



北京数字认证 电子签名电子认证业务规则

3.0.1 版

发布日期：2026 年 10 月 31 日

生效日期：2026 年 10 月 31 日

北京数字认证股份有限公司

Copyright © Beijing Certificate Authority Co.,Ltd.



版本控制表

版本	状态	修订说明	审核/批准人	生效时间
2.0.1	版本发布	新版本发布	公司安全策略管理委员会	2011 年 11 月 16 日
2.0.2	版本发布	修订组织身份鉴别，以及异地备份策略。	公司安全策略管理委员会	2017 年 6 月 27 日
2.0.3	版本发布	依照《网络安全法》，修订用户个人隐私条款。	公司安全策略管理委员会	2017 年 8 月 25 日
2.0.4	版本发布	修订简称“BJCA”为“数字认证公司”。 增加事件型和云端协同型的证书类型，以及生命周期管理业务规则。	公司安全策略管理委员会	2017 年 11 月 9 日
2.0.5	版本发布	修订身份鉴别增加在线鉴别方式。 修订机房监控录像保存时间。	公司安全策略管理委员会	2018 年 4 月 26 日
2.0.6	版本发布	增加标识证书类型，以及标识证书生命周期管理的业务规则。	公司安全策略管理委员会	2019 年 7 月 12 日
2.0.7	版本发布	修订事件型证书业务规则，以及记录归档保存期限等。	公司安全策略管理委员会	2019 年 9 月 27 日
2.0.8	版本发布	修订参与方描述、关于事件型证书的生命周期操作要求，以及证书名称形式等。	公司安全策略管理委员会	2020 年 4 月 26 日
2.0.9	版本发布	修订标识证书业务规则。	公司安全策略管理委员会	2020 年 8 月 7 日
2.0.10	版本发布	修订云端协同证书，增加云端协同证书的密钥管理类型，以及修订云端协同证书生命周期管理的业务规则。	公司安全策略管理委员会	2020 年 9 月 16 日



2.0.1 1	版本发布	修订依赖方描述，以及身份鉴别、事件型证书业务规则等。	公司安全策略管理委员会	2021 年 9 月 3 日
2.0.1 2	版本发布	增加预签证书类型，以及预签证书生命周期管理的业务规则。	公司安全策略管理委员会	2022 年 3 月 31 日
2.0.1 3	版本发布	修订事件型证书业务规则	公司安全策略管理委员会	2022 年 8 月 15 日
2.0.1 4	版本发布	修订身份鉴别、标识证书业务规则等。	公司安全策略管理委员会	2022 年 9 月 30 日
2.0.1 5	版本发布	依照个人信息保护相关要求，修订用户个人隐私条款。	公司安全策略管理委员会	2023 年 2 月 6 日
2.0.1 6	版本发布	修订赔付责任有关条款。	公司安全策略管理委员会	2023 年 7 月 11 日
2.0.1 7	版本发布	修订证书类型，将通用证书改为通用介质证书，并修订证书生命周期管理的业务规则	公司安全策略管理委员会	2024 年 10 月 24 日
2.1.1	版本发布	修订证书类型，将预签证书、标识证书从本业务规则删除。	公司安全策略管理委员会	2025 年 8 月 8 日
2.1.2	版本发布	修订ARL发布、日志分析、CA密钥销毁等业务规则。	公司安全策略管理委员会	2025 年 12 月 8 日
3.0.1	版本发布	名称调整，明确适用电子签名电子认证的业务规则，按照主管部门要求修订CPS，增加证书等级分类，一证四步等规则。	公司安全策略管理委员会	2026 年 10 月 31 日



目 录

1. 概括性描述	11
1.1. 承诺	11
1.2. 基本信息	11
1.3. 文档名称与标识	13
1.4. 电子认证活动参与者	13
1.4.1. 电子认证服务机构	13
1.4.2. 注册机构	14
1.4.3. 订户	14
1.4.4. 依赖方	14
1.5. 证书应用	14
1.5.1. 证书应用分类	14
1.5.2. 证书应用限制	15
1.6. 策略管理	16
1.6.1. 策略文档管理机构	16
1.6.2. 策略文档批准程序	16
1.6.3. 联系人	17
1.7. 定义和缩写	17
2. 信息发布与信息管理	21
2.1. 认证信息的发布	21
2.2. 发布时间或频率	21
2.3. 信息库访问控制	21
3. 身份标识与查验	22
3.1. 身份查验通用要求	22
3.1.1. 通用要求	22
3.1.2. 订户告知	22
3.2. 初始身份确认	22
3.2.1. 证明拥有私钥的方法	22
3.2.2. 个人身份的查验	23
3.2.3. 机构身份的查验	24
3.3. 订户意愿记录	25
3.3.1. 订户意愿记录内容	25
3.3.2. 个人证书的意愿记录	26
3.3.3. 机构证书的意愿记录	26
3.4. 订户协议	27
3.5. 未验证的订户信息	27
3.6. 互操作准则	27
3.7. 命名	28
3.7.1. 名称类型	28
3.7.2. 对名称意义化的要求	28
3.7.3. 订户的匿名或伪名	28
3.7.4. 解释不同名称形式的规则	28
3.7.5. 商标的识别、鉴别和角色	29



4. 证书生存周期操作要求	30
4.1. 通用要求	30
4.2. 证书申请	30
4.2.1. 证书申请实体	30
4.2.2. 执行识别与查验程序	30
4.2.3. 证书申请批准和拒绝	30
4.2.4. 处理证书申请的时间	31
4.3. 证书签发	31
4.3.1. 证书签发过程中电子认证服务机构的行为	31
4.3.2. 电子认证服务机构对订户的通告	31
4.4. 证书接受	32
4.4.1. 构成接受证书的行为	32
4.4.2. 电子认证服务机构对证书的发布	32
4.4.3. 电子认证服务机构在颁发证书时对其他实体的通告	32
4.5. 密钥对和证书的使用	33
4.5.1. 订户私钥和证书的使用	33
4.5.2. 依赖方对公钥和证书的使用	34
4.6. 证书续期	34
4.6.1. 证书续期的情形	34
4.6.2. 请求证书续期的实体	34
4.6.3. 证书续期请求的处理	34
4.6.4. 颁发新证书时对订户的通告	35
4.6.5. 构成接受续期证书的行为	35
4.6.6. 电子认证服务机构对证书续期的发布	35
4.6.7. 电子认证服务机构在颁发证书时对其他实体的通告	35
4.7. 证书密钥更新	35
4.7.1. 证书密钥更新的情形	35
4.7.2. 请求证书密钥更新的实体	35
4.7.3. 证书密钥更新请求的处理	36
4.7.4. 颁发新证书对订户的通告	36
4.7.5. 构成接受密钥更新证书的行为	36
4.7.6. 电子认证服务机构对密钥更新证书的发布	36
4.7.7. 电子认证服务机构在颁发证书时对其他实体的通告	36
4.8. 证书变更	36
4.8.1. 证书变更的情形	36
4.8.2. 请求证书变更的实体	36
4.8.3. 证书变更请求的处理	36
4.8.4. 颁发新证书对订户的通告	37
4.8.5. 构成接受变更证书的行为	37
4.8.6. 电子认证服务机构对变更证书的发布	37
4.8.7. 电子认证服务机构在颁发证书时对其他实体的通告	37
4.9. 证书撤销	37
4.9.1. 证书撤销的情形	37
4.9.2. 请求证书撤销的实体	37



4.9.3. 撤销请求的流程	38
4.9.4. 撤销请求宽限期	38
4.9.5. 电子认证服务机构处理撤销请求的时限	38
4.9.6. 依赖方检查证书撤销的要求	39
4.9.7. CRL 的发布频率	39
4.9.8. CRL 发布的最长滞后时间	39
4.9.9. 撤销信息的其他发布形式	39
4.10. 证书状态信息服务	39
4.10.1. 操作特点	39
4.10.2. 服务可用性	40
4.10.3. 可选特征	40
4.11. 停止使用认证服务	40
4.12. 密钥托管与恢复	41
4.12.1. 密钥托管与恢复的策略和行为	41
4.12.2. 会话密钥的封装与恢复的策略和行为	41
5. 认证机构设施、管理和操作控制	42
5.1. 物理控制	42
5.1.1. 场地位置与建筑	42
5.1.2. 物理访问	42
5.1.3. 电力与空调	43
5.1.4. 水患防治	43
5.1.5. 火灾预防和保护	43
5.1.6. 设备与介质存储	44
5.1.7. 废物处理	45
5.1.8. 异地备份	45
5.2. 操作过程控制	45
5.2.1. 可信角色	45
5.2.2. 每项任务需要的人数	46
5.2.3. 每个角色的标识与鉴别	46
5.2.4. 需要职责分割的角色	46
5.3. 人员控制	47
5.3.1. 资格、经历和无过失要求	47
5.3.2. 背景审查程序	47
5.3.3. 培训与考核要求	47
5.3.4. 再培训周期和要求	48
5.3.5. 工作岗位轮换周期和顺序	48
5.3.6. 未授权行为的处罚	48
5.3.7. 独立合约人的要求	49
5.3.8. 提供给员工的文档	49
5.4. 审计日志程序	49
5.4.1. 记录事件的类型	49
5.4.2. 处理日志的周期	50
5.4.3. 审计日志的保存期限	50
5.4.4. 审计日志的保护	50



5.4.5. 审计日志备份程序	50
5.4.6. 审计日志收集系统	50
5.4.7. 对导致事件实体的通告	50
5.4.8. 脆弱性评估	51
5.5. 记录归档	51
5.5.1. 归档记录的类型	51
5.5.2. 归档记录的保存期限	51
5.5.3. 归档文件的保护	51
5.5.4. 归档文件的备份程序	52
5.5.5. 归档收集系统	52
5.5.6. 获得和检验归档信息的程序	52
5.6. 电子认证服务机构密钥更替	52
5.7. 损害和灾难恢复	53
5.7.1. 业务连续性目标	53
5.7.2. 恢复流程	53
5.7.3. CA 私钥应急处理	53
5.7.4. 事件报告	54
5.7.5. 定期验证	54
5.8. 电子认证服务机构的终止	54
5.9. 重大事项报告	55
5.9.1. 重大事项范围	55
5.9.2. 重大事项报告程序	55
6. 认证系统技术安全控制	56
6.1. 技术安全管理制度要求	56
6.2. 密钥对的生成和安装	56
6.2.1. CA 密钥对的生成和安装	56
6.2.2. 订户密钥对的生成和交付	56
6.2.3. 公钥传送给证书签发机构	57
6.2.4. 电子认证服务机构公钥传送给依赖方	58
6.2.5. 密钥的长度	58
6.2.6. 公钥参数的生成和质量检查	58
6.2.7. 密钥使用目的	58
6.3. 私钥保护和密码模块工程控制	58
6.3.1. CA 私钥保护和密码模块工程控制	58
6.3.2. 订户私钥保护和密码模块工程控制	59
6.3.3. 私钥备份	59
6.3.4. 私钥归档	59
6.3.5. 私钥导入或导出密码模块	59
6.3.6. 私钥在密码模块中的存储	59
6.3.7. 激活私钥的方法	60
6.3.8. 解除私钥激活状态的方法	60
6.3.9. 销毁密钥的方法	60
6.3.10. 密码模块的评估	60
6.4. 密钥对管理的其他方面	61



6.4.1. 公钥归档	61
6.4.2. 证书操作期和密钥对使用期限	61
6.5. 激活数据	61
6.5.1. 激活数据的产生、传输和使用	61
6.5.2. 激活数据的保护	61
6.5.3. 激活数据的销毁	62
6.6. 计算机安全控制	62
6.6.1. 计算机安全控制要求	62
6.6.2. 计算机安全评估	62
6.7. 生存周期安全控制	63
6.7.1. 证书认证中心运行管理要求	63
6.7.2. 密钥管理中心运行管理要求	63
6.7.3. 证书操作流程	63
6.8. 网络的安全控制	63
6.9. 时间戳	64
7. 证书、证书撤销列表和在线证书状态协议	65
7.1. 证书	65
7.1.1. 版本号	65
7.1.2. 算法对象标识符	65
7.1.3. 证书序列号	65
7.1.4. 证书有效期	65
7.1.5. 名称形式	65
7.1.6. 证书扩展项	67
7.1.7. 订户电子签名验证数据	67
7.1.8. CA 电子签名	67
7.1.9. 其他信息	68
7.2. 证书撤销列表	68
7.2.1. 版本号	68
7.2.2. CRL 和 CRL 条目扩展项	68
7.3. 在线证书状态协议	68
7.3.1. 版本号	69
7.3.2. OCSP 扩展项	69
8. 认证机构审计及相关评估	70
8.1. 审计评估制度	70
8.2. 认证业务审计	70
8.3. 全面符合性评估	70
8.4. 评估者的资质	71
8.5. 评估者与被评估者之间的关系	71
9. 法律责任和其他业务条款	72
9.1. 费用	72
9.1.1. 电子认证服务相关费用	72
9.1.2. 退款策略	72
9.2. 财务责任	72
9.3. 业务信息保密	73



