中金金融认证中心有限公司
电子认证业务规则
CFCA Certification Practice Statement
(第六版)

中金金融认证中心有限公司

版权声明：本文档版权属于中金金融认证中心有限公司。任何组织或个人未经许可不得擅自修改、传播或用于商业用途。

版本修订记录

版本	修订说明	修订人	批准人	修订日期
3.0	1. 声明了 J-01 系统下线策略; 2. 增加了 CS 体系的说明; 3. 增加了场景证书及复合证书等说明，将原电子认证业务规则版本升级为 V3.0 版本。	CP/CPS 编写组	CFCA 安全委员会	2015 年 8 月
3.1	补充了 ACS CA 系统的说明。	CP/CPS 编写组	CFCA 安全委员会	2015 年 10 月
3.2	补充了云证通证书等说明。	CP/CPS 编写组	CFCA 安全委员会	2016 年 6 月
3.3	对本证书体系涉及的新建子 CA 系统进行补充；对 GT 系统下的 OCA21 CPS 变更调整进行了说明。	CP/CPS 编写组	CFCA 安全委员会	2017 年 10 月
3.4	增加了对《粤港电子签名证书互认证书策略》适应性扩展项，以及相关算法适应性描述。	CP/CPS 编写组	CFCA 安全委员会	2018 年 11 月
4.0	1. 增加关于 CFCA 证书分级的策略及 OID 说明; 2. 增加了关于证书中含有商标标识时的处理办法; 3. OCSP 遵从的标准修改为 RFC6960; 4. DN 描述及组成规则从 CPS 中删除，将在 DN 规则中统一描述; 5. 增加附录 B（本 CPS 下 CA 说明）; 6. 文档内容错误修订。	CP/CPS 编写组	CFCA 安全委员会	2019 年 5 月

5.0	对 4.0 版本进行了修订: 1. 明确了遵循的法律法规及标准规范; 2. 对 4.0 版本进行补充完善; 3. 进一步健全 4.0 版本，补充附件内容。	CP/CPS 编写组	CFCA 策略管理委员会	2025 年 8 月
6.0	根据团体标准 T/CQAE 11034—2025《电子认证业务规则规范》 进行修订: 1. 增加证书分类分级规则，明确高等级证书、基础级证书业务规则; 2. 修订订户告知与意愿确认规则; 3. 修订订户身份查验规则; 4. 修订证书申请与签发规则; 5. 增加密钥管理规则; 6. 增加偿付责任。	CP/CPS 编写组	CFCA 安全策略委员会	2026 年 6 月

目 录

1. 概括性描述 1
1.1. 承诺 1
1.2. 基本信息 1
1.3. 文档名称与标识 3
1.4. 电子认证活动参与者 3
1.4.1. 电子认证服务机构 4
1.4.2. 订户 4
1.4.3. 依赖方 4
1.4.4. 其他参与者 4
1.5. 证书应用 4
1.5.1. 证书应用分类 4
1.5.1.1. 个人证书 4
1.5.1.2. 机构证书 6
1.5.1.3. 网络应用证书 7
1.5.2. 证书应用限制 8
1.6. 策略管理 9
1.6.1. 策略管理机构 9
1.6.2. 策略文档的批准程序 10
1.7. 定义和缩写 11
2. 信息发布与信息管理 15
2.1. 信息发布 15
2.2. 信息管理 17
3. 身份标识与查验 18
3.1. 身份查验通用要求 18
3.1.1. 通用要求 18
3.1.2. 订户告知 18
3.1.2.1. 告知内容 18
3.1.2.2. 告知方式 19

3.1.2.3. 高等级电子签名认证证书订户告知 19
3.1.2.4. 基础级电子签名认证证书订户告知 19
3.1.2.5. 其他类型证书订户告知 19
3.2. 初始身份确认 20
3.2.1. 证明拥有私钥的方法 20
3.2.2. 个人身份的查验 20
3.2.2.1. 个人身份信息有效性的确认 20
3.2.2.2. 个人订户实人查验方式 21
3.2.2.3. 个人高等级证书的实人查验 22
3.2.2.4. 个人基础级证书的实人查验 22
3.2.2.5. 个人其他类型证书的实人查验 22
3.2.3. 机构身份的查验 22
3.2.3.1. 机构身份信息有效性的确认 22
3.2.3.2. 机构高等级证书的实人查验 23
3.2.3.3. 机构基础级证书的实人查验 23
3.2.3.4. 机构其他类型证书的实人查验 24
3.2.4. 网络应用证书订户身份查验 24
3.2.5. 订户身份查验特别说明 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 25
3.3.2.1. 个人高等级证书的意愿记录 25
3.3.2.2. 个人基础级证书的意愿记录 25
3.3.2.3. 个人其他类型证书的意愿确认 26
3.3.3. 机构证书的意愿记录 26
3.3.3.1. 机构高等级证书的意愿记录 26
3.3.3.2. 机构基础级证书的意愿记录 26
3.3.3.3. 机构其他类型证书的意愿确认 27
3.3.4. 网络应用证书的意愿确认 27

