4 档案管理机构

河北 CA 设立专门的档案管理机构统一管理归档记录。

5.5.4.1 档案管理机构职责

a) 负责全面归集河北 CA 各类归档资料，严格对照归档范围做到应归尽归、完整无缺。
b) 严格执行档案保存管理要求，确保订户档案、各类日志等资料留存时长不低于证书失效后五年。
c) 负责电子、纸质全类型档案的分类存储与日常运维，落实档案规范化保管制度。
d) 严格落实档案权限管控机制，规范授权访问、合规查阅操作，确保操作全程留痕可追溯。
e) 规范档案调取、使用、期满销毁全流程审批管理，保障档案管理合规可控。

5.5.4.2 操作规范

a) 电子档案数据库采用物理或逻辑隔离部署，严禁与外界开展任何信息交互。
b) 纸质档案统一存入专用档案室，完成规范化编号、分类存放与日常保管。
c) 建立档案到期预警机制，严格执行证书失效后五年的最低保存期限要求。
d) 严格执行档案授权查阅、分级审批登记制度，规范查阅流程。
e) 全程登记查阅人员、查阅事由、查阅时间及档案用途等信息，做到全程可追溯。
f) 严禁查阅过程中私自复制、拷贝、篡改、外泄各类归档档案资料。
g) 档案查阅使用完毕后，及时核对复位、规范归档存放。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.5.4.3 安全要求

a) 所有电子归档文件必须加注电子签名锁定数据内容，定期校验档案及签名有效性，及时处置数据异常与篡改问题。
b) 遵循最小权限原则分配岗位操作权限，所有档案操作全程日志留痕、可审计追溯。
c) 人员岗位变动时须及时回收对应操作权限，严禁权限转借、私自授权他人操作。
d) 电子档案存储系统采用隔离机制，杜绝外部入侵及非法数据交互风险。
e) 专用档案室实行封闭式管理，配备防盗、防火、防潮等防护设施，严格管控人员出入。
f) 定期巡检各类存储介质，及时排查更换故障设备，保障存储环境安全稳定。
g) 严禁私自删改、移动、外泄各类归档资料，严禁未经审批擅自销毁档案。
h) 所有档案管理操作必须履行审批登记流程，全程留痕，工作人员严格遵守档案保密制度。
i) 制定档案安全应急预案，有效应对数据篡改、丢失、设备故障等突发安全风险。
j) 常态化开展安全审计工作，主动排查、闭环整改档案各类安全隐患。
k) 档案期满后须经双重核查审批方可启动销毁流程，全程登记留痕。
l) 纸质档案采用粉碎方式销毁，电子档案彻底清零核验，杜绝数据残留与信息外泄。

5.6 电子认证服务机构根证书密钥更替

电子认证服务机构根证书密钥更替指根密钥到期、存在泄露风险、算法升级、合规要求等情形，切换为新密钥签发下级证书、CRL 的操作。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.6.1 密钥更替程序

a) 密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，具体见§6.2；

b) 根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；

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

5.6.2 密钥更替的时间

a) 紧急更替：发现密钥泄露或存在安全隐患，立即启动密钥更替程序；

b) 到期更替：在密钥到期前二年完成密钥更替。

5.7 损害与灾难恢复

5.7.1 业务连续性目标

当遇到自然灾害、系统故障、安全事件（包括密钥泄露、黑客攻击、病毒爆发）及人为操作失误等导致服务中断或安全受损的事件。河北 CA 将启动灾难恢复应急预案，CA 机构承诺，在发生灾难性事件导致认证服务中断时，将按照以下指标执行恢复。

故障类型	故障内容	恢复时间目标 RTO	恢复点目标 RPO
证书库损害	证书库损害	≤24 小时	数据丢失时间范围不超过 24 小时
根密钥损害	根密钥损坏	≤2 小时	恢复到正常状态
	根密钥泄露	≤5 天	业务恢复到正常状态
其他关键资产	物理设施	≤24 小时	恢复正常服务

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

	计算资源单点故障	≤5 分钟	恢复正常服务
	网络环境单点故障	≤24 小时	恢复正常服务
	软件或数据	≤2 小时	恢复正常服务
	其他密钥数据	≤2 小时	恢复正常服务

5.7.2 恢复流程

5.7.2.1 证书库的恢复过程

a) 重建安全运行环境的流程：重建网络安全环境，重建主机运行环境。

b) 生成受影响并被撤销的证书列表：

1) 将备用证书库进行恢复

2) 依托备份数据、运行日志及证书操作记录开展交叉核验，

3) 对需要吊销的证书进行吊销，重新生成 CRL。

c) 对订户密钥的处理方式：对于用户持有签名私钥的，仍然由用户持有，河北 CA 不进行处理。对于私钥委托河北 CA 保管的，河北 CA 通知订户进行密钥更新并吊销原有证书。

d) 重新向订户提供实体公钥证书的要求和流程：按照证书生存周期操作要求和流程向订户提供证书。

5.7.2.2 根密钥损害的恢复过程

a) 重建安全环境的流程：重建网络安全环境，重建主机运行环境，部署根密钥业务系统，如根密钥损害未泄密，从根密钥备份数据中恢复根密钥。如根密钥泄密，则立即启动应急更替程序，按§5.7.3 执行根私钥应急处理。

b) 为订户重新签发公钥证书：使用新的根密钥重新签发订户证书。

c) 向订户提供新的公钥证书的流程：河北 CA 通过网站告知、应用软件提示、短信、电话、邮件等方式通知订户更新证书。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.7.2.3 其他关键资产恢复过程