9.3.1. 保密信息范围	73
9.3.2. 不属于保密的信息	73
9.3.3. 保护保密信息的信息	73
9.4. 个人隐私保护	74
9.4.1. 隐私保护方案	74
9.4.2. 个人隐私信息的收集	74
9.4.3. 个人信息的存储	75
9.4.4. 个人信息的使用	75
9.4.5. 个人信息的共享	75
9.4.6. CA 对于用户个人信息的管理	75
9.4.7. 个人信息的查阅	76
9.4.8. 个人信息的删除和更改	76
9.5. 知识产权	76
9.6. 陈述和担保	76
9.6.1. 电子认证服务机构的陈述与担保	76
9.6.2. 订户的陈述与担保	77
9.6.3. 依赖方的陈述与担保	77
9.6.4. 其他参与者的陈述与担保	78
9.7. 担保免责	78
9.7.1. 责任免除	78
9.7.2. 隐含的担保责任	79
9.7.3. 担保免责的适用规定	79
9.8. 赔付责任规则	79
9.8.1. 赔偿责任范围	79
9.8.2. 赔偿责任限额	80
9.8.3. 赔付监督机制	80
9.8.4. 有限责任	80
9.9. 赔偿	81
9.9.1. 赔偿申请流程	81
9.9.2. 赔偿审核流程	81
9.9.3. 赔偿审批流程	82
9.9.4. 赔偿支付流程	82
9.10. 有效期限与终止	82
9.10.1. 有效期限	82
9.10.2. 效力的终止与保留	82
9.11. 对参与者的个别通告与沟通	83
9.12. 修订和发布	83
9.12.1. 修订程序	83
9.12.2. 通告机制和期限	83
9.12.3. 必须修改业务规则的情形	83
9.13. 争议处理与举证	83
9.13.1. 争议处理	83
9.13.2. 举证	84
9.14. 管辖法律	84



9.15. 与适用法律的符合性	84
9.16. 一般条款	85
9.16.1. 完整规定	85
9.16.2. 分割性	85
9.16.3. 强制执行	85
9.16.4. 不可抗力	85
9.17. 其他条款	85

1. 概括性描述

1.1. 承诺

北京数字认证电子签名电子认证业务规则（以下简称《电子认证业务规则》或 CPS）由北京数字认证股份有限公司（Beijing Certificate Authority Co.,Ltd.，简称数字认证公司）按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范》制定，并报工业和信息化部备案。

本《电子认证业务规则》详细阐述了数字认证公司在实际工作和运行中所遵循的各项规范，数字认证公司承诺：

- a) 开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任；
- b) 与客户建立业务关系前，开展应用业务调研，建立应用接入业务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。

本《电子认证业务规则》适用于数字认证公司及其员工、注册机构、订户和依赖方，各参与方必须完整地理解和执行本《电子认证业务规则》所规定的条款，并承担相应的责任和义务。

1.2. 基本信息

数字认证公司于 2001 年 2 月开始运营，是权威、公正的电子认证服务机构。数字认证公司严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，提供数字证书签发、更新、撤销或管理等服务，并通过以 PKI 技术、数字证书应用技术为核心的应用安全解决方案，为电子商务、企业信息化构建安全、可靠的信任环境。数字认证公司基本信息如下：

机构名称	北京数字认证股份有限公司	法定代表人	林雪焰
住所地址、经营场所地址	北京市海淀区北四环西路 68 号 1501 号 北京市西城区裕民东路 3 号 京版大厦一层	联系电话	010-58045600
电子认证服	ECP11010820009	发证机关	工业和信息化部



务许可证号			
批准日期	2005 年 10 月 19 日	许可证有效期	2020 年 10 月 19 日至 2025 年 10 月 18 日 (换证中)

本《电子认证业务规则》包含的证书链及其证书信息详见下表：

● 根证书信息

根证书	证书编号	颁发机构名称	密码算法	密钥长度	有效期	计划服务时间
ROOTCA	69e2fec0170 ac67b	国家密码管理局	SM2	256	2012-7-14 至 2042-7-7	
BeiJing ROOT CA	1000000000 0000011001	数字认证公司	RSA	2048	2017-5-11 至 2047-5-10	28 年
Public Trust Root CA	1000000000 0000021001	数字认证公司	RSA	2048	2017-5-11 至 2047-5-10	28 年
UTrust Root CA	1000000000 0000041002	数字认证公司	RSA	2048	2017-5-11 至 2047-5-10	28 年

● CA 证书信息：

上级证书	CA 证书	证书编号	颁发机构名称	密码算法	密钥长度	有效期	计划服务时间
ROOTCA	Beijing SM2 CA	75dfc8554a8c03 ab35cf59e8b861 3b9e	国家密码管理局	SM2	256	2012-7-14 至 2042-7-7	28 年
Beijing SM2 CA	BeiJing GCA	1110000000000 000000f	数字认证公司	SM2	256	2016-1-1 至 2033-1-10	15 年
Beijing SM2 CA	MSSPCA	1110000000000 000000b	数字认证公司	SM2	256	2015-8-20 至 2033-1-10	16 年
BeiJing ROOT CA	BJCA	1000000000000 0011003	数字认证公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
BeiJing ROOT CA	BeiJing GCA	1000000000000 0011002	数字认证公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
Public Trust Root CA	Public Trust CA-1	1000000000000 0021002	数字认证公司	RSA	2048	2017-5-11 至 2037-5-10	18 年

Public Trust Root CA	Public Trust CA-2	1000000000000 0021003	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
Public Trust Root CA	MSSPCA RSA	1000000000000 0021008	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
UTrust Root CA	SCCA	1000000000000 0041007	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年
UTrust Root CA	GZCA	1000000000000 0041011	数字认证 公司	RSA	2048	2017-5-11 至 2037-5-10	18 年

1.3. 文档名称与标识

本文档名称是《北京数字认证电子签名电子认证业务规则》，版本号为 3.0.1 版，文档发布日期：2026 年 10 月 31 日，本文档对应的证书策略为《北京数字认证电子签名电子认证证书策略 3.0.1 版》。本文档原本对应的《北京数字认证股份有限公司通用介质证书策略（CP1）》、《北京数字认证股份有限公司事件型证书策略（CP2）》、《北京数字认证股份有限公司云端协同证书策略（CP3）》不再单独发布，自《北京数字认证电子签名电子认证证书策略 3.0.1 版》发布之日起终止实行。

本 CPS 下涉及的电子签名认证证书，证书中记载了所遵循的主管部门的证书策略 OID，根据证书等级区分为：

个人高等级证书 OID：2.16.156.339.2.1.1.2

个人基础级证书 OID：2.16.156.339.2.1.1.1

机构高等级证书 OID：2.16.156.339.2.1.2.2

机构基础级证书 OID：2.16.156.339.2.1.2.1

本 CPS 下涉及的证书记载了数字认证公司向国家 OID 注册管理中心注册的证书策略 OID，其信息如下：

通用介质证书策略 OID：1.2.156.112562.2.2.1

云端协同证书策略 OID：1.2.156.112562.2.2.3。

1.4. 电子认证活动参与者

1.4.1. 电子认证服务机构

电子认证服务机构（简称：CA 机构）是指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

靠性验证的活动的实体。

电子认证服务机构应符合《中华人民共和国电子签名法》和《电子认证服务管理办法》有关规定，依据业务主管部门发布的《电子认证业务规则规范》制定本机构的《电子认证业务规则》，并按照业务规则开展电子认证服务。

1.4.2. 注册机构

注册机构（简称：RA 机构）是指具有受理、审核、批准或拒绝数字证书的申请、更新、恢复和撤销等的实体。注册机构应当按照相关法律法规规范和本 CPS 的规定受理和查验证证书服务申请。

数字认证公司除了承担 CA 机构职责，同时也承担 RA 机构职责。数字认证公司不应将注册机构的身份查验义务委托给外部机构和个人。

1.4.3. 订户

订户是指被颁发给一张证书的证书主体。在不同的阶段，也称为证书申请人、证书持有人。

订户向 CA 机构申请电子签名认证证书，应当提供真实、完整和准确的信息。订户如知悉电子签名私钥数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名私钥数据。

1.4.4. 依赖方

依赖方是指基于对电子签名认证证书或电子签名的信赖从事有关活动的人。依赖方应当按照本 CPS 以及与 CA 机构间的相关约定验证证书和电子签名。

1.5. 证书应用

1.5.1. 证书应用分类

本 CA 机构签发的数字证书适用于企业信息化和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及提供数据加解密等服务。

本 CA 机构签发的数字证书根据证书用途的不同，分为签名证书和加密证书，签名证书在本 CPS 中指电子签名认证证书。

a. 签名证书



签名证书按照证书主体对象的类型和风险等级，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，分别适用于对应对象在相应风险等级下的身份认证和电子签名应用场景。四种类型证书的扩展项中记录了主管部门制定发布的证书策略 OID，其具体类型、证书策略 OID、适用的应用场景具体见下表：

证书类型	主管部门 证书策略 OID	适用的应用场景
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

b. 加密证书

加密证书用于数据加密和解密，保障信息传输的机密性。

根据密钥存储方式的不同，分为通用介质证书、云端协同证书。具体如下：

➤ 通用介质证书

通用介质证书是数字认证公司签发的保存在订户持有或指定的证书载体中的一类证书。证书载体包括但不限于智能密码钥匙、密码设备、密码模块。

➤ 云端协同证书

面向移动互联网和云服务新技术领域，数字认证公司创新出一类特定的云端协同证书，适用于订户在移动化和云服务环境中的证书应用。协同数字证书必须由订户终端和云平台协同配合才能完成可靠的电子签名。

数字认证公司还签发预签证书、证据型证书和标识证书等其他类型证书，安全级别属于密码应用级，这些证书不适用于电子签名认证，一般用于身份认证、完整性保护和数据加密等业务场景中。对于这些证书，数字认证公司发布了《北京数字认证股份有限公司安全认证服务证书策略与业务规则》，可通过公司官网查阅、下载。

1.5.2. 证书应用限制

本 CA 机构发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，具体包含但不限于以下情形：



- 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. 策略文档管理机构

数字认证公司安全策略管理委员会是《电子认证业务规则》的管理机构，负责本《电子认证业务规则》的制订、发布、更新等事宜。

安全策略管理委员会成员如下：

主 任：首席安全官/分管网络安全工作的公司高管

成 员：由公司主管合规、产品技术、财务、运营和质量的副总经理、总监等负责人组成。

安全策略委员会的日常工作由运营管理部门负责。

安全策略管理委员会具体职责如下：

- 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；
- 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。

安全策略委员会重大决议的相关文件和会议记录应妥善保存。

1.6.2. 策略文档批准程序

本《电子认证业务规则》由数字认证公司安全策略管理委员会，组织 CPS 编写小组进行编写，编写小组的人员组成和小组成立由安全策略管理委员会或运营中心指定。编写小组完成编写 CPS 草案后，由数字认证公司安全策略管理委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交数字认证公司安全策略管理委员会审批。经数字认证公司安全策略管理委员会审批通过后，在数字认证公司的网站上对外公布。



本《电子认证业务规则》经数字认证公司安全策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.6.3. 联系人

本《电子认证业务规则》在数字认证公司网站发布，对具体个人不另行通知。

网站地址：<http://www.bjca.cn>

电子邮箱地址：cps@bjca.org.cn

联系地址：北京市海淀区北四环西路 68 号双桥大厦 15 层(左岸工社)(100080)

电话号码：8610-58045600

传真号码：8610-58045678

1.7. 定义和缩写

下列定义适用于本《电子认证业务规则》：

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。

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。

公钥 Public Key

非对称密码算法中可以公开的密钥。

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 (PKI) Public Key Infrastructure

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（CA） Certification Authority

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、可靠性验证的活动的实体。

数字证书 Digital Certificate

也称公钥证书，由电子认证服务机构（CA）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关联的数字证书。

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电子签名的信赖从事有关活动的人。

订户 Subscriber

被颁发给一张证书的证书主体。

对象标识符 Object Identifier (OID)

用于无歧义地标识对象的全局唯一值。

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。

证书策略对象标识符 CP OID

对某个证书策略进行唯一标识的 OID。

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

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。

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（CA）签发并发布的被撤销证书的列表。

CA 撤销列表(ARL) Certificate Authority Revocation List

一个经电子认证服务机构电子签名的列表，标记已经被撤销的 CA 的公钥证书的列表，表示这些证书已经无效。

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。

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。

协同运算 Collaborative Computing

协同运算是指用户终端和服务端协同配合完成电子签名的过程。数字认证公司为协同运算申请两项专利：一种协同密钥管理的方法、装置及系统（专利号：201510276343.5）和一种协同数字签名系统及其方法（专利号：201510048860.7）。

云签名服务平台 eSignature Cloud Platform

云签名服务平台（以下简称：云平台）是搭建在云端或服务器端，与订户终端设备协同，共同完成订户电子签名或其他证书应用的平台系统，能够为订户或依赖方提供数字证书和电子签名服务。

安全授权认证 Secure Authorization

安全授权认证是指通过口令、短信验证码、生物识别信息、数字证书等认证凭证对其订户身份进行核验，同时作为订户对其私钥的控制的激活数据。

下列缩略语适用于本《电子认证业务规则》：

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)

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)

2. 信息发布与信息管理的

2.1. 认证信息的发布

数字认证公司的信息库包括：电子认证业务规则及其历史版本、证书策略及其历史版本、证书链、证书信息、状态信息、业务办理指南、依赖方协议、投诉处理政策及投诉方式以及其他由数字认证公司不定期发布的信息。

数字认证公司在官网 <http://www.bjca.cn> 公布了 CPS 与 CP 的现行版本及历史版本、证书链、证书依赖方协议等信息；同时，在自助服务平台 <http://help.bjca.org.cn> 详细列出了在线证书状态服务 URL、证书撤销列表 URL、各类业务详细办理指南、服务网点分布详情、投诉处理政策、投诉热线电话、投诉邮箱以及内部监督部门等信息，方便相关方查阅、下载。

若国家电子认证服务管理平台发布备案要求，CA 机构承诺按要求备案，同时与平台进行证书信息技术对接。

数字认证公司将按监管要求与国家电子认证服务管理平台技术对接，实现国家电子认证服务管理平台根据证书唯一编码、订户身份信息等维度查询本 CA 机构签发的电子签名认证证书的功能。