3.4. 订户协议 27
3.5. 未验证的订户信息 27
3.6. 互操作要求 28
3.7. 命名 28
3.7.1. 命名规则 28
3.7.2. 名称唯一性 29
3.7.3. 商标权的处理策略 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 31
4.2.1. 证书申请实体 31
4.2.2. 证书申请程序 31
4.2.3. 证书申请处理时限 32
4.3. 证书签发 32
4.3.1. 证书签发程序 32
4.3.2. 证书签发结果通告 32
4.4. 证书接受 33
4.5. 证书和密钥对的使用 34
4.5.1. 交付前的安全保护 34
4.5.2. 私钥管理服务要求 34
4.5.3. 安全事件反馈 35
4.5.4. 订户对证书及私钥的使用 35
4.5.5. 依赖方对证书及公钥的使用 35
4.6. 证书续期 36
4.7. 证书密钥更新 36
4.8. 证书变更 37
4.9. 证书撤销或冻结 37
4.9.1. 证书撤销的情形 37
4.9.1.1. 订户撤销证书的情形 37

4.9.1.2. 本机构撤销证书的情形 38
4.9.1.3. 其他参与者撤销证书的情形 39
4.9.2. 证书撤销程序 39
4.9.2.1. 订户撤销证书程序 39
4.9.2.2. 本机构撤销证书程序 40
4.9.2.3. 其他参与者撤销证书程序 40
4.9.3. 依赖方检查证书撤销的要求 40
4.9.4. 证书冻结及解冻 40
4.9.4.1. 证书冻结程序 41
4.9.4.2. 证书解冻程序 41
4.9.5. 其他说明 41
4.10. 证书状态信息服务 42
4.11. 停止使用认证服务 42
4.12. 密钥托管与恢复 43
5. 认证机构设施、管理和操作控制 44
5.1. 物理控制 44
5.1.1. 基础设施 44
5.1.2. 分区管理与访问控制 44
5.1.3. 电力与空调 45
5.1.4. 门禁与监控 45
5.1.5. 灾备 45
5.1.6. 环境保障措施 45
5.1.7. 消防措施 45
5.1.8. 设备管理 45
5.1.9. 存储媒体管理 46
5.2. 操作过程控制 46
5.2.1. 可信角色 46
5.2.2. 职责分离 48
5.3. 人员控制 49

5.3.1. 可信人员资格要求 49
5.3.2. 可信人员培训要求 49
5.4. 审计日志程序 50
5.4.1. 记录范围 50
5.4.2. 记录内容 51
5.4.3. 保存期限 51
5.4.4. 日志审计内容 51
5.4.5. 审计周期 52
5.5. 记录归档 52
5.5.1. 归档范围 52
5.5.2. 保存期限 52
5.5.3. 保护措施 52
5.6. 电子认证服务机构根证书密钥更替 53
5.6.1. 密钥更替的时间 53
5.6.2. 密钥更替程序 53
5.7. 损害与灾难恢复 53
5.7.1. 业务连续性目标 53
5.7.2. 恢复流程 53
5.7.3. 根私钥泄露应急处理 54
5.7.4. 事件报告 54
5.7.5. 定期验证 54
5.8. 电子认证服务机构终止 54
5.9. 重大事项报告 56
5.9.1. 重大安全事件 56
5.9.2. 重大安全事件报告程序 57
6. 认证系统技术安全控制 59
6.1. 技术安全管理制度要求 59
6.2. 密钥对的生成和安装 59
6.2.1. 根证书密钥对的生成和安装 59