河北 CA 对业务系统及其他重要系统的资源、软件、数据及其他密钥数据进行了备份，并制定了相应的应急处理流程。当发生网络通信资源毁坏、计算机设备不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，河北 CA 将按照灾难恢复计划实施系统、配置及数据的恢复。

对于电力系统、服务器、网络设备等硬件设施河北 CA 采用将启用备用设备快速完成灾难恢复，同时制定相应的流程规范指导技术运维人员快速实施备用设备启用，保障并恢复服务正常运行。例如：配备 UPS 供电系统、备用服务器、备用密码机、备用网关等。

5.7.3 根私钥应急处理

根私钥泄露属于一级特大安全事件，事发须即刻启动最高级应急响应，以阻断证书伪造、非法验签风险，全面重建全域 PKI 信任体系为核心处置目标；常态化落实应急管控工作，每年组织 1 次根私钥泄露全流程专项应急演练，迭代优化应急流程、补齐处置管控短板。具体应急处理流程、响应时效、责任人、处置步骤和事件上报要求如下：

a) 事件核验及应急响应启动（0-30 分钟）

核验告警信息，判定河北 CA 根私钥泄露是否属实。确认属实后，立即启动最高级响应机制。由安全策略委员会、系统管理、技术运维、密钥管理、业务管理、运营审计等人员组建专项应急小组，具体责任分工如下：

1) 安全策略委员会负责统筹安排。

2) 系统管理、技术运维人员负责风险控制、根密钥替换。

3) 合规部负责全程监督及录音录像。

4) 密钥管理小组负责密钥相关操作。

5) 业务协调组负责对业务系统、依赖方、订户的通知和业务风险预警。

6) 合规部负责事件上报、各项流程合规审查。

b) 风险控制与证据固定（0-30 分钟）

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

对涉事设备立即执行断电、物理断网隔离操作，固定泄露全链路日志、封存涉事设备完成证据留存。

c）事件上报（45 分钟-2 小时）

核验根私钥泄露属实后，合规部 15 分钟内上报单位主要负责人及属地监管部门，2 小时书面上报工业和信息化部和国家密码管理局。同时负责根密钥更替后的上报。

d）河北 CA 根密钥紧急废止（0-4 小时）

河北 CA 密钥小组在 CA 系统中使用新的根密钥生成新的河北 CA 根证书请求，向国家密码管理局申请吊销河北 CA 原根证书，生成根证书撤销列表 ARL，并签发新的河北 CA 根证书。

同步下发待吊销预警，告知所有依赖方、下游订户拦截原根证书验签、阻断伪造证书访问。

e）河北 CA 取得国家新发根证书后落地替换（4 小时-业务全恢复）

1）在隔离安全机房，使用国家密码管理局签发的全新河北 CA 根证书，重新签发原旧根下所有订户证书，全程由审计人员录音录像、步骤留痕归档。

2）业务协调组通知全部依赖单位、业务系统卸载旧根证书，加载河北 CA 新根证书并更新 CRL；同步通知所有下游订户更换新根签发的业务证书。

5.7.4 事件报告

见§5.9 重大事项报告。

5.7.5 定期验证

河北 CA 定期验证备份的设备、数据可用性和恢复流程的有效性，包括备份恢复测试和功能验证，每年至少开展一次包括证书库、系统数据、密钥备份等在内的全面灾难恢复演练，并形成记录。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.8 电子认证服务机构终止

河北 CA 终止运营时，将严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及其他相关法律规定的步骤终止运营。具体流程和通告机制如下：

a) 起草并发布 CA 终止声明，至少提前九十日通知订户、依赖方等相关实体，至少提前六十日向主管部门报告；
b) 具有资质的电子认证服务业务承接单位并签署承接协议，明确约定承接机构的工作范围与责任；
c) 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
d) 停止证书状态服务并归档相关数据；
e) 停止认证中心的服务并归档相关数据；
f) 停止密码服务设备并归档相关密钥数据；
g) 及时撤销或冻结业务管理员和业务操作员的操作权限；
h) 对所有存档文件记录进行整理和封存；
i) 对所有敏感文档和数据进行安全处理和封存；
j) 清除主机和密码硬件设备中的敏感数据；
k) 所有涉及 CA 运营的数据、密钥安全地转移至承接单位后进行安全销毁。

5.9 重大事项报告

5.9.1 重大事件类型及判断标准

重大事件包括但不限于以下形式：

a) 证书认证系统迁移或改造

证书认证系统软件、网络、部署出现以下任意之一的重大改变：

1) 机房迁移，或机房内服务区、管理区或核心区划设范围改变；
2) 变更电子签名认证证书签发逻辑；
3) 新增远程证书注册子系统；
4) 新增、更改或者删除用于签发电子签名认证证书的证书链；

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5） 其他对电子认证服务安全、用户资料安全有影响的改变。

b） 重大安全事故

电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形，具体包括：

1） 证书签发及验证服务连续停机时间超过 24 小时；

2） 发生根证书密钥等关键数据泄露；

3） 持续或较大范围未经授权的私钥访问记录或其他异常活动；

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

c） 订户信息泄露事件

电子认证服务机构存储的订户身份信息、证书申请资料等敏感数据被泄露的情形，具体包括：

1） 个人信息泄露事件影响范围较广，造成经济损失或客户投诉；

2） 数据丢失导致无法恢复证书状态信息。

d） 合规性事件

电子认证服务机构内部人员违反操作规范、安全管理制度或法律法规，进行违规的证书签发、管理等行为；业务运营不符合相关法律法规、行业标准或监管要求，受到相关监管部门处罚、审计未通过或引发社会舆论关注；具体包括：