2.2. 发布时间或频率

本 CA 机构的 CPS 按照 § 1.6.2 所述的批准流程发布，每年至少发布一次，一经发布到数字认证公司的网站，即时生效。

信息发布内容如有变化，应在变化生效后 1 个工作日内在发布网站更新。

2.3. 信息库访问控制

对于公开发布的 CP、CPS 和 CA 证书等公开信息，本 CA 机构允许公众自行通过网站进行查询和访问。

只有经授权的 RA/CA 管理员可以查询 CA 机构数据库中的其他数据。

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

本 CA 机构在受理订户的电子签名认证证书申请时，不会将身份查验服务委托给外部机构或个人，由本 CA 机构向订户和/或受委托人进行告知、身份确认、意愿记录和协议签署。

3.1.2. 订户告知

CA 机构在受理证书申请时，应告知订户以下内容：

- a) 订户的权利和义务；
- b) 服务收费的项目和标准；
- c) 电子签名认证证书、电子签名的使用条件；
- d) 信息安全保障措施；
- e) CA 机构和订户的责任划分；
- 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。

根据证书等级的不同，CA 机构采取不同的告知方式：

- 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，并保留告知记录；
- b) 基础级证书可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，并保留告知记录。

3.2. 初始身份确认

3.2.1. 证明拥有私钥的方法

订户签名密钥对应按照本 CPS § 6.2.2 的要求，由订户生成或委托 CA 机构生成。订户或 CA 机构在符合国家安全标准的智能密码钥匙、密码模块中产生签名公私钥，通过证书请求中包含的数字签名来证明订户持有与注册公钥对应的私

钥。本 CA 机构签发订户证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户拥有私钥。

3.2.2. 个人身份的查验

对于个人证书申请，CA 机构应对个人订户的身份有效性和真实性进行查验，确保查验过程规范、结果可追溯。订户需主动提供能表明其真实身份的有效身份证件或有效身份证件信息，配合 CA 机构完成查验工作。

个人有效身份证件指政府部门签发的合法有效证件，包括但不限于：中国居民身份证、港澳台居民居住证、港澳居民来往内地通行证、台湾居民来往大陆通行证、护照、外国人永久居留身份证、军官证。

个人订户申请证书时，证书申请人出示个人有效身份证件原件或提交有效身份证件信息，CA 机构将通过证件机读工具、权威数据库对个人订户身份资料的真实性和有效性进行核验，确保信息无误。

对于高等级证书，CA 机构应通过面对面、远程人工面对面、生物特征验证或主管部门认可的其他方式进行身份查验，具体查验方式可选择任意一种或多种。

对于基础级证书，CA 机构可采用以下方式之一进行身份查验：

- a) 采取高等级证书的身份查验方式验证；
- b) 通过运营商三要素核对姓名、证件号码、手机号的一致性，并回填随机短信验证码验证；
- c) 通过银行卡四要素核对姓名、证件号码、银行卡号、银行预留手机号的一致性，并使用预留手机号回填随机验证码验证；
- d) 通过申请人持有的有效电子签名认证证书签名验证；
- e) 通过主管部门认可的其他核验方式。

个人电子签名认证证书原则上应订户本人亲自办理。特殊情况需要代办的，受托人需出示受托人与订户的有效身份证件原件或提供双方有效身份证件信息，同时提交由订户本人签署的有效书面授权证明。CA 机构查验受托人与订户身份证件的有效性和真实性，核对受托人身份与授权文件载明信息一致，确认授权行为真实有效。

CA 机构以可追溯方式留存高等级证书查验全过程及结果，基础级证书完整保存查验记录及结果，每张证书建立单独的身份验证记录。

3.2.3. 机构身份的查验

对于机构证书申请，CA 机构将对机构订户的身份和代表机构办理证书的人员的身份的有效性和真实性进行查验，确保查验过程规范、结果可追溯。

机构证书可由法定代表人（包括其他单位、团体、非法人组织等机构的负责人，本 CPS 中统称“法定代表人”）或受托人办理，申请过程中需主动提供机构有效身份证件原件或扫描件，配合 CA 机构完成查验工作。

机构的有效证件指法律法规或国家有关文件规定证件，包括但不限于：营业执照、事业单位法人证书、社会团体法人登记证书、民办非企业单位登记证书、统一社会信用代码证书、政府主管部门的批文或登记证书。

对于机构高等级证书，CA 机构通过权威数据库查验机构有效身份证件的真实性和有效性，并通过以下措施开展法定代表人或受托人查验。

a. 由法定代表人代表机构申请高等级证书时，查验如下：

（1）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法定代表人身份证件的真实性和有效性；

（2）通过面对面、远程人工面对面、生物特征验证或主管部门认可的其他方式进行法定代表人实人查验，具体查验方式可选择任意一种或多种。

b. 由受托人代表机构申请高等级证书时，查验如下：

（1）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受托人身份证件的真实性和有效性；

（2）查验机构加盖公章的有效书面授权证明，核对受托人身份与授权文件载明信息一致；

（3）通过面对面、远程人工面对面、生物特征验证或主管部门认可的其他方式进行实人查验，具体查验方式可选择任意一种或多种。

（4）通过机构对公账户打款验证（随机金额或附言）或主管部门认可的其他方式验证进行查验。

对于机构基础级证书，CA 通过权威数据库查验机构有效身份证件的真实性和有效性，并通过以下措施开展实人查验。

a. 由法定代表人代表机构申请基础级证书时，查验如下：

（1）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法定代表人身份证件的真实性和有效性；

（2）采用以下方式之一进行法定代表人实人查验：

- 采取高等级证书的身份查验方式验证；
- 通过运营商三要素核对姓名、证件号码、手机号的一致性，并回填随机短信验证码验证；



- 通过银行卡四要素核对姓名、证件号码、银行卡号、银行预留手机号的一致性，并使用预留手机号回填随机验证码验证；
- 通过申请人持有的有效电子签名认证证书签名验证；
- 通过主管部门认可的其他核验方式。

b.由受托人代表机构申请基础级证书时，查验如下：

（1）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受托人身份证件的真实性和有效性；

（2）查验机构加盖公章的有效书面授权证明，核对受托人身份与授权文件载明信息一致

（3）采用以下方式之一进行受托人实人查验：

- 采取高等级证书的身份查验方式验证；
- 通过运营商三要素核对姓名、证件号码、手机号的一致性，并回填随机短信验证码验证；
- 通过银行卡四要素核对姓名、证件号码、银行卡号、银行预留手机号的一致性，并使用预留手机号回填随机验证码验证；
- 通过申请人持有的有效电子签名认证证书签名验证；
- 通过主管部门认可的其他核验方式。

c.由订户持有的同等级或者更高级的有效机构证书签名验证。

对于机构有效授权存在争议等情形，CA 机构可以要求申请人提供其他证明材料或增加查验手段，如机构法定代表人本人确认并加盖公章等，证明本机构对办理人的授权。

CA 机构以可追溯方式留存高等级证书查验全过程及结果，基础级证书完整保存查验记录及结果，每张证书建立单独的身份验证记录。

3.3. 订户意愿记录

3.3.1. 订户意愿记录内容

CA 机构应当对订户申请证书的意愿进行记录，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. 个人证书的意愿记录

a) 个人高等级证书

CA 机构对高等级证书订户意愿的确认，将采用以下方式之一：

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

b) 个人基础级证书

CA 机构对基础级证书订户意愿的确认，将采用以下方式之一：

- 与高等级证书相同的方式；
- 采用强制阅读、短信或邮件确认等电子方式。

CA 机构将保留完整、可追溯的订户意愿记录。

3.3.3. 机构证书的意愿记录

a) 机构高等级证书

CA 机构对高等级证书订户意愿的确认，将采用下列方式之一：

- 法定代表人申请时，按照本 CPS § 3.3.2 a) 的方式确认机构法定代表人的意愿；
- 受托人申请时，查验加盖机构公章的授权文件，并按照本 CPS § 3.3.2 a) 的方式确认受托人的意愿。

订户意愿应采用录音录像或通过主管部门认可的其他方式进行记录。

b) 机构基础级证书

CA 机构对基础级证书订户意愿的确认，将采用下列方式之一：

- 法定代表人申请时，按照 CPS § 3.3.2 b) 的方式确认机构法定代表人的意愿；
- 受托人申请时，查验加盖机构公章的授权文件，并按照 CPS § 3.3.2 b) 的方式确认受托人的意愿。

CA 机构将保留完整、可追溯的订户意愿记录。



3.4. 订户协议

CA 机构制定电子认证服务协议，约束 CA 机构与订户权利义务，规范证书使用行为，双方均需严格遵守。协议中包含本 CPS § 3.1.2 规定的订户告知内容。

订户在申请数字证书时，CA 机构应当与订户签订《电子认证服务协议》。协议签订的方式可以通过订户在纸质文件上签字/盖章，或对在线电子版协议进行勾选、点击确认或其他表明认可协议的操作形式完成。

3.5. 未验证的订户信息

CA 机构签发的电子签名认证证书，在证书中载明《电子签名法》第二十一条规定的信息内容，其中包含证书持有人名称在内的订户信息，记录在证书甄别名中（详见本 CPS § 3.7 规定的命名规则）。证书中不能包含未经验证的订户信息。

电子签名认证证书中载明的信息，订户或依赖方通过以下两种方式与流程之一进行查验：

a) 自助查验。直接打开证书文件，查看详细信息中记录的内容。然后查看证书路径（证书链），该项内容中的所有证书链必须与本 CA 机构官方网站公示的证书链完全一致，且验证证书文件中不存在错误的 CA 机构电子签名。其中 CA 机构的电子签名按照证书格式规范采用 ASN.1 编码保存。

b) 人工查验。订户或依赖方可以通过 CA 机构公布的联系方式（详见官方网站），联系 CA 机构客户服务人员，提供需要查验的电子签名认证证书。客户服务人员在验证证书载明的信息后，将验证结果进行反馈。

3.6. 互操作准则

互操作可能是交叉认证、单向交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

CA 机构将根据业务需要，在遵循本《电子认证业务规则》的各项控制要求的基础上，与本 CA 的证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示本 CA 机构批准了或赋予了其他 CA 中心或电子认证服务机构的权利。

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）。

数字证书中的主体的 X.500 DN 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(DN)必须具有一定的代表意义。

个人证书的甄别名通常包含订户姓名，在 DN 或扩展项中还包含有效证件类型及证件号码（或相关信息的映射，包括但不限于散列值、掩码等）。

机构证书的甄别名通常包含机构名称，在 DN 或扩展项中还包含机构有效证件类型及证件号码。

DN 项结构定义应符合 GB/T 16264.8 的要求，证书主体 DN 项编码规则见下表：

代码	说明	示例
C	国家	CN
S	省份（可选）	北京
L	城市（可选）	北京
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

个人证书、机构证书可以通过证书记录的姓名/单位名称和证件号码信息，追溯到证书对应的唯一实体。

3.7.3. 订户的匿名或伪名

在 CA 证书服务体系中，订户不得使用匿名或伪名。

3.7.4. 解释不同名称形式的规则

甄别名（DN）的内容一般由 CN、OU、O、C 等部分组成，具体的命名规则详见本 CPS § 7.1.5 名称形式。

3.7.5. 商标的识别、鉴别和角色

订户在申请证书时，不得使用可能侵犯他人知识产权的内容作为订户信息用于申请证书。CA 机构在受理证书申请时，查验记载在证书主体甄别名中的订户信息真实性，但并不验证该信息是否包含知识产权或处于知识产权纠纷中。

当发生有关知识产权的争议纠纷时，本 CA 机构有权拒绝相应的证书申请或撤销已发放的证书。

4. 证书生存周期操作要求

4.1. 通用要求

CA 机构遵循《电子认证证书策略》和《电子认证业务规则》所规定的要求，明确自身与订户在证书全生存周期中的责任，确保证书申请、签发、使用、撤销等环节合规有序。

- CA 机构职责：

- a. 承担数字证书注册通道的建立、运营和维护责任，搭建安全、稳定、可追溯且符合相关安全标准的注册通道；

- b. 承担与证书订户签订电子认证服务协议的责任；

- c. 承担妥善记录并保存证书生存周期相关信息的责任，对订户申请资料、身份查验记录、意愿确认记录、服务协议、证书签发及变更记录等进行规范归档保管，确保信息的完整性、保密性和可追溯性。

- 订户职责：

承担在证书申请过程中提供准确、完整、真实信息的责任，不得提供虚假信息、冒用他人身份信息或隐瞒重要信息。信息发生变更时需及时书面通知 CA 机构更新，自行承担因信息不实、不完整导致的相关风险和损失。

4.2. 证书申请

4.2.1. 证书申请实体

证书申请实体包括个人、法人和其他组织机构(包括事业单位、企业单位、社会团体和人民团体等)。

4.2.2. 执行识别与查验程序

CA 机构按照本《电子认证业务规则》所规定的程序对订户的身份进行识别与查验。具体的查验程序详见本 CPS § 3 身份标识与查验。

4.2.3. 证书申请批准和拒绝

CA 机构按照本《电子认证业务规则》相关规定，完成订户告知、身份确认、

意愿记录、协议签署等动作，并根据身份查验结果决定批准或拒绝证书申请。

如果订户未能通过身份查验，CA 机构将拒绝订户的证书申请，并通知订户验证失败，同时向订户提供失败的原因(法律禁止的除外)。被拒绝的订户可以在准备正确的材料后，再次提出申请。