6.2.2. 订户密钥对的生成和交付 59
6.3. 私钥保护和密码模块工程控制 60
6.3.1. CA 私钥保护和密码模块工程控制 60
6.3.2. 订户私钥保护和密码模块工程控制 61
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 62
6.5.1. CA 私钥激活数据的保护 62
6.5.2. 订户私钥激活数据的保护 62
6.6. 计算机安全控制 62
6.7. 生存周期安全控制 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. 证书基本项 65
7.1.2. 版本号 65
7.1.3. 序列号 65
7.1.4. 签名算法 65
7.1.5. 颁发者 66
7.1.6. 有效期 66
7.1.7. 主体 66
7.1.8. 主体公钥信息 66
7.1.9. 证书扩展项 66
7.1.9.1. 颁发机构密钥标识符 67
7.1.9.2. 主体密钥标识符 67
7.1.9.3. 证书策略及对象标识符 67
7.1.9.4. 机构信息访问 68

7.1.9.5. 基本限制 68
7.1.9.6. 密钥用法 68
7.1.9.7. 扩展密钥用法 69
7.1.9.8. CRL 分发点 69
7.1.9.9. 主体替换名称 69
7.1.9.10. 关键证书策略扩展项的处理规则 69
7.2. 证书撤销列表 70
7.3. 在线证书状态协议 70
8. 认证机构审计及相关评估 71
8.1. 审计评估制度 71
8.2. 认证业务审计 71
8.3. 全面符合性评估 72
9. 法律责任和其他业务条款 73
9.1. 费用 73
9.2. 财务责任 73
9.3. 业务信息保密 74
9.3.1. 保密信息范围 74
9.3.2. 不属于保密的信息 74
9.3.3. 保密信息的保护责任 75
9.4. 个人隐私保护 75
9.5. 知识产权 75
9.6. 陈述和担保 76
9.6.1. 本机构的陈述与保证 76
9.6.2. 订户的陈述、保证与义务 76
9.6.3. 依赖方的陈述、保证与义务 78
9.6.4. 其他参与者的陈述与保证 79
9.7. 担保免责 79
9.8. 偿付责任规则 80
9.9. 赔偿 81

9.10. 有效期和终止 81
9.11. 对参与者的个别通告与沟通 81
9.12. 修订和发布 82
9.13. 争议处理与举证 82
9.14. 管辖法律 83
9.15. 与适用法律的符合性 83
9.16. 一般条款 83
9.17. 其他条款 84
附录：CFCA 电子认证系统及证书链 85

前　言

中金金融认证中心有限公司（China Financial Certification Authority，简称 CFCA），是由中国人民银行于 1998 年牵头组建，经国家信息安全管理机构批准成立的权威电子认证机构，持有工业和信息化部颁发的《电子认证服务许可证》及国家密码管理局颁发的《电子认证服务使用密码许可证》。

《中华人民共和国电子签名法》规定：电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。《电子认证服务管理办法》规定：电子认证服务机构应当按照工业和信息化部公布的《电子认证业务规则规范》等要求，制定本机构的电子认证业务规则和相应的证书策略，在提供电子认证服务前予以公布，并向工业和信息化部备案。

依据前述法律法规要求，CFCA 制定《电子认证业务规则》（Certification Practice Statement，简称 CPS），并向工业和信息化部备案。本 CPS 适用于电子认证服务机构、订户、依赖方等电子认证活动参与者。CFCA 按照 CPS 开展电子认证服务，各参与者应充分理解 CPS，承担相应的责任和义务。

版本修订说明（2026 年 6 月）

本次修订依据团体标准 T/CQAE 11034—2025《电子认证业务规则规范》对相关业务规则进行调整。

本次修订的主要内容：一是增加证书分类分级管理，明确高等级证书与基础级证书的业务规范；二是优化完善订户告知与意愿确认、订户身份查验、证书申请及签发等环节业务规则；三是健全密钥管理机制，明确订户签名私钥管理要求与技术保障措施；四是建立偿付责任规则，明确赔付专项备用资金保障方式，压实主体责任与风险兜底。

1. 概括性描述

1.1. 承诺

中金金融认证中心有限公司作为权威电子认证服务机构，依据《中华人民共和国电子签名法》《电子认证服务管理办法》及本机构《电子认证业务规则》，郑重作出如下承诺:

一、合规经营，践行责任。开展电子认证经营与服务活动时，严格遵守国家法律、行政法规，坚守以人民为中心的服务理念，主动承担数字信任体系建设、金融信息安全保障等社会责任。