1） 涉及电子认证服务的司法判定；

2） 收到行政部门违规通知或处罚决定。

e） 人力资源类事件

核心管理层一个月内集体离职、大规模劳动纠纷、重大职场安全事件等。具体包括：

1） 涉及 2 名及以上管理层人员离职或 10%以上可信人员的离职；

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

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

5.9.2 报告的程序、时限与内容

a) 内部紧急报告程序

1) 任何员工发现或知悉上述重大事件时，应立即在 30 分钟内向所在部门负责人及信息安全主管口头报告。报告内容包括：事件发生时间、地点、简要情况、已采取的初步措施。

2) 部门负责人或信息安全主管接到报告后，应立即核实情况，并在 1 小时内向公司管理层（总经理或分管安全副总经理）报告。核实报告内容包括：事件详细情况、初步判断的原因、当前影响范围、已采取的应急处置措施、需要协调的资源。

b) 向监管部门报告程序

1) 应在 24 小时内向工业和信息化部、国家密码管理局以及其他相关管理部门提交书面《重大事件情况报告》。书面报告应经公司法定代表人签字或加盖公司公章，内容包括：

- 事件基本情况：发生时间、地点、经过、发现方式；
- 事件原因分析：初步原因及进一步计划；
- 影响评估：受影响用户数量、范围、经济损失预估、数据泄露情况等；
- 应急处置措施：已采取的措施及效果、服务恢复情况；
- 后续工作计划：根本原因调查、整改措施、预防机制；
- 附件材料：相关日志、记录、截图等证据材料。

2) 事件处置结束后，应在 3 个工作日内向工业和信息化部、国家密码管理局以及其他相关管理部提交总结报告，内容包括：事件最终原因、处置过程、整改措施完成情况、责任追究情况、经验教训及制度完善情况。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6 认证系统技术安全控制

6.1 技术安全管理制度要求

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

6.2 密钥对的生成和安装

6.2.1 根密钥对的生成和安装

河北 CA 根证书密钥对的生成与安装按以下要求执行：

a) 根证书密钥对在河北 CA 屏蔽机房中存放、使用。该屏蔽机房按照《GB 12190-2000 加密屏蔽机房安装设计规范》建设，依据《GJB 5792-2006 军用涉密信息系统电磁屏蔽体等级划分监督和测量方法》进行检测，并且定期进行复检，确保根证书密钥对不会因电磁原因泄露。根证书密钥对由国家密码管理局认可的硬件密码设备：服务器密码机生成。

b) 生成、备份、恢复、销毁过程实施五选三多人控制机制，操作在安全策略委员会授权下进行，并通过录音录像方式全程记录，保存期限不少于操作完成后十年。

6.2.2 订户密钥对的生成和交付

订户签名密钥对的生成、交付及控制方式符合以下要求之一：

a) 由订户持有的符合国家安全标准的密码模块（如 USBKey、服务器密码机、协同签名模块等）产生和存储；

b) 对于由河北 CA 产生、保管的订户签名私钥，河北 CA 将采用技术手段保证订户对私钥的独占控制权。具体的技术措施包括：

1) 订户私钥由河北 CA 采用国密局检测认证通过的密码模块生成，并在密码模块中运算，以加密的方式进行存储，不以明文形式出现在密码

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

模块之外。

2) 私钥存储时与订户的激活数据（包括但不限于手机号、生物特征等）进行一对一关联。用户每次使用私钥时，均需要订户主动提供激活数据，保证每次私钥调用均在订户的参与下才能完成。

3) 河北 CA 不会将托管私钥的控制权交由除订户之外的任何第三方应用，防止应用劫持订户私钥。

河北 CA 将完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期不少于证书失效后五年。

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

河北 CA 根证书私钥保护按照以下国家相关标准进行保护：

a) 根证书私钥生成使用通过国家密码主管部门认可的服务器密码机型号 SJJ1862-G，符合《GB/T 37092-2018 信息安全技术密码模块安全要求》密码模块安全二级的要求。

b) 根证书私钥实施严格的分割保护机制，生成、备份、恢复均采用五选三多人控制机制，单人无法获取完整私钥。

c) 根证书私钥备份由密钥管理员分别保存在河北 CA 具有多重安全防护机制的屏蔽机房保险柜中。

6.3.2 订户私钥保护和密码模块工程控制

订户签名私钥保护符合下列要求之一：

a) 订户签名私钥由订户持有

河北 CA 在电子认证服务协议中明确规定订户应妥善保管激活数据（包括口令、短信验证码、人像），严禁泄露、转借他人。

b) 河北 CA 接受订户委托保管订户签名私钥

1) 河北 CA 采用的电子签名模式包括：订户生物特征、订户预留手机短

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

信验证码、PIN 码等。

2) 采用的安全措施包括：

- 河北 CA 定期提醒订户进行 PIN 码修改、进行弱口令校验、具有防暴力破解功能。
- 订户签名私钥加密保存
- 签名私钥加密数据进行定期备份和恢复演练
- 对以上安全措施进行定期安全评估。

c) 每次签名私钥调用必须获得订户的明确授权，并完整保存授权记录。

d) 河北 CA 通过网站、应用 APP 等方式向订户提供关于签名私钥及激活数据安全使用的指导与建议。

e) 河北 CA 提供订户签名私钥托管服务时，采用的电子签名模式和控制措施符合相关标准或采用经主管部门认可的其他方式。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