如果订户身份查验结果为合格，并履行了其应尽的义务（如接受相关协议的内容和要求、支付所需的费用等），CA 机构将批准证书申请，为订户制作并颁发数字证书。

4.2.4. 处理证书申请的时间

CA 机构将做出合理努力来尽快确认证书申请信息，一旦 CA 机构收到了所有必须的相关信息，将在 2 个工作日内处理证书申请。

CA 机构能否在上述时间期限内处理证书申请，取决于订户是否真实、完整、准确地提交了相关信息，以及是否及时地响应了 CA 机构的管理要求。

如有特殊情况，CA 机构应与订户协商，适当延长证书处理时间。

4.3. 证书签发

4.3.1. 证书签发过程中电子认证服务机构的行为

CA 机构在批准证书申请之后，将签发证书。在签发证书的过程中，RA 与 CA 建立安全通道，CA 接收到 RA 的证书申请后，对证书申请格式、RA 签名等进行验证，验证通过后签发证书。

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。

4.3.2. 电子认证服务机构对订户的通告

CA 机构对订户的通告有以下几种方式：

- a) 通过面对面的方式，通知订户证书签发的结果；
- b) 通过系统提示、短信、电话、电子邮件或邮政信函等方式通知订户；
- c) 通过主管部门认可的其他方式通知订户。

4.4. 证书接受

4.4.1. 构成接受证书的行为

CA 机构交付证书、订户接受证书的方式如下：

a) CA 机构将数字证书当面、寄送或电子方式交付订户，订户从获得数字证书起，就视为已经接受证书；

b) CA 机构通过网络下载方式交付证书的，证书下载的系统记录表明订户已经接受证书；

c) 对于云端协同证书，CA 机构将证书发送到终端模块或云平台的方式交付证书，订户未提出异议即视为订户已经接受证书；

d) 将证书应用于对应的电子签名或其他密码运算时起，就视为订户已经接受证书；

e) CA 机构也可以通过其他安全的方式交付数字证书。

订户如果拒绝接受证书，应当在CA机构交付证书后两个工作日内提出异议，视为订户拒绝接受证书。

CA 机构保存订户接受证书的记录，包括接受时间、方式、操作人等信息。

4.4.2. 电子认证服务机构对证书的发布

CA 机构在签发完数字证书后，采用数据库或目录服务方式，实现数字证书的存储与发布。对已发布的数字证书，CA 机构提供证书目录信息查询服务。

查询方式包括但不限于用户在线自助或人工受理等。查询申请用户需要提供必要的查询条件信息，包括但不限于序列号、证书主体信息、办理渠道、证书链、有效期。对于订户查询，CA 机构核实身份后提供查询服务。对于其他实体查询，为保护证书订户的数据安全和隐私保护，CA 机构只承诺对其他实体提交的证书进行核实。

4.4.3. 电子认证服务机构在颁发证书时对其他实体的通告

CA 机构采用数据库或目录服务方式对证书进行发布，其他实体可以通过 CA 机构提供的查询方式自行查询。

4.5. 密钥对和证书的使用

4.5.1. 订户私钥和证书的使用

CA 机构帮助订户生成签名私钥的，在将签名私钥交付订户前，应采取有效措施保护私钥的安全性，包括但不限于选择符合国家安全的标准的密码模块中生成订户私钥，私钥传输需通过加密通道进行，杜绝明文传输。证书的密码算法应当符合国家密码主管部门和行业安全需求对密码算法的要求。

CA 机构提供订户签名私钥托管服务时，除采取以上安全措施外，同时向订户承诺：

- 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) 对机构证书签名私钥的使用，应设置法定代表人或受托人作为授权主体，如果机构订户需要指定其管理的应用系统代表机构使用签名私钥的，应作出对应授权。
- 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，且存储条件符合安全标准；
- e) 所有涉及签名私钥的操作有完整、可追溯的记录。

订户接受了 CA 机构所签发的证书后，视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。订户应当妥善保管其持有或控制的私钥、证书口令（PIN）或其他私钥保护信息，不得泄露或交付他人。

通用介质证书订户接受到数字证书，使用介质控制证书实施电子签名。订户应妥善保管其证书对应的私钥。

云端协同证书订户必须使用其终端和云平台协同配合才能完成一次电子签名。私钥在终端和云平台协同运算生成的，订户必须通过协同运算才能使用私钥进行签名；私钥在云平台生成的，订户必须通过安全授权认证才能使用私钥进行签名，对于机构证书订户，应设置法定代表人或受托人作为授权主体。云端协同证书通过以上两种方式保证私钥仅由订户持有与控制。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受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撤销之后，订户必须停止使用该证书对应的私钥。

CA 机构提供热线电话、在线客服等渠道提供安全事件反馈，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。

4.5.2. 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份和证书等级，验证证书有效性，并通过公钥验证对方电子签名的真实性。

依赖方查看证书了解对方的身份时，应查看该证书的甄别名、内容、证书策略，对应本 CPS § 3.2 定义的不同的身份查验方法，选择是否信任证书中标识的身份，承担不同查验方法可能存在的风险。依赖方查看证书了解证书等级时，应查看证书策略 OID 中记录的证书等级，根据自身所涉及的业务等级要求，选择信任不低于该等级的证书。

验证证书的有效性包括：

- a) 用 CA 机构的证书验证证书中的签名，确认该证书是 CA 机构签发的，并且证书的内容没有被篡改。
- b) 检验证书的有效期，确认该证书在有效期之内。
- c) 检验证书有效性，需要检查该证书没有被撤销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6. 证书续期

4.6.1. 证书续期的情形

证书续期指在不改变证书订户信息的情况下，为订户签发一张新证书。

证书中有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到 CA 机构申请证书续期。

4.6.2. 请求证书续期的实体

证书订户或其受托人可以请求证书续期。

4.6.3. 证书续期请求的处理

证书申请者应在证书到期前，采取面对面或在线的方式向 CA 机构提交证书续期申请。

证书续期申请的身份查验可采用有效的原证书进行电子签名验证的方式进

行身份确认，或采用与新申请证书相同的身份查验流程进行确认。采用原证书签名验证的方式查验的，应满足自上次完成身份查验之日起至本次申请续期申请日未满三年，或经核实查验订户身份的信息未发生改变，否则应使用本 CPS § 3 规定的身份查验进行确认。CA 机构查验身份通过后为订户签发新的证书。

订户证书失效后申请证书续期，需要对订户身份进行重新验证。

4.6.4. 颁发新证书时对订户的通告

同 4.3.2。

4.6.5. 构成接受续期证书的行为

同 4.4.1。

4.6.6. 电子认证服务机构对证书续期的发布

同 4.4.2。

4.6.7. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.7. 证书密钥更新

4.7.1. 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，CA 机构提供证书更新时，密钥必须同时更新。

证书密钥更新的具体情形如下：

- a) 当订户证书即将到期时；
- b) 当订户证书密钥遭到损坏时；
- c) 当订户证实或怀疑其证书密钥不安全时；
- d) 其它可能导致密钥更新的情形。

4.7.2. 请求证书密钥更新的实体

订户或其受托人可以请求证书密钥更新。

4.7.3. 证书密钥更新请求的处理

同 4.6.3。

4.7.4. 颁发新证书对订户的通告

同 4.3.2。

4.7.5. 构成接受密钥更新证书的行为

同 4.4.1。

4.7.6. 电子认证服务机构对密钥更新证书的发布

同 4.4.2。

4.7.7. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.8. 证书变更

4.8.1. 证书变更的情形

证书变更是指在证书有效期内，除证件号码以外订户证书信息发生变化，在不改变订户公钥的情况下，CA 机构经核验后签发一张新证书。

4.8.2. 请求证书变更的实体

订户或其受托人可以请求证书变更。

4.8.3. 证书变更请求的处理

证书变更应采用与本 CPS § 3 章节的流程进行标识与查验，验证变更信息的真实性，若发起方不是证书订户，CA 机构应取得订户同意，验证通过后为订户签发新的证书。

4.8.4. 颁发新证书对订户的通告

同 4.3.2。

4.8.5. 构成接受变更证书的行为

同 4.4.1。

4.8.6. 电子认证服务机构对变更证书的发布

同 4.4.2。

4.8.7. 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.9. 证书撤销

4.9.1. 证书撤销的情形

- a) 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本《电子认证业务规则》；
 - 4) 认为当前密钥管理方式的安全性得不到保证。
- b) 发生下列情形之一的，CA 机构可以强制撤销其签发的数字证书：
 - 1) 订户提供的信息不真实；
 - 2) 订户没有履行双方合同规定的义务，或违反本 CPS；
 - 3) 数字证书的安全性得不到保证；
 - 4) 法律、行政法规规定的其他情形。

4.9.2. 请求证书撤销的实体

根据不同的情况，订户、受托人、CA 机构或依赖方可以请求撤销最终用户证书。当发生 CPS § 4.9.1 a) 所列情形时，订户本人或受托人可以请求撤销证书；当发生 CPS § 4.9.1 b) 所列情形时，依赖方可以请求撤销证书，CA 机构也可以直接启动强制撤销流程。

4.9.3. 撤销请求的流程

CA 机构通过热线电话、在线客服等渠道，向相关方提供证书撤销流程咨询服务，并记录影响证书或私钥安全的事件（如密钥遗失、泄露等）。

证书撤销流程如下：

a) 证书撤销的申请人到 CA 机构现场或在线提交证书撤销申请，并注明撤销原因；

b) CA 机构审核申请人的身份和权限，以及证书撤销理由、证书是否在有效期内等信息，决定撤销证书或拒绝撤销证书；

c) CA 机构撤销订户证书后，订户证书在 24 小时内进入 CRL，向外界公布。

强制撤销是指当 CA 机构确认发生本 CPS § 4.9.1b) 强制撤销证书情形时，对订户证书进行强制撤销，撤销后将通过官网公告或其他安全可行的方式通告订户。

4.9.4. 撤销请求宽限期

如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在 48 小时内提出。

4.9.5. 电子认证服务机构处理撤销请求的时限

CA 机构接到撤销请求后，在 1 个工作日内，按照本 CPS § 4.9.3 的流程处理证书撤销请求。

CA 机构每日签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

CRL 的结构如下：

- a) 版本号(version)
- b) 签名算法标识符(signature)
- c) 颁发者名称(issuer)
- d) 本次更新(this update)
- e) 下次更新(next update)
- f) 用户证书序列号/撤销日期(user certificate/revocation date)
- g) 签名算法(signature algorithm)
- h) 签名(signature value)

4.9.6. 依赖方检查证书撤销的要求

在具体应用中，依赖方可以使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL 查询：利用证书中标识的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验。

b) 在线证书状态查询(OCSP)：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经 CA 机构发布并且签名的。

4.9.7. CRL 的发布频率

CA 机构可采用实时或定期的方式发布 CRL、ARL。发布频率根据证书策略确定，对于订户证书一般不超过 24 小时发布 1 次 CRL，对于中级 CA 证书通常不超过 12 个月发布 1 次 ARL。

4.9.8. CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9. 撤销信息的其他发布形式

证书撤销信息通过 CRL 服务方式发布，予以公告。

CA 机构还可以采取官网通知的方式公告。

4.10. 证书状态信息服务

4.10.1. 操作特点

CA 机构提供证书状态信息查询服务，包括证书撤销列表 CRL、在线证书状态查询服务 OCSP 等状态信息查询服务，以供依赖方获取证书有效性信息。

CA 机构对证书状态信息服务的查询请求有合理的响应时间和并发处理能力。一般情况下 OCSP 响应时间不超过 5s，CRL 响应时间不超过 30s。

4.10.2.服务可用性

CA 机构提供 7X24 小时的证书状态查询服务，服务可用性指标不低于 99.95%。在服务不可用时，依赖方可通过热线电话或邮件等方式向 CA 机构申请查询。

4.10.3.可选特征

根据请求者的要求，在请求者支付相关费用后，CA 机构可以提供以下通知服务：

- a) 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被撤销；
- b) 提供通知服务，当指定的证书被撤销时，CA 机构将通知请求该项服务的请求者。

4.11. 停止使用认证服务

以下三种情形，订户应当停止使用认证服务：

- a) 证书有效期已经过期，且订户未重新申请证书，或证书在有效期内被撤销时；
- b) 证书在有效期内，订户主动申请终止认证服务；
- c) 法律法规规定的订户应当停止使用认证服务的其他情形。

对于 b)和 c)的情形，CA 机构将根据订户申请，或按照本 CPS 的规定，在 1 个工作日内以证书撤销方式处理。

由 CA 机构提供密钥托管服务的，停止使用认证服务后，CA 机构应当安全销毁订户签名私钥，并完整记录操作过程。

对于相关认证信息中涉及用户的数据，CA 机构将继续依法保存，保存期限在证书失效后不少于 5 年。当依据法律规定应当销毁用户数据时，CA 机构应在销毁前进行安全审计，形成审计报告并存档备查。如因各种情况，CA 机构需要终止运营时，数据将按要求转移交给承接单位。

停止使用认证服务后，CA 机构按法律规定和双方协议约定，继续拥有保存订户认证信息相关数据的权利，并履行安全、妥善保管的义务。

在停止使用认证服务前，订户已经使用证书及签名私钥实施的签名行为，其效力与法律后果不因停止使用认证服务而终止。

4.12. 密钥托管与恢复

4.12.1. 密钥托管与恢复的策略和行为

CA 机构的根私钥和 CA 私钥不会托管给任何第三方或个人，存储私钥的密码设备均放置在屏蔽机房且不可离开该机房。CA 私钥备份采取多人控制，需全部密钥管理员到场方可执行备份操作，导出的密钥备份文件会被存放在安全的区域。当遇到异常情况需要恢复密钥时，需由 3 名或以上的密钥管理员到场授权方可执行密钥恢复操作，并在安全物理环境中执行。