二、严审准入，防控风险。与应用方建立业务关系前，全面开展应用业务调研，建立应用接入业务风险评估及内部定责机制，坚决不为存在违法违规风险的业务提供电子认证服务。

三、合规用密，保障安全。始终采用经国家密码管理局审查通过的电子认证服务系统开展电子认证服务，严格遵循密码管理相关规定，确保电子认证服务的安全性、可靠性与合规性。

四、接受监督，长效治理。主动接受政府主管部门监管与社会公众监督，对检查发现的问题及时、全面整改；建立问题纠治长效机制，持续优化业务流程与管理体系，确保电子认证服务长期符合监管要求。

中金金融认证中心有限公司严格恪守上述承诺，诚恳接受社会各界监督。

1.2. 基本信息

中金金融认证中心有限公司（China Financial Certification Authority，简称 CFCA），是由中国人民银行于 1998 年牵头组建，

经国家信息安全管理机构批准成立的权威电子认证机构，持有工业和信息化部颁发的《电子认证服务许可证》及国家密码管理局颁发的《电子认证服务使用密码许可证》。

本机构基本信息如下：

机构名称	中金金融认证中心有限公司
法定代表人	赵海
机构地址	北京市西城区平原里小区 20 号楼 1 层 1-7、2 层 1-9、3 层 1-10
	北京市西城区菜市口南大街平原里 20-3
联系电话	400-880-9888
投诉电话	010-87549600
网站地址	https://www.cfca.com.cn
电子邮箱	cps@cfca.com.cn

本机构《电子认证服务许可证》如下：

证书名称	《电子认证服务许可证》
证书编号	ECP11010420002
发证机关	工业和信息化部
批准日期	2005 年 8 月 19 日
有效期起止时间	2020 年 8 月 19 日至 2025 年 8 月 18 日（换证中）

本机构《电子认证服务使用密码许可证》如下：

证书名称	《电子认证服务使用密码许可证》
证书编号	0008
发证机关	国家密码管理局

批准日期	2005 年 5 月 20 日
有效期起止时间	2025 年 3 月 1 日至 2030 年 2 月 28 日

本机构发布的电子认证系统（简称 CA 系统）及证书链详见附录《CFCA 电子认证系统及证书链》。本机构的所有 CA 系统（含子 CA 系统）均由本机构所有并直接管控。

1.3. 文档名称与标识

本文档为 CFCA《电子认证业务规则》第六版（简称本 CPS）。

本 CPS 遵循 CFCA《电子认证业务证书策略》第六版及广东省人民政府《粤港电子签名证书互认证书策略（1.1 版本）》的相关要求。

本 CPS 历史版本相关信息详见本文档版本修订记录。

本文档及关联文档的对象标识符(Object Identifier,简称 OID)如下:

OID	说明
2.16.156.112554.1	CFCA《电子认证业务规则》文档标识
2.16.156.112554.10	CFCA《证书策略》文档标识

本 CPS 引用的法律法规、标准规范、内部管理文档及其他规范性文件中，凡是标注日期的引用文件，仅以标注日期的版本适用于本 CPS；凡是未标注日期的引用文件，以其最新版本适用于本 CPS。

本 CPS 中含有“应”的约束性条款，均为相关各方必须遵照执行的强制性要求。

1.4. 电子认证活动参与者

本 CPS 所涵盖的电子认证活动参与者包括：电子认证服务机构、

订户、依赖方及其他参与者，具体如下:

1.4.1. 电子认证服务机构

电子认证服务机构（Certificate Authority，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、可靠性验证的实体。本 CPS 电子认证服务机构仅指 CFCA。

1.4.2. 订户

订户是指被电子认证服务机构颁发数字证书的实体。

1.4.3. 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实体。

1.4.4. 其他参与者

其他参与者是指除上述参与者以外，参与电子认证服务相关活动的各类实体。

1.5. 证书应用

1.5.1. 证书应用分类

本机构签发的证书按照证书主体对象，分为个人证书、机构证书、网络应用证书。

1.5.1.1. 个人证书

个人证书是以数字形式存在的自然人电子身份凭证，用于在网络环境中标识自然人真实身份信息，可实现身份认证、电子签名、数据加密、行为抗抵赖等作用，适用于自然人网上办事、线上签约、政务