公钥证书签发后立即归档，最大间隔不超过 24 小时。

6.4.2 证书操作期和密钥对使用期限

a) 证书操作期规定：指证书载明的 NotBefore 至 NotAfter 时段，为证书合法生效、可用于签名验签、加密解密、身份认证的操作周期。河北 CA 根证书有效期为 2012 年至 2032 年，有效期 20 年。订户证书有效期不超过 5 年，到期自动失效，签名私钥不可用于电子签名。证书到期前，订户可申请续期或重签。

b) 各类密钥对使用期限：

1) 根证书密钥对：河北 CA 根证书密钥对有效期为 2012 年至 2032 年，有效期 20 年。机构将提前 2 年启动根证书续期或更新工作，原根证书到期后，将不再签发各级 CA 证书及订户证书，后续全部使用更

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

新、续期后的新根证书开展证书签发业务。河北 CA 根证书到期后，其对应私钥不再用于签发新的订户证书。

2) 订户证书密钥对：订户证书密钥对最长有效期不超过 5 年，订户证书密钥对累计有效期超过 5 年的，订户需重新生成密钥对并提交新的证书申请，不得在原密钥对基础上续期。

3) 其他各类密钥对：河北 CA OCSP 响应者密钥对有效期为 2 年。

6.5 激活数据

6.5.1 激活数据的生成和传输

激活数据是私钥保护的密码，可以是 PIN 码、手机验证码或者生物特征信息。

a) 河北 CA 根密钥激活数据的生成：

由密钥管理员采用五选三的方式，按照服务器密码机使用说明生成。

b) 订户激活数据的生成和传输方式：

1) 激活数据由河北 CA 调用密码模块生成，并通过短信、系统提示等方式安全地传输给订户。

2) 激活数据由订户自行生成。

6.5.2 激活数据的使用和保管

a) 河北 CA 根密钥激活数据的使用和保管：

河北 CA 根密钥激活数据使用时由密钥管理员采用五选三的方式进行使用和保管。

b) 订户激活数据的使用和保管：

1) 河北 CA 向订户提供激活数据的正确的使用方式。

2) 订户激活数据由订户自行保管，河北 CA 并不保管订户激活数据。

3) 订户激活数据丢失、遗忘，可向河北 CA 申请进行申请，订户身份核验通过后可重置激活数据。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

6.5.3 激活数据的销毁

a) 河北 CA 根密钥激活数据的销毁

河北 CA 根密钥激活数据销毁时由密钥管理员采用五选三的方式按照服务器密码机销毁私钥的方式进行激活数据销毁。

b) 订户激活数据的使用和保管

河北 CA 不提供单独的激活数据销毁服务，订户可通过申请证书撤销或对密钥存储介质进行物理破坏的方式进行激活数据的销毁。

6.6 计算机安全控制

河北 CA 建立并实施符合 GB/T 25056 中 8.2 要求的计算机安全控制体系。包括但不限于：

a) 至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；
b) 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；
c) 对所有服务器和操作终端安装杀毒软件；
d) 病毒库每月进行更新，遇重大安全威胁时立即升级；
e) 每月进行一次病毒扫描。

6.7 生存周期安全控制

河北 CA 建立并实施符合 GB/T 25056-2018 中第 10、11、12 章要求的生存周期安全控制体系。

6.8 网络安全控制

河北 CA 建立并实施符合 GB/T 25056-2018 中 5.3.8 要求的网络安全控制体系。包括但不限于：

a) 网络结构满足 GB/T 25056-2018 附录 A 中 B/S 连接模式；
b) 对所有 Web 服务配置防火墙、Web 应用防火墙、入侵检测系统等网络安

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

全防护措施；

c) 建立并维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致；

d) 网络访问控制：

1) 限制证书注册子系统必要模块以外的系统或终端访问证书签发子系统和数据库；

2) 禁止不特定的外部系统或终端访问证书注册子系统和数据库。

e) 网络监控：

1) 每日对系统日志进行分析；

2) 分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9 时间戳

河北 CA 未部署时间戳服务。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

河北 CA 签发的所有证书包括电子签名认证证书均采用 X.509 V3 证书格式，格式符合 GB/T 20518 的要求，包括但不限于：

a) 支持的数字证书格式版本号；

b) 密码算法对象标识符；

c) CA 和订户的名称；

d) 证书策略对象标识符，其中包含主管部门制定的相应等级证书策略 OID 或河北 CA 制定遵循的证书策略 OID（见§1.5.1）；

e) 证书序列号；

f) 证书有效期；

g) 订户的电子签名验证数据；

h) CA 的电子签名。

7.2 证书撤销列表

河北 CA 签发的证书撤销列表（CRL）采用 X.509 V2 格式，符合 GB/T 20518-2018 中 5.3 的要求。

7.3 在线证书状态协议

河北 CA 在线证书状态服务符合 GB/T 19713-2025 中第 7 章的要求。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

8 认证机构审计及相关评估

8.1 审计评估制度

河北 CA 已制定审计评估机制，制度内容包括但不限于：

8.1.1 审计评估的类型

包括认证业务审计和全面符合性评估。

8.1.2 执行审计评估的频率，或是引发评估事件的条件

a) 根据《中华人民共和国电子签名法》《电子认证服务管理办法》等相关法律法规的要求，接受上级主管部门每年一次的评估和检查。
b) 根据国家相关要求和本 CPS 的规定，河北 CA 按照内部审计评估制度，每月进行一次认证业务审计，每年至少执行一次全面符合性评估，包括对河北 CA 和其他关联服务机构的审计评估。
c) 当河北 CA 怀疑存在电子认证服务风险时，由安全策略委员会可随时安排进行审计。