订户密钥恢复是指订户加密密钥对的恢复。密钥恢复分为两类：用户密钥恢复和司法密钥恢复。

a) 用户密钥恢复：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。订户向 CA 机构申请，经审核后，通过 CA 机构向密钥管理中心请求；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) 司法密钥恢复：司法取证人员在密钥管理中心申请，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。

CA 机构不提供订户签名密钥的恢复。

4.12.2. 会话密钥的封装与恢复的策略和行为

非对称算法组织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

a) CA 机房的建筑物和机房建设按照下列标准实施：

- 1) GB 50174-93：《电子计算机机房设计规范》
- 2) GB 2887-89：《计算站场地技术条件》
- 3) GB 9361-88：《计算站场地安全要求》
- 4) GB 6650-1986：《计算机机房用活动地板技术条件》
- 5) GB 50034-1992：《工业企业照明设计标准》
- 6) GB 5054-95：《低压配电装置及线路设计规范》
- 7) GBJ 19-87：《采暖通风与空气调节设计规范》
- 8) GB 157：《建筑防雷设计规范》
- 9) GBJ 79-85：《工业企业通信接地设计规范》

b) CA 机房位于北京市西城区裕民东路 3 号京版大厦一层，实行分层访问的
安全管理：

CA 机房依据 GB/T 25056 《信息安全技术 证书认证系统密码及其相关安全技术规范》要求进行建设和管理，分为四个区域：公共区、服务区、管理区、核心区。

公共区、服务区采用身份识别卡和指纹识别校验相结合的控制方法。工作人员需通过身份识别卡和指纹识别校验后，方可进入该区域。离开时，需刷卡离开。

管理区、核心区，采用身份识别卡和指纹校验相结合的控制方法，且需要双人同时校验通过后才能进入核心机房。离开时，需双人同时刷卡离开。

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、监控手段。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：

a) 门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间记录和信息提示。



b) 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c) 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，对机房区域进行 24 小时不间断录像。

所有门禁访问记录和视频监控记录保留不少于 6 个月，在销毁前会进行安全审计，形成审计报告并存档备查。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

5.1.3. 电力与空调

机房电源供电系统包括机房区的动力、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，计算机设备和动力设备分开供电。供电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用中央空调，并采用独立空调作为备份。其组成包括精密空调、通风管路、新风系统。机房室内夏季温度保持在 $23 \pm 2^{\circ}\text{C}$ ，冬季温度保持在 $20 \pm 2^{\circ}\text{C}$ ；相对湿度保持在 40%-60%。

CA 机房的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4. 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

CA 机房的系统有充分保障，能够防止水侵蚀。

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提供（7X24）实时检测。

5.1.5. 火灾预防和保护

火灾预防：

a) CA 机房建筑物的耐火等级符合二级耐火等级。

b) CA 机房设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。

c) CA 机房配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器及消防自救呼吸器。CA 机房内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

d) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

e) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟。

f) 办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

g) 紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。CA 机房采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

h) 外聘第三方机构每月开展消防安全巡检，每两年开展消防安全检测。

灭火系统采用电动，手动，紧急启动三种方式：

a) 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

b) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

c) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

CA 机房通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.6. 设备与介质存储

CA 机构制定设备管理制度，建立设备管理台账，设备管理台账包含每台设备责任人、使用状态、维护周期等。设备管理员定期进行设备盘点和核对，确保账实相符。

CA 机房的存储介质包括硬盘、磁带、光盘等，介质存储地点和 CA 机房系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。对于存放重要数据的存储介质，CA 机构制定了详细的使用、报废管理规定，完整地记录其领用、归还、报废等操作行为，以防止重要信息的泄露与人为故意产生的危害和破坏。

5.1.7. 废物处理

当 CA 机房存档的敏感数据或密钥已不再需要或存档的期限已满时，应当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。

CA 机构对所有处理行为进行记录并存档。

5.1.8. 异地备份

CA 主机房位于北京市西城区裕民东路 3 号，同城数据备份位于北京市朝阳区工体北路 1 号(工体云数据中心)。主机房的电子认证数据实时传输到容灾备份中心，用于容灾备份系统应急恢复，容灾备份中心位于武汉市东西湖区临空港经济技术开发区网安大道 9 号中金武汉数谷大数据中心机房，距离主机房 900 公里。

5.2. 操作过程控制

5.2.1. 可信角色

涉及证书认证系统操作、维护与管理，且能从本质上影响证书生存周期或 CA 密钥安全的岗位，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

系统管理员负责 CA 系统日常管理，包括策略配置、用户与权限管理等。

b) 技术运维员

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

数据库管理员负责数据库日常运维、性能优化及数据备份等。

d) 安全管理员

安全管理员全面负责物理环境、网络、系统的安全管理工作，拟订安全管理制度和操作流程，监督各岗位安全工作落地执行。

e) 系统审计员

系统审计员负责系统和网络日志的审计、管理，生成审计报告等。

f) 密钥管理员

密钥管理员负责 CA 密钥材料管理、CA 密钥生存周期管理等。

g) 证书业务管理员

证书业务管理员负责证书注册系统的业务管理，包括证书业务操作员与权限



管理等。

h) 证书业务操作员

证书业务操作员负责证书申请的受理与审核，订户的身份与意愿鉴证。

i) 客户档案管理员

客户档案管理员负责证书相关档案资料的归档与保密等。

j) 运营审计员

运营审计员负责对证书签发、客户服务等核心业务进行独立审计等。

5.2.2. 每项任务需要的人数

CA 机构按照职责分离原则和岗位备份原则，对关键操作的角色采取双人操作或监督机制：

a) 涉及关键操作的角色，如密钥管理、审计、鉴证、系统管理等，应实现双人操作或复核机制；

b) 涉及业务连续性相关操作的角色，如运维、鉴证、审计等，应按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；

c) 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。

5.2.3. 每个角色的标识与鉴别

CA 机构的从业人员，按照所担任角色的不同进行身份鉴别。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。CA 机构将独立完整地记录其所有的操作行为。

5.2.4. 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即 CA 机构的可信角色由不同的人担任。需要职责分离的角色，包括但不限于下列角色：

a) 系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任；

b) 同一证书业务的录入与审核环节不得由同一业务操作员完成；

c) 业务操作员、客户档案管理员、运营审计员之间不得兼任；

d) 密钥管理员不得与系统管理员、技术运维员兼任。

5.3. 人员控制

5.3.1. 资格、经历和无过失要求

CA 机构对所有可信角色的资格、经历与背景进行调查，包括但不限于：

- a) CA 机构需对可信人员进行背景调查，核实其从业经历，并要求提交无犯罪记录证明；
- b) 可信人员应具备履行岗位职责所必需的专业技能要求，专业技能要求参考 GB/T 35288《信息安全技术 电子认证服务机构从业人员岗位技能规范》；
- c) CA 机构与可信人员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；
- d) CA 机构与可信人员签署劳动合同。

5.3.2. 背景审查程序

CA 机构与有关的政府部门和调查机构合作，完成对 CA 机构可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工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《可信雇员调查表》，报主管领导批准后准予上岗。

5.3.3. 培训与考核要求

岗前培训：CA 机构对运营人员按照其岗位和角色安排不同的培训，上岗前



培训时长不少于 20 学时，并通过考核。

持续培训：对于运营人员，其 CA 的相关知识技能，每年至少要总结一次并由 CA 机构组织培训与考核。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。

培训内容包括：

- a) 电子认证服务相关法律法规与标准；
- b) 岗位通用职责要求及各角色特定的工作要求；
- c) CA 机构内部管理政策、制度及流程；
- d) PKI 和密码技术基础知识；
- e) CPS、CP；
- f) 安全管理策略和机制；
- e) 订户身份查验、审核策略和流程；
- h) 电子认证服务运营体系构成；
- i) 电子认证服务技术体系构成；
- g) 灾难恢复和业务连续性管理。

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 CA 机构组织的培训一次。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。每人每年培训时长不少于 20 学时，并通过考核。

5.3.5.工作岗位轮换周期和顺序

对于可替换角色，CA 机构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.未授权行为的处罚

当 CA 机构员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 CA 系统或进行越权操作，CA 机构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 CA 机构内部的工作人员，但从事 CA 有关业务的人员等独立签约者，CA 机构的统一要求如下：

- a) 正规劳务公司派遣人员；
- b) 具有相关业务的工作经验；
- c) 必须接受 CA 组织的岗前培训。

5.3.8. 提供给员工的文档

为使得系统正常运行，CA 机构向其员工提供完成其工作所必须的文档。

5.4. 审计日志程序

5.4.1. 记录事件的类型

CA 机构记录与系统相关的事件，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、事件类型、事件的内容和事件相关的实体等。对系统的关键操作应由操作人员进行电子签名。

CA 机构记录的日志信息包括但不限于：

- a) CA 证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；
- b) 系统访问行为：所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；
- c) 系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；
- d) 网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；
- e) 证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；
- f) 机房门禁控制等物理环境事件：包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

5.4.2. 处理日志的周期

CA 机构建有 CA 应用系统的日志收集分析系统，实时收集应用日志并归档保存。CA 机构每季度对日志进行跟踪处理，对系统异常、未授权尝试访问、资源使用异常、配置变更等安全事件，排查潜在的安全隐患与合规风险，形成审计报告，并基于审计结果进行改进。

5.4.3. 审计日志的保存期限

与证书相关的审计日志至少保存到证书失效后五年。

5.4.4. 审计日志的保护

CA 机构授权的人员才能对审计日志进行相应操作。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。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

CA 系统审计日志备份采用数据库自身备份程序，根据记录的性质和要求，按照实时、每日、每周等策略进行备份。

5.4.6. 审计日志收集系统

审计日志收集系统涉及：

- a) 证书注册系统；
- b) 证书签发系统；
- c) 证书受理系统；
- d) 网站和数据库系统；
- e) 网络安全等其他需要审计的系统。

CA 机构使用审计工具满足对上述系统审计的各项要求。

5.4.7. 对导致事件实体的通告

CA 机构发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，CA 机构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。

CA 机构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

CA 机构每年对系统进行漏洞扫描和渗透测试等脆弱性评估，以降低系统运行的风险。

5.5. 记录归档

5.5.1. 归档记录的类型

CA 机构对以下记录进行归档，包括但不限于：

- 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) 密码设备日常操作与使用记录；
- e) CA 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. 归档记录的保存期限

与证书申请相关的归档记录保存期为证书失效后五年，与密码设备、CA 证书、CA 密钥相关的归档记录为永久保存，其余归档记录保存期为五年。

5.5.3. 归档文件的保护

CA 机构指定运营生产部门作为用户资料档案管理机构，制定用户资料档案管理制度，明确档案管理操作规范和安全要求。

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。CA 机构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 CA 主机房的存储库，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。CA 机构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. 归档收集系统

CA 系统的相关信息由自动归档备份系统收集和存储，并由具备相关权限的人进行管理。

5.5.6. 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6. 电子认证服务机构密钥更替

CA 证书有效期不超过 30 年，CA 密钥对的使用期限和 CA 证书有效期应保持一致。在 CA 证书到期前，数字认证公司将按照密钥安全管理制度对 CA 密钥进行更替，生成新的 CA 证书。

数字认证公司 CA 密钥更替方式如下：

- a) CA 证书到期时间小于订户有效期之前，应停止签发新的订户证书（“停止签发日期”）；
- b) 在屏蔽机房内产生新的密钥对，签发新的 CA 证书；生成过程详见 § 6.2.1
- c) 将新的 CA 公钥证书通过官网发布给订户和依赖方；
- d) 在“停止签发日期”之后，将采用新的 CA 密钥签发订户证书；
- e) 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。

CA 机构在 CA 密钥到期前两年完成 CA 证书密钥更替，当发生 CA 证书密钥泄露或存在安全隐患时，应立即启动密钥更替程序进行紧急更替。

5.7. 损害和灾难恢复

5.7.1. 业务连续性目标

CA 机构为确保业务的连续性，有效应对可能的损害和灾难，设定了业务连续性目标。恢复时间目标（RTO） ≤ 8 小时，恢复点目标（RPO） ≤ 30 分钟。为达成目标，CA 机构建设采用了本地热备方案和远程灾备方案，并制定了相应的损害与灾难恢复预案及流程。

5.7.2. 恢复流程

CA 机构应对损坏与灾难的恢复流程如下：

a) 证书库的恢复过程：证书库出现故障时，优先由本地热备设备接管服务，或启用远程热备站点接管服务。对故障中无法恢复的订户证书，应当进行撤销，生成受影响并被撤销的证书列表，通知订户为其重新签发公钥证书，对原证书进行撤销；对于 CA 机构托管的订户签名私钥，在征得订户同意后进行销毁；

b) 根密钥损害的恢复过程：当 CA 密钥遭受损害时，CA 机构将成立应急处理小组评估损害情况。若密钥未泄露，将在安全的本地屏蔽机房或异地屏蔽机房内使用备份密钥设备接管服务。如备份密码设备也遭受损害，将采购新密码设备，并在安全的本地屏蔽机房或异地内屏蔽机房内也开展密钥恢复；

若发生密钥泄露，CA 机构将启动密钥泄露应急响应机制，在安全的本地屏蔽机房或异地屏蔽机房内组织生成安全的密钥、签发 CA 证书，重新搭建 CA 系统。CA 机构组织通知订户和依赖方，提供新的 CA 证书与身份验证机制。CA 机构在征得订户同意后，将重新签发并交付订户证书。

c) 其他关键资产恢复过程：当 CA 机构遭到攻击，出现通信网络资源损坏、计算机设备系统服务异常、软件破坏、数据库被篡改等问题，或因不可抗力的灾难，CA 机构将按照业务连续性计划实施恢复，优先启用本地热备设备接管服务，也可采用远程热备站点接管服务。