服务、金融业务、电子签章等场景。

个人证书按照证书用途，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、个人数据加密证书、个人数字身份证书。

（1）个人高等级电子签名认证证书：可证实个人与电子签名制作数据有联系的数字证书。个人高等级电子签名认证证书属于《中华人民共和国电子签名法》规定的电子签名认证证书，适用于涉及生命健康、财产权益等高风险业务场景，为各类电子文件提供可靠电子签名。

（2）个人基础级电子签名认证证书：可证实个人与电子签名制作数据有联系的数字证书。个人基础级电子签名认证证书属于《中华人民共和国电子签名法》规定的电子签名认证证书，适用于个人高等级电子签名认证证书规定场景以外的业务场景，为各类电子文件提供可靠电子签名。

（3）个人数据加密证书：绑定个人身份与公钥信息，适用于数据传输、存储及业务交互场景下实现信息加密、密钥协商与隐私保护的数字证书，保障数据在流转、储存过程中的保密性。个人数据加密证书不属于电子签名认证证书。

（4）个人数字身份证书：适用于个人可信身份的数字证书，可在网络业务、系统访问、线上交互等场景中识别个人真实身份，防范身份冒用风险，为各类数字化业务准入与权限管控提供可信身份依据。如个人网上银行、个人手机银行、系统登录等身份识别业务场景。个人数字身份证书不属于电子签名认证证书。

个人证书策略 OID 如下:

证书类型	证书策略 OID	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	适用于涉及生命健康、财产权益等高风险业务场景，为各类电子文件提供可靠电子签名的数字证书。
个人基础级 电子签名认证证书	2.16.156.339.2.1.1.1	适用于除高等级证书规定的场景外，为各类电子文件提供可靠电子签名的数字证书。

1.5.1.2. 机构证书

机构证书是以数字形式存在的组织机构电子身份凭证，用于在网络环境中标识企业、事业单位、政府机关、社会团体等组织机构真实身份信息，可实现身份认证、电子签名、数据加密、行为抗抵赖等作用，适用于组织机构电子签章、对公金融业务、供应链签约、电子商务、互联网政务服务等场景。

机构证书按照证书用途，分为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、机构数据加密证书、机构数字身份证书。

（1）机构高等级电子签名认证证书：可证实机构与电子签名制作数据有联系的数字证书。机构高等级电子签名认证证书属于《中华人民共和国电子签名法》规定的电子签名认证证书，适用于涉及生命健康、财产权益等高风险业务场景，为各类电子文件提供可靠电子签名。

（2）机构基础级电子签名认证证书：可证实机构与电子签名制作数据有联系的数字证书。机构基础级电子签名认证证书属于《中华人民共和国电子签名法》规定的电子签名认证证书，适用于机构高等

级电子签名认证证书规定场景以外的业务场景，为各类电子文件提供可靠电子签名。

（3）机构数据加密证书：绑定机构身份与公钥信息，适用于数据传输、存储及业务交互场景下实现信息加密、密钥协商与隐私保护的数字证书，保障数据在流转、储存过程中的保密性。机构数据加密证书不属于电子签名认证证书。

（4）机构数字身份证书：适用于机构可信身份的数字证书，可在网络业务、系统访问、线上交互等场景中识别机构真实身份，防范身份冒用风险，为各类数字化业务准入与权限管控提供可信身份依据。如企业网上银行、企业手机银行、系统登录等身份识别业务场景。机构数字身份证书不属于电子签名认证证书。

机构证书策略 OID 如下：

证书类型	证书策略 OID	应用场景
机构高等级 电子签名认证证书	2.16.156.339.2.1.2.2	适用于涉及生命健康、财产权益等高风险业务场景，为各类电子文件提供可靠电子签名的数字证书。
机构基础级 电子签名认证证书	2.16.156.339.2.1.2.1	适用于除高等级证书规定的场景外，为各类电子文件提供可靠电子签名的数字证书。