8.1.3 参与执行审计评估人员的专业背景

在进行内部审计评估时，河北 CA 要求评估人员至少具备安全审计的相关知识，熟悉本 CPS，并具备计算机、网络、信息安全等方面的知识和实际工作经验。

8.1.4 审计评估所涵盖的主题和评估的方法

审计评估的主题包括：物理基础设施安全、密钥与证书全生命周期管理、人员权限管控、系统密码安全、证书业务及依赖方合规、风险应急与文档管理。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

采用的评估方法包括：文档资料核查、现场实地勘查、系统技术检测、业务流程模拟、抽样定量核验、合规对标打分等多类评估方法，从制度、现场、人员、技术、流程多维度验证 CPS 体系合规性与安全管控有效性。

8.2 认证业务审计

认证业务审计方式，包括但不限于：

a) 审计周期：每月一次。

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

c) 审计采用抽样审计方式，审计抽样率为 3‰。

d) 对于审计发现的问题，通知相关部门和人员及时整改，并跟踪整改落实情况。

8.3 全面符合性评估

符合性评估方式，包括但不限于：

a) 评估周期不少于每年一次。

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

c) 审计采用抽样方式，抽样率不低于 3‰；

d) 对于审计发现的问题，通知被审计部门及时整改，并跟踪整改落实情况；在 1 月底前将上一年度符合性评估报告报送主管部门。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9 法律责任和其他业务条款

9.1 费用

河北 CA 开展了服务成本核算并制定价格策略。河北 CA 向用户收取证书签发、续期、密钥更新、证书变更等服务费用，具体收费标准在数字证书申请的实际业务场景中公布，双方另有约定的从其约定。

9.1.1 退款规定

a) 证书正式交付前，因订户原因主动放弃证书申请，或因河北 CA 原因导致证书无法在约定时间内交付的，订户可申请退款。
b) 因河北 CA 原因导致证书所载信息与订户申请内容不一致的，订户可申请退款。
c) 其他情况均不予退款。

相关退款规定在订户协议中进行公布。

9.2 财务责任

河北 CA 预留了与业务规模相适配的赔付专项备用资金，资金保障额度不低于上一年度营业收入的 1.5%，资金由经营收入产生，由财务部门建立单独备用金账户保管。

9.3 业务信息保密

9.3.1 保密信息的范围

保密信息的范围包括但不限于以下方面：

a) 在双方披露时标明为保密的；
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；

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

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。

对于河北 CA 保密信息的范围包括但不限于以下方面：

a) 最终用户的私人签名密钥；

b) 保存在审计记录中的信息；

c) 年度审计结果；

d) 除非有法律要求，由河北 CA 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。

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

9.3.2 非保密信息的范围

不属于保密的信息包括但不限于以下方面：

a) 信息主体同意公开的信息不属于保密信息。

b) 依据法律、行政法规规定可以公开的信息，河北 CA 可以选择公开。

c) 订户数字证书相关的信息可以通过河北 CA 目录服务等方式向外公布，但河北 CA 认为涉及订户保密信息的除外。

d) 其他可以通过公共、公开渠道获得的信息。

9.4 个人隐私保护

依据相关法律、法规，河北 CA 在受理客户申请证书及相关电子签名业务时需由证书申请人及/或受托人提供相关个人信息。其中个人信息包括：姓名、联系方式、身份证号、地址和身份证（原件及/或任何形式的复本）等个人隐私信息。《河北 CA 电子认证业务规则》有关用户个人信息保护条款的完整内容见河北省电子认证有限公司网站公布的《个人信息保护政策》。河北 CA 针对用户隐私信息提供如下保障措施。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.4.1 隐私保密方案

在数字证书生命周期中，河北 CA 在用户个人隐私信息的收集、使用、存储环节中，采取有效手段，保护个人隐私信息。

河北 CA 保护证书申请人所提供的、证明其身份的资料。河北 CA 采取必要的安全措施（如重要信息查阅权限控制、加密存储、数据备份等），防止证书申请人资料被遗失、盗用与篡改。

河北 CA 将实施信息安全管理制度以及行业通行的安全技术和程序来确保用户的个人信息不被丢失、泄露、篡改、毁损或滥用。

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，通常不认为是隐私信息，法律或行政法规另有规定的除外。

9.4.4 用户个人信息的收集

根据《电子签名法》第二十条规定，河北 CA 作为合法的第三方电子认证企业，在受理用户（含自然人个人以及公司法人与非法人组织）申请数字证书时有权对用户的身份进行核实。河北 CA 要求用户即证书申请人申请证书时通过纸质申请表、电子申请表、证书服务系统等方式提供其能够证明其真实身份的证明材料。河北 CA 在《证书申请表》等相关协议中已明确告知用户河北 CA 对用户包含但不限于用户个人的姓名、性别、年龄、身份证号码、家庭住址、联系方式等信息进行收集。