5.7.3. CA 私钥应急处理

CA 机构已针对密钥泄露制定了相应的应急预案。在获知密钥泄露报告后，CA 机构将立即启动应急响应机制，并按流程逐级上报至安全策略管理委员会。安全策略委员会负责组织相关人员对泄露情况进行确认，确认后将组建应急处置小组，并于 24 小时内完成情况上报与通报。应急处置小组负责生成新密钥、签

发新的 CA 证书、通知受影响订户，并为其签发新的公钥证书。

CA 机构每年组织开展一次密钥泄露应急演练，并根据演练结果及实际工作需要，对预案进行合理修订。

5.7.4. 事件报告

详见 § 5.9 重大事项报告。

5.7.5. 定期验证

CA 机构每季度对备份设备和备份数据的可用性进行验证，包括对备份设备的功能测试以及对备份数据的恢复检验。此外，每年会组织开展一次灾难恢复演练，并根据演练结果与实际工作需求，对预案进行合理修订。

5.8. 电子认证服务机构的终止

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

CA 机构采用以下措施终止业务：

- a) 起草并发布 CA 终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；
- b) 选定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) 停止其他电子认证相关服务并归档相关数据；
- f) 停止密码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。



5.9. 重大事项报告

5.9.1. 重大事项范围

当发生以下任一情形时，本 CA 机构将上报公司管理层、上级机构和主管部门：

- a. 证书认证系统迁移或改造：
 - 机房迁移，或机房内服务区、管理区或核心区划设范围改变；
 - 变更电子签名认证证书签发逻辑；
 - 新增远程证书注册子系统；
 - 新增、变更或者删除用于签发电子签名认证证书的证书链；
 - 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：
 - 证书签发及验证服务连续停机时间超过 24h；
 - 发生 CA 证书密钥等相关数据泄露；
 - 持续或较大范围未经授权的私钥访问记录或者其他异常活动；
 - 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：
 - 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；
 - 数据丢失导致无法恢复证书状态信息。
- d. 合规性事件：
 - 涉及电子认证服务的司法判定；
 - 收到行政部门违规通知或处罚决定。
- e. 人力资源类事件：
 - 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；
 - 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。

5.9.2. 重大事项报告程序

当重大事件发生后，CA 机构中负有报告义务的人员应在知悉或应当知悉该事件的当日，立即通过书面形式、面谈、邮件或电话等方式，向相关责任方的直管领导及高层领导报告；同时需根据事件类型与级别进行分析判断，若按相关规定需上报上级机构和主管部门的，应当经安全策略委员会主任审批在三个工作日



内向上级机构报告，经安全策略委员会主任审批五个工作日内向主管部门报告。报告内容应包含但不限于以下信息：

- a) 重大事件的发生原因、基本情况及对公司经营的影响等；
- b) 所涉及的法律、法规、法院判决及相关情况说明等；
- c) 公司内部针对该重大事件的处置方法；
- d) 公司认为需要提供的其他材料。

6. 认证系统技术安全控制

6.1. 技术安全管理制度要求

CA 机构已建立涵盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，安全策略委员会每年至少开展一次评审。

6.2. 密钥对的生成和安装

6.2.1. CA 密钥对的生成和安装

CA 系统的密钥对是在屏蔽机房的密码机内部产生，密码机应具有商用密码产品认证证书。所有对 CA 密钥的操作，包括生成、备份、恢复、销毁等，经安全策略委员会审批后方可实施。在生成 CA 密钥对时，CA 机构按照密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 名密钥管理员，采用五选三控制机制，由密钥管理员凭借安全介质（如智能 IC 卡、USBKey）对密钥进行控制。密钥对生成全程由内部审计人员进行监督并录像，视频记录保存期限不少于操作完成后的十年。

6.2.2. 订户密钥对的生成和交付

（一）订户签名密钥对的生成、交付及控制方式要求

订户签名密钥对的生成、交付及控制方式，应符合以下三种要求之一：

- a) 由订户持有的符合国家安全标准的密码模块产生和存储；
- b) 由 CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权；
- c) 采用通过主管部门认可的其他创新保护方案。

（二）各类订户签名密钥对的生成、交付及控制方式

本 CPS 中各类电子签名认证证书订户签名密钥对的生成、交付及控制方式，

以及符合上述三种要求的规则方式如下：

a) 通用介质证书

通用介质证书订户签名密钥对的生成、交付及控制方式，符合“由订户持有的符合国家安全标准的密码模块产生和存储”的要求。其订户的签名密钥对在订户持有或指定的符合国家安全标准的证书载体中产生并存储，由订户直接控制实施电子签名。证书载体包括但不限于智能密码钥匙、密码设备、密码模块。加密密钥对由密钥管理中心生成，通过安全通道传到订户手中的证书载体中。

a) 云端协同证书

云端协同证书订户签名密钥对的生成、交付及控制方式分为协同运算生成和云平台生成两种方式。

协同运算生成的，符合“由订户持有的符合国家安全标准的密码模块产生和存储”的要求。订户签名密钥对分为终端密钥因子和云平台密钥因子，由订户持有的终端密码模块和云平台密码模块中协同运算生成，终端密码模块和云平台密码模块均符合国家安全标准。其中终端密钥因子由终端设备信息、用户知晓的控制因子、随机数等部分协同运算产生，需要终端与云平台协同运算才能完成订户签名密钥对的使用，确保只有持有该终端设备，并知晓用户密码的订户，才能使用签名密钥对实施电子签名，从而保护订户对签名密钥对的唯一控制。

云平台生成的，符合“由 CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权”的要求。订户签名密钥对在 CA 机构的云平台，由符合国家安全标准的密码模块生成，并保存在云平台密码模块中。CA 机构云平台提供安全措施确保仅订户可以唯一控制签名私钥。签名用户调用云平台的签名私钥实施电子签名时，CA 机构将通过安全授权认证机制，验证签名用户是签名私钥对应的证书订户本人或其授权的受托人，确保订户对签名私钥的独占控制权。

（三）CA 机构的记录规则

CA 机构参与保管订户签名私钥时，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，保存期限不少于证书失效后五年。

6.2.3. 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传递到 CA 机构。

从 RA 到 CA 以及从密钥管理中心到 CA 的传递过程中，采用符合国家安全标准的通讯协议及密钥算法，保证传输中数据的安全。

6.2.4. 电子认证服务机构公钥传送给依赖方

依赖方可以从数字认证公司的网站(<http://www.bjca.cn>)下载根证书和 CA 证书, 从而得到 CA 的公钥。

6.2.5. 密钥的长度

密钥算法和长度符合国家或行业相关安全标准要求, CA 机构对不符合要求的(如 RSA 密钥长度小于 2048 位、使用 MD5、SHA-1 等不安全算法)拒绝颁发证书。

6.2.6. 公钥参数的生成和质量检查

公钥参数由符合国家安全标准的密码设备或密码模块生成。对生成的公钥参数的质量检查, 同样由密码设备或密码模块进行, 这些设备内置的协议、算法等均符合国家或行业相关安全标准。

6.2.7. 密钥使用目的

订户的签名密钥可以用于身份认证、不可抵赖性和信息的完整性保护等, 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

CA 系统生成密钥的密码模块(密码机)安置在机房屏蔽区域的核心区, 使用通过商用密码产品认证的密码机, 且至少符合 GB/T37092-2018《信息安全技术密码模块安全要求》二级及以上。

CA 证书私钥的生成、更新、撤销、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 个管理员介质中, 只有其中超过半数以上管理员在场并许可的情况下, 才能对私钥进行上述操作。

CA 证书私钥备份由管理员分别存放在屏蔽机房的保险柜内。



6.3.2. 订户私钥保护和密码模块工程控制

订户签名私钥由订户自己保管的，订户应依据订户协议中的要求，采取预防措施防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用。

CA 机构受订户委托保管签名私钥的，采用的电子签名模式为 CA 机构的云平台响应订户的电子签名请求，订户通过云平台的验证后，调用云平台中托管的签名私钥实施电子签名。订户仅能通过安全授权认证（包括但不限于通过口令、短信验证码、生物识别信息、数字证书等）调用控制签名私钥，以确保签名私钥控制权由订户专有。CA 机构应每年对安全控制措施进行安全评估。CA 机构应向订户提供签名私钥及激活数据安全规范使用的指导，每次发起数字签名调用，必须取得订户明确授权，并完整留存相关授权记录。以上电子签名模式和安全控制措施具体应当符合相关标准或采用主管部门认可的其他方式。

订户加密证书对应的私钥由密钥管理中心托管，密钥管理中心严格保证订户密钥对的安全，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。

6.3.3. 私钥备份

CA 机构和密钥管理中心不备份订户的签名密钥。

加密私钥由密钥管理中心备份，备份数据以密文形式存在。

6.3.4. 私钥归档

订户加密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。

6.3.5. 私钥导入或导出密码模块

CA 私钥在硬件密码模块中产生。在需要备份或迁移 CA 私钥时，从密码模块中导出的私钥必须由多人控制。

CA 机构不提供订户私钥从密码设备或密码模块中导出的方法。

6.3.6. 私钥在密码模块中的存储

CA 私钥存储在符合国家安全标准的密码设备中，这些设备内置的协议、算



法等均符合国家或行业相关安全标准要求。

订户私钥在符合国家安全标准的密码设备或密码模块中加密保存。

6.3.7. 激活私钥的方法

CA 私钥存放在硬件密码设备中，具有激活私钥权限的管理员使用含有自己身份的安全介质（如智能 IC 卡、USBKey）登录，启动密钥管理程序，进行激活私钥的操作，需要超过半数以上的管理员同时在场。

订户证书私钥需在订户提供 PIN 码等激活数据，或通过安全授权认证（包括但不限于通过口令、短信验证码、生物识别信息、数字证书等）后才能被激活和使用。

6.3.8. 解除私钥激活状态的方法

对于 CA 私钥，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安全介质（如智能 IC 卡、USBKey）登录，启动密钥管理程序，进行解除私钥的操作，需要超过半数以上的管理员同时在场。

6.3.9. 销毁密钥的方法

对于 CA 私钥，具有销毁密钥权限的管理员使用安全介质（如智能 IC 卡、USBKey），通过 PIN 口令等授权访问措施登录并启动密钥管理程序，进行销毁密钥的操作，且在此过程中必须保证超过半数以上的管理员同时在场。在 CA 私钥销毁后，所有用于激活私钥的安全介质、PIN 口令等也必须被销毁或者收回。

6.3.10. 密码模块的评估

CA 机构使用通过检测认证的服务器密码机，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) 并发容量：可支持同时并发 100 个的独立安全处理容量；
- d) 密钥管理：密钥不以明文形式出现在服务器密码机以外；通信密钥通过身份鉴别后协商得到；
- e) 身份鉴别：采用安全介质（如智能 IC 卡、USBKey）对用户进行身份鉴



别管理，以控制对加密系统的使用；

f) 处理速度：数据加解密处理能力大于 100Mbps；

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。它们由 CA 机构和密钥管理中心定期归档，归档最大间隔不超过证书失效后五年。

6.4.2. 证书操作期和密钥对使用期限

CA 证书的有效期和其对应的密钥对的有效期一致，有效期最长不超过 30 年，CA 证书到期后，签名私钥不可用于电子签名。

订户证书的有效期和其对应密钥对的有效期保持一致，有效期最长不超过 5 年，订户证书到期后，签名私钥不可用于电子签名。

特殊情况下，对于签名证书，为验证在证书有效期内签名的信息，公钥可以在证书有效期限以外使用。

6.5. 激活数据

6.5.1. 激活数据的产生、传输和使用

激活数据用于保护订户的私钥。

CA 私钥的激活数据，必须按照密钥激活数据分割和密钥管理制度的要求，进行生成、分发和使用。

通用介质证书存储介质（如：智能密码钥匙）出厂时设置了缺省的 PIN 值，证书制作时更改此 PIN 值并通过安全的方式告知订户，订户可以自行设置或更改，订户自行设置 PIN 值应至少含 8 位字符且具有一定的复杂度。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。

云端协同证书应通过安全授权认证（包括但不限于通过口令、短信验证码、生物识别信息、数字证书等）激活私钥并使用私钥。

6.5.2. 激活数据的保护

CA 私钥的激活数据按照可靠的方式分割后，由不同的可信人员掌管，且掌

管人员必须符合职责分割的要求。

订户私钥的激活数据由订户采取妥善的方式保护，当发现激活数据失密，应告知 CA 机构并申请证书撤销。

6.5.3. 激活数据的销毁

当私钥的激活数据不需要时应该销毁，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或者全部，比如记录有口令的纸张必须粉碎。

6.6. 计算机安全控制

6.6.1. 计算机安全控制要求

为保障电子认证服务系统的安全稳定运行，防范计算机系统被攻击、入侵、病毒感染等安全风险，保护订户信息及证书相关数据的保密性、完整性和可用性，CA 机构建立并实施符合 GB/T 25056-2018 中 8.2 要求的计算机安全控制体系，实施全面的安全防护措施，具体要求包含但不限于以下内容：

- a) 系统升级补丁至少每半年检查一次，安装前需进行影响评估，经审批通过后方可实施，并做好审批及实施过程记录；
- 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，并定期更新病毒库；
- d) 每月进行病毒库更新，若遇到重大病毒爆发、新型病毒出现等特殊情况，手动触发病毒库紧急更新；
- e) 每周进行病毒扫描。

6.6.2. 计算机安全评估

CA 系统及其运行环境通过了国家密码管理局和工信部的审查，并取得了相应资质。

CA 系统使用的网络设备、主机、系统软件等均取得了国家有关认证检测机构出具安全标准的凭证。

6.7. 生存周期安全控制

6.7.1. 证书认证中心运行管理要求

CA 机构按照 GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》第 10 章要求建立证书认证中心运行管理体系。