1.5.1.3. 网络应用证书

网络应用证书是面向业务服务载体的数字证书，适用于各类数字化服务场景，为信息化应用系统的安全运行提供可信支撑，保障业务数据传输完整性、保密性以及服务主体有效性。

网络应用证书按照证书用途，分为网站证书、设备证书、通讯证

书、电子邮件证书、智能体证书等。网络应用证书不属于电子签名认证证书。

（1）网站证书：又称 SSL 证书，用于标识网站所有者真实身份，在网站服务器与客户端浏览器之间构建安全加密通信信道，保障网站数据传输的保密性与完整性。

（2）设备证书：用于标识网络设备身份，实现设备之间的可信身份认证及传输数据加密处理，搭建安全可靠的设备通信传输链路。

（3）通讯证书：用于核验通讯参与方的主体身份，在通讯交互过程中实现数据加密传输、身份合法鉴别，保障传输数据的真实性、可信性与安全性。

（4）电子邮件证书：用于验证电子邮件地址及其归属主体身份，实现电子邮件传输过程中的信息签名、加解密等安全机制，防范电子邮件篡改、伪造、泄露等安全风险。

（5）智能体证书：用于标识智能体身份，在智能体交互、通讯过程中完成身份识别与可信核验，实现交互数据加密传输、行为信息安全签名，保障智能体间通信数据的真实性、完整性与保密性。

1.5.2. 证书应用限制

本 CPS 项下所有证书禁止应用于任何违反国家或地方法律法规的领域以及任何未经过安全检测的环境，具体包括但不限于：

（1）《中华人民共和国电子签名法》第三条列明的不适用电子签名的场景；

（2）超出证书策略标识范围开展的证书应用；

（3）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。

违规使用证书所引发的一切法律责任与相关后果，由证书使用方自行承担。

本机构用于技术测试、业务验证等用途签发的证书，即证书甄别名（DN）中包含“测试”或“Test”标识的证书，不属于正式证书，不具备司法效力。

1.6. 策略管理

1.6.1. 策略管理机构

本 CPS 的管理机构是“中金金融认证中心有限公司电子认证业务安全策略委员会”（以下简称“安全策略委员会”）。安全策略委员会由本机构高级管理人员、中级管理人员、业务领域专家、技术专家等成员组成，安全策略委员会成员由本机构任命并在本机构范围内公示。安全策略委员会根据最新的政策法规、标准规范以及业务发展需要，制定、修订、评审、发布、备案本 CPS。

安全策略委员会职责为：

（1）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；

（2）协调本机构信息安全委员会对信息安全策略、涉及根证书密钥的重要安全操作和流程进行审批；

（3）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；

（4）每年组织运营风险评估并形成报告。

本机构妥善保存安全策略委员会重大决议相关文件和会议记录。

1.6.2. 策略文档的批准程序

本 CPS 的制定、修订、评审、发布、备案，由安全策略委员会统筹负责，批准程序如下:

（1）起草小组的成立流程

安全策略委员会发起组建 CPS 编写小组，承担 CPS 的起草、修订工作，形成 CPS 初稿。

（2）安全策略委员会的审批流程

CPS 编写小组提交 CPS 初稿，安全策略委员会专家组开展专家评审，审议通过后形成 CPS 评审稿。

CPS 评审稿提交本机构法务部门进行合规审查，审查通过后形成 CPS 法审稿。

CPS 法审稿报请本机构总经理办公会审议批准。

（3）向主管机关的备案流程

CPS 自内部批准之日起 30 日内，安全策略委员会向工业和信息化部履行备案手续。

（4）发布流程

CPS 自内部批准之日起 30 日内，在本机构官方网站发布。

本机构官方网站地址为：https://www.cfca.com.cn

安全策略委员会定期评估 CPS 适用性，依据评估结果启动修订。修订版按上述起草、批准、备案、发布流程执行。

已发布的 CPS 版本自生效日起，对生效日后申请证书的订户具有约束力。订户及依赖方应定期访问本机构官方网站查阅 CPS 最新版本。

订户、依赖方在 CPS 最新版本发布 15 日后，仍继续使用 CFCA 数字证书，视为已接受最新版本约束；对新版本条款有异议的，应立即停止使用相关数字证书。

1.7. 定义和缩写

下列定义适用于本 CPS。

序号	名词	定义
1	电子认证服务机构	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。
2	数字证书	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、有效期以及拓展信息的一种数据结构。[GB/T 25056-2018 3.9]
3	电子签名认证证书	可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。[《中华人民共和国电子签名法》第三十四条（三）]
4	证书策略	一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和(或)具体应用类的适用性。[GB/T 25056-2018 3.3]
5	电子认证服务业务规则	关于电子认证服务机构指明其在签发证书时所使用的业务准则及标准的声明。
6	证书撤销列表	由证书认证机构(CA)签发并发布的被撤销证书的列表。[GB/T 25056-2018 3.4]