与河北 CA 建立证书服务合作的合作方，河北 CA 要求合作方建立收集用户个

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

人信息的管理制度，要求合作方在开展业务过程中遵守合法、正当、必要的原则，以书面形式明确告知用户收集个人信息的目的、方式和范围，并征得用户书面同意。

河北 CA 不会以非公司名义或授权员工个人收集用户个人信息；亦不会对与电子认证业务无关及非必要的个人信息进行收集。

9.4.5 个人信息的存储

河北 CA 将收集到的用户个人信息统一录入证书用户管理系统。河北 CA 建立独立的机房设备存储已收集到的用户个人信息，采取严格的技术手段对存储的数据信息进行加密处理，确保用户个人信息不被窃取、泄露，但该等措施并不排除在河北 CA 的数据信息存储系统受到恶意黑客入侵等特殊情况及地震、洪水等不可抗力的自然因素而可能发生数据信息泄露的风险。

9.4.6 用户个人信息的使用

河北 CA 不会在与用户自身使用证书服务及应用无关的系统或场合使用证书用户个人信息。发生下列情形之一的，河北 CA 将依法提供用户个人相关信息：

a） 基于国家法律、行政法规、规章的规定而提供的；

b） 经过用户本人书面授权或同意提供的。

除上述情形外，河北 CA 不会向任何第三方提供用户的个人信息，不会将用户个人信息用于其他用途。

9.4.7 用户个人信息的共享

河北 CA 不会以商业目的或未取得用户自身同意或授权的情况下与其他组织或个人共享证书用户的个人信息。

在遵守国家相关法律法规前提下，河北 CA 经过用户本人书面授权或同意提供的用户个人信息，并有义务要求接收方采取有效手段保护上述信息。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.4.8 CA 对于用户个人信息的管理

河北 CA 通过以下措施规范用户个人信息的内部管理：

a) 河北 CA 遵循法律法规的要求及行业规范要求采取对个人信息安全保护措施；

b) 河北 CA 内部建立严格的用户个人信息收集、查阅、使用、处理等管理制度；

c) 河北 CA 通过加强内部员工关于个人信息保护的培训，要求员工参加学习培训并签到；

d) 河北 CA 注册机构建立不能低于河北 CA 对用户个人信息的保护级别的用户个人信息保护制度。

9.4.9 个人信息的查阅

用户如需查阅及浏览自身的个人信息，请用户按河北省电子认证有限公司官方网站公布的联系方式联系河北 CA 查询。

9.4.10 个人信息的删除和更改

a) 个人信息的删除

按照法律法规要求或与用户电子认证服务协议的约定，河北 CA 有权对证书用户个人信息进行删除。

b) 个人信息的更改

用户在使用 CA 证书服务过程中，个人信息发生变更的，应当自个人信息变更之日起 2 日内通过河北省电子认证有限公司官方网站公布的联系方式提出；由于用户自身原因未及时将变更信息通知河北 CA 的，由此发生的风险由用户自身承担。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.5 知识产权

河北 CA 开展电子认证业务所使用的认证系统、软件程序、业务文档、CPS 文本、操作手册、平台界面等作品著作权，数字证书管理、密码安全、可信验证相关技术专利，以及河北 CA 注册的品牌、服务商标等全部知识产权均归河北 CA 所有，受著作权法、专利法、商标法及商用密码相关法律法规保护。

订户、依赖方仅可在合法使用数字证书、电子认证服务范围内获得有限、非独占、不可转授权的使用权，不得复制、篡改、逆向解析、商用传播本机构知识产权成果，不得仿冒、擅自使用河北 CA 商标。任何未经许可的侵权行为，将依法追究侵权方全部法律责任。

9.6 陈述与担保

9.6.1 CA 的陈述与担保

河北 CA 在提供电子认证服务活动过程中承诺如下：

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

b) 河北 CA 保证使用的系统及密码符合国家相关标准，保证自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) 除非已通过河北 CA 发出河北 CA 的私钥被破坏或被盗的通知，河北 CA 保证其私钥是安全的。

d) 河北 CA 签发给订户的证书符合本 CPS 的所有要求。

e) 在现有技术条件下，河北 CA 保证签发的数字证书在有效期内的有效性和可靠性。

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

g) 河北 CA 按要求及时吊销证书，并发布到 CRL 上供依赖方查询。

h) 河北 CA 拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

i） 证书公开发布后，河北 CA 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。

j） 按照本 CPS 的所有要求，审慎执行订户注册相关操作。

k） 接受订户申请，妥善留存足以核验订户申请信息的相关资料。

l） 在接受订户申请时，严格核验订户身份，并恰当作出注册决定。

9.6.2 订户的陈述与担保

订户一旦接受河北 CA 签发的证书，就被视为向河北 CA、注册机构及依赖方做出以下承诺：

a） 订户熟悉本 CPS 的所有条款和与其证书相关的证书政策，并同意承担证书持有人有关证书的相关责任和义务。

b） 订户在证书申请时提交的所有信息完整、真实、正确，可供河北 CA 或注册机构检查和核实。

c） 订户妥善保管河北 CA 签发的数字证书载体（含数字证书和私钥）及密码，采取安全、合理的措施来防止证书数字证书载体及密码的遗失、泄露和被篡改等事件的发生。

d） 私钥为订户本身所访问和使用，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、遗忘密码、泄密以及其他情况，订户立刻通知河北 CA 或注册机构，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，应立即通知河北 CA 或注册机构吊销证书。

9.6.3 依赖方的陈述与担保

依赖方必须熟悉本 CPS 的条款以及和订户数字证书相关的证书政策（CP），并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户数字证书前，必须采取合理步骤，查证订户数字证书及数