6.7.2. 密钥管理中心运行管理要求

CA 机构按照 GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》第 11 章要求建立密钥管理中心运行管理体系。

6.7.3. 证书操作流程

CA 机构证书操作全流程遵循 GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》第 12 章规定，覆盖证书申请、更新、撤销、用户加密、密钥恢复、司法密钥恢复等全部环节。

6.8. 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。CA 机构按照 GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》中关于网络安全控制的要求执行。

- a) 网络结构：CA 机构的网络结构采用 B/S 模式，并依据规范进行网络配置；
- b) 网络安全防护：CA 机构对所有 Web 服务配置有防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施；
- c) 网络拓扑图：CA 机构应编制网络拓扑图，该图要体现所有网络设备、连接关系和安全边界，并定期更新，确保与机房实际情况保持一致；
- d) 网络访问控制：CA 机构应建立网络访问控制白名单机制，针对证书签发子系统及数据库的配置白名单，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问。针对证书注册子系统和数据库的也应配置访问控制白名单。
- e) 网络监控：CA 机构应对网络访问情况进行实时监控，并每月进行审计分析，分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9. 时间戳

CA 机构部署有时间戳服务，该服务仅面向外部客户使用，通过时间戳接口的方式对外提供服务。保障机制方面，时间戳系统部署于安全的机房环境，并采用防火墙保障服务安全；同时，采用冗余部署方式保证时间戳服务的高可用性。时间源采用国家授时中心提供的标准时间，并配备专业运营团队，定期进行系统维护、数据备份、安全审计。

时间戳服务在技术实现上应遵循 GB/T 20520《网络安全技术 公钥基础设施 时间戳规范》、GB/T 36631《信息安全技术 时间戳策略和时间戳业务操作规则》及国际标准时间戳协议（RFC3161）等技术标准。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

本 CA 机构签发的电子签名认证证书适用于企业信息化和电子商务等领域，可为订户提供身份认证、电子签名等服务。

订户可通过 CA 机构建立的数字证书注册通道提交证书申请，CA 机构按照本 CPS § 3 身份标识与查验的要求进行身份查验，查验通过后为订户签发证书，订户应妥善保管私钥和证书，或委托 CA 机构保管私钥。

本 CA 机构签发的数字证书符合《中华人民共和国电子签名法》、《电子认证服务管理办法》及《电子认证服务密码管理办法》等法律法规要求，本 CA 机构签发的数字证书格式符合 GB/T 20518《信息安全技术公钥基础设施 数字证书格式》的要求。

7.1.1. 版本号

X.509 V3。

7.1.2. 算法对象标识符

符合国家密码管理部门批准的算法对象标识符。

7.1.3. 证书序列号

证书序列号是 CA 分配给每张证书的一个十六进制正整数，且在 CA 的信任域内必须唯一。

7.1.4. 证书有效期

证书有效期是证书起始时间和终止时间的时间段，该时间段不应大于 CPS 对于证书有效期的规定。

7.1.5. 名称形式

数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录



唯一名字。除 C 项、E 项外，其余各项使用 UTF8String 编码。

CA 证书 DN 格式如下：

C=CN

O=××

OU= ××

CN=××

- C（Country）应为 CN，表示中国；
- O（Organization）中内容通常为 BJCA；
- OU（Organization Unit）中内容通常为 BJCA 或 CA 证书名称；
- CN（Common Name）中内容为 CA 机构定义的 CA 证书名称。

订户证书主体 Subject 的 X.500 DN 支持多级 O 和 OU，其格式可选择如下：

C=CN

S=××

L=××

O=××

O=××

OU= ××

OU=××

CN=××

- C（Country）应为 CN，表示中国；
- S（State）为可选项，S 中内容为省份；
- L（Locality）为可选项，L 中内容为城市/地区；
- O（Organization）为可选项，O 中的内容为证书主体或者证书主体所属单位名称全称；
- OU（Organization Unit）为可选项，OU 中的内容为证书主体或者证书主体所属部门的名称全称或简称；
- CN（Common Name）中的内容为：
 - a) 个人证书中应为证书主体的姓名，还可以包含其他标识信息；
 - b) 机构证书中应为证书主体机构的标准名称或简称，还可以包含其他标识信息（如机构证件代码等）。

订户不得使用可能侵犯他人知识产权的内容作为订户信息用于申请证书。CA 机构在受理证书申请时，查验记载在证书主体甄别名中的订户信息真实性，但并不验证该信息是否包含知识产权或处于知识产权纠纷中。

当发生有关知识产权的争议纠纷时，本CA机构有权拒绝相应的证书申请或撤销已发放的证书。

若证书 DN 中存在 E 项，应为证书主体的有效电子邮件地址。

7.1.6. 证书扩展项

CA 证书扩展项除使用 IETF RFC 5280 中定义的证书扩展项，还支持私有扩展项。

CA 采用的 IETF RFC 5280 中定义的证书扩展项：

- 颁发机构密钥标识符 Authority Key Identifier
- 主体密钥标识符 Subject Key Identifier
- 密钥用法 Key Usage：电子签名认证证书包含的密钥用法为数字签名（digitalSignature）、不可抵赖（nonRepudiation）
- 扩展密钥用途 Extended Key Usage
- 私有密钥使用期 Private Key Usage Period
- 主体可选替换名称 Subject Alternative Name
- 基本限制 Basic Constraints
- 证书策略 Certificate Policy：该项包含证书策略标识符，可区分证书等级和密钥存储方式（参考本 CPS § 1.3 的规定），该项还包含 CPS 发布地址
- 证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份证号码 Identify Card Number
- 企业营业执照（统一社会信用代码）IC Registration Number

对于涉及用户隐私数据的私有扩展项（如个人身份证号码、个人社会保险号码、银行基本帐号信息），应以这些信息的某种映射录入证书，包括但不限于散列值、掩码等。

7.1.7. 订户电子签名验证数据

订户的电子签名验证数据是指用于验证电子签名的公钥。

7.1.8. CA 电子签名

CA 机构在签发数字证书时，使用 CA 的私钥对证书内容的哈希值进行加密，生成数字签名。

7.1.9. 其他信息

订户和依赖方可以通过查看电子签名认证证书中的信息了解证书用途、建立的流程、签名私钥的保存方式和相关的法律符合性。其中：

- 证书用途可以根据证书扩展项中的密钥用法了解，digitalSignature 表示该证书的密钥可以用于数字签名，nonRepudiation 表示该证书的密钥可以用于保护签名行为的不可抵赖，同时查看证书扩展项中证书策略项，根据该项 OID 对应了解该证书是否为高等级电子签名认证证书，判断是否适用于涉及生命健康、财产权益等高风险活动。
- 建立的流程、签名私钥的保存方式，可以从证书扩展项证书策略获取 CPS 的发布地址，浏览 CPS 了解具体的建立流程和签名私钥的保存方式。
- 相关法律的符合性：可以查看证书扩展项中证书策略项，证书策略中如果记录了本 CPS § 1.5.1 中主管部门的证书策略 OID，则表明该证书符合《中华人民共和国电子签名法》对电子签名认证证书的法律规定。

7.2. 证书撤销列表

CA 签发的证书撤销列表符合 GB/T 20518《信息安全技术公钥基础设施 数字证书格式》中的相关要求。

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

7.3. 在线证书状态协议

CA 机构的在线证书状态服务符合 GB/T 19713《信息安全技术公钥基础设施 在线证书状态协议》的要求。

7.3.1. 版本号

使用 OCSP 版本 1（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

CA 机构制定有审计评估制度，制度内容包括不限于：

- a) 审计评估的类型分为认证业务审计、全面符合性评估及业务专项审计。
- b) 每季度执行一次认证业务审计，每年开展一次全面符合性评估，当发现业务风险事件时将执行业务专项审计评估。
- c) CA 机构内部参与执行审计评估人员需要具备电子认证法律法规、PKI 技术、运维、运营、信息安全等专业知识并在 CA 机构从业不少于 5 年的工作经历。外部审计则需审计机构具有信息安全服务认证资质、网络安全等级测评与检测评估机构服务认证资质、商用密码检测机构资质、会计师事务所资质等专业资格之一。
- d) 审计评估所涵盖的具体主题包括：人员管理审计、证书业务合规审计、运营服务审计、系统安全与运维管理审计等方面。全面符合性评估则依据电子认证法律法规、标准要求及本规则制定审计评估列表，并按审计评估列表逐条进行符合性评估。

8.2. 认证业务审计

CA 机构每季度开展一次认证业务审计，对业务全生命周期进行检查，包括证书申请、续期、密钥变更、更新、撤销等环节，并对各环节中的订户告知、身份查验、意愿记录、协议签署、资料保存情况进行合规性检查。

CA 机构开展审计工作一般采用全面审计或抽样审计，若抽样审计，审计抽样率不少于 0.01%。

在审计过程中发现的问题，将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

CA 机构依据法律、法规、标准要求及本规则至少每年开展一次开展全面符合性评估工作。

评估内容为 CA 机构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。CA 机构一般采用抽样审计，

审计抽样率不少于 0.01%。

在评估过程中发现的问题，将通知被审计部门及时整改，并跟踪整改落实情况。

CA 机构应在每年 1 月底前将上一年度符合性评估报告报送主管部门。

8.4. 评估者的资质

内部审计人员的选择一般包括：

- CA 的安全负责人及安全管理人员；
- CA 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。

8.5. 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。

9. 法律责任和其他业务条款

9.1. 费用

9.1.1. 电子认证服务相关费用

CA 机构可以根据提供的电子认证服务向订户收取相应的费用。就每一项服务的费用，CA 机构开展对应的成本核算，制定价格策略，同时市场相关部门对费用有规定的，依据规定执行。

证书颁发、证书续期（证书更新）、证书密钥更新、签名服务、电子签名验证报告服务的收费标准，CA 机构通过以下任意一种或多种方式公布：

- a) 在 CA 机构官方网站或自助服务平台公示收费标准；
- b) 在合同或订单中列明对应服务的收费标准或具体价格；
- c) 设立在线客服及热线电话，为公众提供与收费相关的咨询服务。

CA 机构可以根据市场需求，针对不同订户群体采取不同的费用策略或优惠措施，如果具体合同或订单中列明的价格与 CA 机构公布的不一致，以具体合同或订单中的价格为准。

为满足用户正当、合理的使用或信赖证书，目前 CA 机构不收取证书撤销、证书状态信息查询、CA 机构公开信息库的访问的服务费用，但对于用户提出的频繁、不合理等方式的服务使用，CA 机构保留收取费用的权利。同时，若用户提出特殊需求，需要 CA 机构订制各类服务的，CA 机构将于用户协商对应的费用。

9.1.2. 退款策略

在实施证书操作和签发证书的过程中，CA 机构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，CA 机构将不办理退证、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，CA 机构将不退还剩余时间的服务费用。

9.2. 财务责任

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

CA 机构的赔付能力资金保障方式为购买职业责任保险，确保资金保障额度

不低于上一年度营业收入 1.5%。赔付能力的具体资金来源，为根据保险合同，启动理赔获取的保险理赔资金。管理方式为公司定期设置职业责任保险预算，按周期购买职业责任保险，需要赔付时，按保险合同启动理赔程序。

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 CA 机构来说，保密信息包括但不限于以下方面：

- a) 最终用户的签名私钥都是保密的；
- 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) 除法律和行政法规规定外，其他由 CA 机构掌握的个人和公司信息，未经用户同意的视为保密。

CA 机构不保存任何证书应用系统的交易信息。

9.3.2. 不属于保密的信息

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，CA 机构可以选择公开。
- c) 订户数字证书的相关信息可以通过 CA 机构目录服务等方式向外公布，但 CA 机构认为涉及订户保密信息的除外。
- d) 其他可以通过公共、公开渠道获取的信息。

9.3.3. 保护保密信息的责任

a) 各方有保护自己和其他人员或单位的机密信息的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。

b) 当 CA 机构在任何法律、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，CA 机构应按要求，向执法部门公布相关的保密信息，CA 机构无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4. 个人隐私保护

依据相关法律、法规，CA 机构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/或经办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。本《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数字认证公司网站公布的《个人信息保护政策》。CA 机构根据有关法律法规和 GB/T 35273《信息安全技术 个人信息安全规范》，针对用户隐私信息提供如下保障措施。

9.4.1. 隐私保护方案

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

CA 机构应保护证书申请人所提供的、证明其身份的资料。CA 机构应采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

CA 机构将实施信息安全管理制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. 个人隐私信息的收集

根据《电子签名法》第二十条规定，CA 机构作为合法的第三方电子认证服务机构，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查验。CA 机构要求用户即证书申请人申请证书时通过纸质材料、电子材料或证书服务系统在线交互等方式提供能够证明其真实身份的证明材料。CA 机构在《电子认证服务协议》等相关协议中已明确告知用户 CA 机构对用户包含但不限于用户个人的姓名、证件号码、住址、联系方式等信息进行收集。

与 CA 机构建立证书服务合作的合作方，CA 机构要求合作方建立收集用户

个人信息的管理制度，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。

CA 机构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。

9.4.3. 个人信息的存储

CA 机构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，但该措施并不排除在 CA 机构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。

9.4.4. 个人信息的使用

订户的个人信息仅用于证书服务或证书各类应用有关的用途，以及取得用户同意的用途，除非符合法律、行政法规、部门规章规定的情形，CA 机构不会将订户个人信息用上述用途之外的其他场景。

9.4.5. 个人信息的共享

CA 机构不会以商业目的或未取得用户自身同意或授权的情况下向其他组织或个人提供订户的个人信息，除非符合法律、行政法规规定的情形，如依据法律规定，就电子签名真实性存在争议的诉讼、仲裁等活动中履行提供证据的义务。