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

字签名的有效性。

证书依赖方对证书的信赖行为表明了解本 CPS 的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

9.7 担保免责

9.7.1 担保责任的否定描述

有下列情况之一的，应当免除河北 CA 的责任：

a) 订户在申请和使用河北 CA 数字证书时，有违反如下义务之一的：

1) 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息。如果订户故意或无意地提供不完整、不可靠、不真实或已过期的信息，得到河北 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人全部承担。如订户已提供的关键材料或信息有变更，可能影响证书使用的，订户应当及时通知河北 CA。如因材料或信息变更未及时通知河北 CA，给订户本人或第三方造成的损失，河北 CA 不承担责任。

2) 订户应当妥善保管河北 CA 所签发的数字证书载体、私钥、保护密码 PIN 安全，不得泄漏或随意交付他人；

3) 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

4) 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知河北 CA 及相关各方，并终止使用该电子签名制作数据；

5) 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度不得将数字证书用于河北 CA 规定使用范围外的其他任何用途使用；

6) 订户必须在证书有效期内使用该证书；不得使用已失密或可能失密已过有效期、被冻结、被吊销的数字证书；

7) 订户有义务根据规定按时向河北 CA 交纳服务费用。

b) 由于下列依赖方的原因造成的损失，河北 CA 不承担任何赔偿责任，由

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

依赖方自行承担。

1）依赖方未经检验证书的状态即决定信赖证书的；

2）依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的。

c） 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。

d） 因河北 CA 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。

e） 如果河北 CA 能够证明其提供的服务是符合法律、行政法规相关规定实施的，河北 CA 将不对订户或依赖方承担任何赔偿或补偿责任。

f） 订户因证书丢失、私钥泄漏等原因需办理挂起、吊销手续，在订户办理证书挂起或吊销手续前及自订户提交挂起或吊销申请后 24 小时内造成的损失，河北 CA 不承担相关责任。

以上未尽事宜，依照中华人民共和国现行法律、法规执行。

9.7.2 隐含担保责任的描述

河北 CA 仅作出法定及本 CPS 载明的有限明示担保，不存在任何隐含担保。不对证书适配特定业务场景、交易收益、系统兼容性、第三方软硬件安全、间接损失、预期收益作出默示保证；不推定证书可无条件用于金融、政务、交易等高风险场景，所有超出书面载明范围的隐含担保均不予成立。

9.7.3 担保免责条款的适用规定

a） §9.7.1 全部免责情形统一适用于订户、依赖方全部索赔主张，不因河北 CA 提供证书服务、出具证书状态查询记录而自动排除免责适用。

b） 免责条款独立生效，部分条款被认定无效不影响其余免责内容效力。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

c) 订户、依赖方明知或应知本章节免责规则仍使用证书服务的，视为自愿接受全部免责约束。

d) 除法律强制性规定不得免除的责任外，凡符合§9.7.1任一情形，河北CA均可直接免除赔偿责任。

9.8 偿付责任规则

9.8.1 财务赔偿范围

河北CA财务赔偿范围涵盖CA在履行服务职责时可能面临的各种风险，包括但不限于技术故障、人为错误、安全漏洞等。如出现下述情形，河北CA承担相应有限赔偿责任：

a) 在订户提交信息或资料真实、完整、准确的情况下，河北CA签发的证书含有错误信息，导致订户或依赖方遭受损失；

b) 由于河北CA致使证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失；

c) 对于订户申请吊销的证书，河北CA未能及时吊销证书由此导致依赖方遭受损失。

河北CA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三个月内向河北CA书面提出赔偿申请，期间届满未提出的，视为放弃赔偿申请权利。期满后提出的，河北CA有权拒绝申请。

9.8.2 赔付计算方式

a) 由于河北CA原因造成证书所载信息与订户申请内容不一致，订户未仔细核对即接受并使用该证书，进而致使订户或证书依赖方产生损失的河北CA承担赔偿责任，赔偿金额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五倍。

b) 由于河北CA致使证书私钥被破译、窃取、泄露，导致订户或依赖方遭

地址：河北省石家庄市桥西区红旗大街88号翰林观天下23号楼27层
客服热线：400-707-3355
网址：http://www.hebca.com

受损失。河北 CA 赔偿金额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。

河北 CA 对所有当事实体（包括但不限于订户、申请人或依赖方）的合计责任不超过该特定证书适用的赔偿责任上限。

9.8.3 赔付监督机制

河北 CA 建立健全电子认证服务赔付监督制度，设立赔付备用金以保障赔付能力；明确赔付责任范围、理赔申请与处理流程，由合规部对赔付申请受理、责任核查、赔付执行实行监督检查。通过内部岗位制衡、内部审计实施监督，确保赔付工作规范、透明、可追溯，并主动接受电子认证服务监管部门的监督检查，切实维护证书用户及依赖方合法权益。

9.9 赔偿

河北 CA 建立规范的电子认证服务赔偿申请、审核、审批及支付流程。确需河北 CA 赔偿的，按照以下流程时限进行处理。

a) 申请：赔偿申请人提交书面申请及相关证明材料。

b) 审核：河北 CA 在 3 个工作日内完成申请受理与材料初审。

c) 审批：初审通过后，河北 CA 在 10 个工作日内完成责任认定与损失核查并核算赔偿金。

d) 支付：对于符合赔偿条件的，5 个工作日内完成赔偿金支付；对不予赔偿的，及时与申请人沟通并说明理由。

9.10 有效期和终止

9.10.1 有效期限

《河北 CA 电子认证业务规则》中详细注明版本号及发布日期，自发布之日起正式生效。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.10.2 终止