CA 机构可以为实现有效查验订户真实身份的目的，委托相关身份核验技术厂商或权威数据平台，核验订户信息。但该数据处理行为属于个人信息的委托处理，不属于信息共享的情形。

9.4.6. CA 对于用户个人信息的管理

CA 机构通过以下措施规范用户个人信息的内部管理：

- 1、CA 机构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；
- 2、CA 机构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。

9.4.7. 个人信息的查阅

订户如需查询本人证书有关的个人信息，除直接通过证书内容查阅外，可以联系 CA 机构官方网站公布的联系方式联系 CA 机构查询。

CA 机构在响应查询申请时，为保护个人隐私，有权要求查询申请人配合证明其身份。

9.4.8. 个人信息的删除和更改

1、个人信息的删除

CA 机构可以根据法律规范的规定，或基于订户本人的申请，删除或销毁订户的个人信息，但《电子签名法》《电子认证服务管理办法》及其他法律法规规定 CA 机构应当妥善保存的信息除外。

2、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 日内向 CA 机构提出变更申请；由于用户自身原因未及时将变更信息通知 CA 机构的，由此发生的风险由用户自身承担。

9.5. 知识产权

除非额外声明，CA 机构享有并保留对证书以及 CA 机构提供的全部软件的一切知识产权，包括但不限于所有权、名称权、著作权、专利权和利益分享权等。CA 机构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 CA 机构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数字认证公司所有，这些知识产权包括所有相关的文件和使用手册。

9.6. 陈述和担保

9.6.1. 电子认证服务机构的陈述与担保

CA 机构在提供电子认证服务活动过程中的承诺如下：

a) CA 机构遵守《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领导，对签发的数字证书承担相应的法律责任。

b) CA 机构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 CA 机构证书库发出了 CA 的私钥被破坏或被盗的通知，CA 机构保证其私钥是安全的。

d) CA 机构签发给订户的证书符合 CA 机构的 CPS 的所有实质性要求。

e) CA 机构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，通报的有效形式包括但不限于邮件通知、官网公告。

f) CA 机构将及时撤销证书。

g) CA 机构拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

h) 证书公开发布后，CA 机构向证书依赖方证明，数字证书中载明的订户信息都是准确的。

9.6.2. 订户的陈述与担保

订户一旦接受 CA 机构签发的证书，就被视为向 CA 机构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 CA 机构检查和核实。

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、泄露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 CA 机构，申请采取撤销等处理措施。

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 CA 机构撤销其证书。

9.6.3. 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电子签名的有效性。

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。

9.6.4. 其他参与者的陈述与担保

其他参与者的陈述与担保同 9.6.3。

9.7. 担保免责

9.7.1. 责任免除

有下列情况之一的，应当免除 CA 机构之责任。

a) 订户在申请和使用 CA 机构数字证书时，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 CA 机构。如因材料或信息变更未及时通知 CA 机构，给订户本人或第三方造成的损失，CA 机构不承担责任；

(2) 订户应当妥善保管 CA 机构所签发的数字证书载体、私钥、保护密码 PIN 及云端协同证书身份凭证的安全，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 CA 机构及相关各方，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 CA 机构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、被撤销的数字证书；

(7) 订户有义务根据规定按时向 CA 机构交纳服务费用。

b) 由于下列依赖方的原因造成的损失，CA 机构不承担任何赔偿责任，由依赖方自行承担。

(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。关于不可抗力的描述参见 § 9.16.4。



d) 因 CA 机构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 CA 机构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，CA 机构将不对订户或依赖方承担任何赔偿或补偿责任。

9.7.2. 隐含的担保责任

为明确 CA 机构电子认证服务的责任边界，杜绝任何隐含担保意思表示的误解，特明确：本 CA 机构的所有业务表述、服务承诺及与证书持有人、依赖方签订的各类协议、告知书等，仅约定电子认证服务相关权利义务，不包含任何隐含担保、事实保证，亦不产生任何隐含担保责任。

9.7.3. 担保免责的适用规定

CA 机构的担保免责条款，仅适用于电子认证服务相关的担保责任免除，免责条款的适用不得违反法律、行政法规的强制性规定，不得损害国家利益、社会公共利益及第三方合法权益，违法无效的免责约定不适用。

9.8. 赔付责任规则

9.8.1. 赔偿责任范围

如出现下述情形，CA 机构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，CA 机构签发的证书含有错误信息，导致订户或依赖方由此遭受损失；

b) 由于 CA 机构原因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) 对于订户申请撤销的证书，CA 机构未能及时撤销证书由此导致依赖方遭受损失。

CA 机构只在证书有效期限内承担损失赔偿责任。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年内向 CA 机构书面提出索赔。

9.8.2. 赔偿责任限额

CA 机构对所有当事实体（包括但不限于订户、信赖方）的合计责任不超过该特定证书适用的赔偿责任上限。对于一份证书产生的所有数字签名和交易处理，CA 机构对于任何实体有关该特定证书赔偿的合计责任应该限制在一个不超过下述赔偿责任上限的范围内。这种赔偿上限可以由 CA 机构根据情况重新制定，CA 机构会将重新制定后的 CPS 公布于 CA 机构网站（<https://www.bjca.cn>）以通知相关当事人。如在本 CPS 公布修订的 1 个月后继续使用 CA 机构提供的数字证书服务，即表明同意接受此等修订的约束。如果不予接受本 CPS 中的约束，订户可以停止使用证书或在上述期限内以书面形式向 CA 机构申请撤销证书。

CA 机构所颁发数字证书的赔偿责任上限如下：

个人电子签名认证证书：800 元人民币。

机构电子签名认证证书：4000 元人民币。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有上限而不考虑电子签名和交易处理等有关的其他索赔的数量。当超过责任上限时，可用的责任上限将首先分配给最早得到索赔解决的一方。CA 机构没有责任为每份证书支付高出责任上限的赔偿，而不管责任上限的总量在索赔提出者之间如何分配的。

赔偿的计算方式如下：

具体赔偿金额的计算，按本 CPS § 9.9 规定的程序，审核评估属于 CA 机构赔偿责任范围内真实合理的损失数额。损失数额不高于赔偿责任上限的，赔偿金额计算参考损失数额，损失数额高于赔偿责任上限的，赔偿金额按赔偿责任上限计算。

9.8.3. 赔付监督机制

订户提交赔付申请且 CA 机构受理后，为保障订户的合法权益，赔偿事件调查小组将对赔付流程全程跟进监督，赔偿事件结案后，CA 机构负责对赔偿事件相关记录、证据材料等及时整理、归档。

若订户对 CA 机构的赔付结论或执行结果有异议，则通过司法程序解决。

9.8.4. 有限责任

a) CA 机构所有的赔偿义务不得高于本 CPS § 9.8.2 规定的赔偿责任上限。



b) CA 机构根据判决或裁定应当承担赔偿或补偿责任的, CA 机构将按照法院的判决、仲裁机构的裁定承担相应的赔偿或补偿责任。

c) 无论本 CPS 是否有相反或不同规定, 就以下损失或损害, CA 机构不承担任何赔偿和/或补偿责任:

(1) 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件;

(2) 由上述第(1)项所述的损失相应生成或附带引起的损失或损害;

(3) 非 CA 机构的行为而导致的损失;

(4) 因不可抗力而导致的损失, 如罢工、战争、灾害、恶意代码病毒等。

9.9. 赔偿

CA 机构按照本《电子认证业务规则》§ 9.8 条款承担赔偿责任。

9.9.1. 赔偿申请流程

CA 机构在接到证书订户或依赖方提出的赔偿诉求时, 先对申请人的基本情况、赔偿的诉求与理由、相关证据等进行收集、整理并做书面记录, 形成《证书赔偿事件记录》。

CA 机构应当在收到申请人的赔偿诉求后十个工作日内做出处理。申请人的相关赔偿申请信息与材料充分完整的, 应予受理; 信息与材料不完整的, 应通知申请人进行补足; 发现赔偿申请不合理、虚假、无效或存在其他不应受理情形的, 拒绝申请人的赔偿申请。

9.9.2. 赔偿审核流程

CA 机构对赔偿事件进行调查取证, 核查赔偿申请是否属实、是否造成损害、申请的赔偿数额是否合理等, 同时成立赔偿事件调查小组并组织召开赔偿事件分析会, 依据赔偿事件记录、证据材料等, 对赔偿事件进行研判。包括:

(一) 证书订户或依赖方是否具有符合《电子签名法》的规定的主体资格;

(二) 请求赔偿的时效情况;

(三) 造成的实际损害;

(四) 计算赔偿金, 确定赔偿方式, 提出拟处理建议。

赔偿审核一般情况下应在六十个工作日内完成, 情况复杂需要延期的, 应当通知申请人原因以及需要延长的审核时间。

9.9.3. 赔偿审批流程

CA机构在赔偿事件分析会后5个工作日内形成《证书赔偿事件分析报告及处置方案》，并根据赔偿事件的分级逐级上报审批。赔偿审批一般情况下应当在30个工作日内完成，上级单位对赔偿审批有特别规定的，按其规定执行。

9.9.4. 赔偿支付流程

CA机构与证书订户或依赖方就赔偿事项达成一致的，与其签订《证书赔偿处置协议书》。财务部依据双方签署的《证书赔偿处置协议书》和赔偿费用支付流程，向证书订户或依赖方支付赔偿费用。

赔偿事件调查小组自双方签署《证书赔偿处置协议书》或者作出不予赔偿决定之日起一个月内形成《证书赔偿事件结案报告》，完成赔偿支付流程。赔偿事件结案后，CA机构对赔偿事件相关记录、证据材料等及时归档。

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。

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》自动到期。

9.10.2. 效力的终止与保留

对于旧版本的《电子认证业务规则》到期之后新签发的证书，旧版本的《电子认证业务规则》的效力全部终止，按新版本的文档执行。

对于旧版本的《电子认证业务规则》到期之前已经签发的证书，旧版本的《电子认证业务规则》中涉及CA机构为相关方提供的查询等支持服务的部分效力终止，按新版本的文档执行。

对于订户和依赖方，应当遵守对应证书签发时生效版本的《电子认证业务规则》，且不因该版本《电子认证业务规则》到期而终止。但与CA机构专门订立合同，约定《电子认证业务规则》版本适用条件的特定参与者，按合同约定决定相应版本的《电子认证业务规则》适用或终止。

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必须使用安全通道, 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, 由数字认证公司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, 数字认证公司安全策略管理委员会进行审批, 审批通过后将在数字认证公司的网站(<http://www.bjca.cn>)上发布新的《电子认证业务规则》。

《电子认证业务规则》将进行严格的版本控制。

9.12.2. 通告机制和期限

本《电子认证业务规则》在数字认证公司的网站(<http://www.bjca.cn>)上发布。

版本更新时, 最新版本的《电子认证业务规则》在数字认证公司的网站发布, 对具体个人不做另行通知。

9.12.3. 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时, 必须修改《电子认证业务规则》。

9.13. 争议处理与举证

9.13.1. 争议处理

就电子认证服务活动及 CPS 规则执行的范围中, 证书订户、依赖方等实体与 CA 机构产生的争端按照以下步骤解决:

a) 相关方首先通知 CA 机构, 就涉及的电子认证服务活动, 具体争议问题进行沟通;

b) CA 机构将根据本 CPS, 确定是否属于电子认证服务相关争议, 争议中的分歧、责任等事项;



c) 各方应通过友好协商解决，CA 机构在协商过程中，应合理、及时的与相关方沟通解决。协调不成的，可以通过法律途径解决。

d) 针对争议，CA 机构与各方的协商时限，原则上不超过 60 个工作日。超过的，任何一方可以通过法律途径解决。

任何与 CA 机构在电子认证活动中产生的任何争端及或对本《电子认证业务规则》所产生的任何争议，均应提请北京仲裁委员会按照其仲裁规则在北京进行仲裁。仲裁裁决是终局的，对双方均有约束力。

9.13.2. 举证

CA 机构建立完善的管理制度及能力体系，覆盖证书全生存周期，满足举证需求，具体包括：

a) 证书签发环节完整留存身份验证记录、材料审查记录、告知记录、意愿确认记录等相关资料，留存期限不低于电子签名认证证书失效后 5 年；

b) CA 机构代订户生成并保管签名私钥的（如云端协同证书），CA 机构应详细记录签名请求验证、签名操作日志等签名环节信息；

c) 验证签名环节妥善留存签名验证请求记录、验证结果记录、异常情况处理记录等；

d) 提供举证材料的时间承诺，有相关法律法规规定，或双方约定的，CA 机构按法律规范或约定的时间提供。没有规定或约定的，CA 机构承诺一般情况下提供举证材料的时间不超过 10 个工作日。特殊情况，如调取的材料数量过多、涉及多笔不同证书服务业务的，提供举证材料的时间可以合理延长。

申请方提出的向 CA 机构调取上述证据的需求，应当符合法定及约定条件的，证据调取涉及申请方之外的他人个人信息，或商业秘密的，CA 机构有权依法进行保密处理。

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. 与适用法律的符合性

无论在任何情况下，本《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大陆地区的法律法规，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》及《电子认证服务密码管理办法》。

9.16. 一般条款

9.16.1. 完整规定

《电子认证业务规则》的全部文档包括《电子认证业务规则》的标题、版本控制表、目录、正文等主体内容。

本《电子认证业务规则》将替代先前的或同时期的相关文档。电子认证服务协议、依赖方协议中明确标明对应的 CPS 版本。

9.16.2. 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

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，CA 机构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

数字认证公司对本《电子认证业务规则》拥有最终解释权。