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

当河北 CA 终止业务时，《河北 CA 电子认证业务规则》自动终止。

当证书到期或吊销后，订户协议即终止。

9.10.3 效力的终止与保留

《河北 CA 电子认证业务规则》的某些条款在终止后继续有效，如信息保密、隐私保护和知识产权等条款。

9.11 对参与者个别通告与沟通

为确保电子认证业务沟通合法有效、具备法律约束力，河北 CA 与证书订户之间的业务通告、状态告知、规则变更及异常处置等个别沟通工作，均通过可追溯、可核验、不可抵赖的合规渠道开展，包括官方认证邮件、CA 业务平台站内通知、带电子签章的正式公文及书面回执通知等。所有业务沟通与通告记录进行完整留存，作为权责界定的合法依据。

订户需预留并及时更新有效联系方式，因未及时报备联系方式变更导致通知无法送达的，相关责任由订户自行承担。双方通过合规渠道送达的通告信息，一经送达即视为有效，对双方均具有法律约束力。

9.12 修订和发布

9.12.1 规则修订的条件

当相关法律、适用标准及操作规范等有重大改变时，必须修改《河北 CA 电子认证业务规则》。

CPS 起草小组每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.12.2 通告机制和周期

河北 CA 将修订的《河北 CA 电子认证业务规则》通过河北 CA 网址发布，其地址为：http://www.hebca.com。在认为有必要时，河北 CA 将通过电子邮件、信件、媒体等方式通知有关各方。

河北 CA 安全策略委员会批准修订版本后，7 日内进行发布，30 日内向工业和信息化部完成备案。

9.13 争议处理与举证

9.13.1 争议受理范围

河北 CA 受理的争议仅限与本机构电子认证服务、CP 及 CPS 规则适用直接相关的民事及服务类争议。主要覆盖证书全生命周期业务、认证服务履约、规则条款释义与权责认定、服务信息安全、服务费用合规等场景产生的纠纷，凡是与本机构认证服务无关的个人纠纷、第三方侵权纠纷及非本机构业务引发的争议，均不在受理范围内。

9.13.2 争议处理流程

本机构电子认证相关争议遵循先行沟通协商、后组织调解、最终通过法定途径裁决的递进式处置流程。争议发起方可通过本机构官方沟通渠道及业务系统提交争议诉求并附相关佐证材料，本机构收到诉求后 3 个工作日内完成核查并反馈受理结果，受理通过后即刻启动处置流程，协商无果可直接转入调解环节。

9.13.3 协商时限

各方整体沟通协商周期统一控制在 15 个工作日内，在规定时限内积极促成各方达成一致意见，时限届满未形成有效共识的，直接终止协商并转入调解流程。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

9.13.4 调解规则

争议调解遵循合法、自愿、公正、保密原则，由投诉处理小组受理开展调解工作，必要时安排法务人员参与，调解周期不超过 20 个工作日。调解期间将核实争议事实、核验证据、梳理争议焦点，依据现行法律法规、行业规范及本机构 CP、CPS 规则拟定调解方案并征询各方确认，全程留痕存档。调解达成一致的，由各方按约定履约；未达成共识或拒不配合的，即刻终止调解。调解全过程及未生效调解方案严格保密，不得作为后续裁决的不利依据，法律法规另有规定的除外。

9.13.5 仲裁与诉讼管辖规则及适用条件

争议经协商、调解无法解决的，可依法通过仲裁、诉讼方式处置，所有争议纠纷统一由河北 CA 住所地对应的仲裁机构、人民法院专属管辖。相关争议处置均适用我国现行法律法规、行业规范及本机构有效 CP、CPS 规则，以仲裁、司法机关出具的生效文书作为最终处置依据。

9.13.6 举证制度和能力体系

河北 CA 举证制度和能力体系覆盖证书全生存周期，包括但不限于：

a) 证书签发环节，身份验证记录、材料审查记录、告知记录、意愿确认记录等。

b) 签名环节，签名请求验证、签名操作日志、时间戳记录等。

c) 验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等。

d) 河北 CA 根据证书订户、依赖方等实体要求举证的信息内容，协商确定提供举证材料的时间，协商一致后提供举证服务。

9.14 管辖法律

本机构电子认证服务全部业务活动、CP 及 CPS 规则的释义、执行与适用，

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com

均适用中华人民共和国现行有效的法律、行政法规及行业监管规范。所有因电子认证服务及本机构规则引发的各类纠纷与争议，经协商、调解无法解决的，统一由河北 CA 住所地有管辖权的司法、仲裁机构专属管辖，相关生效法律文书为最终处置依据，对所有参与主体具备法律约束力。

9.15 与适用法律的符合性

电子认证活动参与者应当严格遵守适用的法律法规，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

a) 本 CPS 由《河北省电子认证有限公司电子认证业务规则》单一文档构成，不包含其他补充性文件。本《河北 CA 电子认证业务规则》将替代所有先前或同时期的相关文档。

b) 河北 CA 在订户协议及依赖方协议中均已标明对应的本 CPS 版本号。

9.17 其他条款

本 CPS 由河北 CA 负责解释，解释时遵循诚实信用原则，结合条款目的、行业惯例及公平合理原则作出解释。

地址：河北省石家庄市桥西区红旗大街 88 号翰林观天下 23 号楼 27 层
客服热线：400-707-3355
网址：http://www.hebca.com