7	在线证书状态协议	确定证书当前状态的协议，替代或作为对周期性 CRL 进行检查的补充，规定了在检查证书状态的应用程序和提供状态信息的服务器之间需要交换的数据。[GB/T 27913-2022 3.42]
8	证书链	证书链是一个用于证书验证的证书序列。
9	时间戳	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。[GB/T 25069-2022 3.541]
10	订户	被颁发给一张证书的证书主体。[GB/T 26855-2011 3.15]
11	电子签名依赖方	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。[《中华人民共和国电子签名法》第三十四条（二）]
12	身份查验	证实某个实体就是所声称身份的过程。
13	激活数据	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。[GB/T 25069-2022 3.267]
14	密钥	控制密码变换操作的符号序列。[GB/T 25069-2022 3.389]
15	私钥	非对称密码算法中只能由拥有者使用的不公开密钥。[GB/T 25069-2022 3.580]
16	公钥	非对称密码算法中可公开的密钥。[GB/T 25069-2022 3.211]
17	加密	对数据进行密码变换以产生密文的过程。[GB/T 25069-2022 3.278]
18	数字签名	附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。[GB/T 25069-2022 3.576]
19	电子签名	数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。[《中华人民共和国电子签名法》第二条]
20	电子印章	一种经制作者签名，包括持有者信息和图形化内容，可用于签署电子文件的数据。[GB/T 25069-2022 3.121]
21	电子签章	使用电子印章签署电子文件的过程。[GB/T 25069-2022 3.120]

22	高等级电子签名认证证书	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。
23	基础级电子签名认证证书	适用于除高等级证书以外的其他低风险场景的电子签名认证证书。
24	密钥更新	用新密钥替换旧密钥的过程。[GB/T 25069-2022 3.400]
25	密钥恢复	将归档或备份的密钥恢复到可用状态的过程。[GB/T 25069-2022 3.405]
26	证书续期	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。
27	证书撤销	CA 机构在证书有效期内，因错误签发、私钥泄露、不再使用等原因，提前终止证书效力，并通过证书撤销列表（CRL）、在线证书状态协议（OCSP）对外公示的行为。本机构 CPS 历史版本中的吊销、注销与本文中的撤销含义一致。

下列缩略语适用于本 CPS。

缩略语	英文名称	释义
CA	Certification Authority	电子认证服务机构
CPS	Certification Practice Statement	电子认证业务规则
CP	Certification Policy	证书策略
CRL	Certificate Revocation List	证书撤销列表
CSR	Certificate Signing Request	证书请求文件
DN	Distinguished Name	甄别名称
KM	Key Management	密钥管理系统
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LEI	Legal Entity Identifier	全球法人识别编码
OCSP	Online Certificate Status Protocol	在线证书状态协议
OID	Object Identifier	对象标识符

RTO	Recovery Time Objective	恢复时间目标
RPO	Recovery Point Objective	恢复点目标

2. 信息发布与信息管理

2.1. 信息发布

本机构为保障证书订户、依赖方及监管机构知情权，规范电子认证服务信息公开管理，在 CFCA 官方网站对外发布公示信息。所有公开内容真实、准确、完整、可查询。本机构信息公开范围如下:

（1）CP、CPS 所有版本文件

本机构公示电子认证业务规则（CPS）、证书策略（CP）全部历史版本及现行有效版本，支持各方在线查阅、下载、核验。

CP、CPS 发布地址: https://www.cfca.com.cn/cfcacps/

（2）证书链信息

本机构公开 CFCA 全部可信证书链结构，包含根证书、中级证书等全部层级证书信息，提供证书链下载、验证指引，保障依赖方完成证书链校验。

证书链发布地址: https://www.cfca.com.cn/zhengshuzizhu/

（3）证书查询服务

本机构提供线上证书查询服务通道，支持社会公众、订户、依赖方查询证书基础信息、签发信息、有效期、证书状态（未下载、激活、冻结、撤销）等信息。撤销的证书信息可通过数字证书内的 CRL 分布点查询获取；证书状态信息可通过证书状态查询服务（OCSP）等方式获取。

证书信息查询地址: https://cs.cfca.com.cn/

（4）业务办理指南

本机构提供详细的业务办理指南，涵盖证书申请、签发、更新、撤销等全流程操作指引；公示服务网点详细地址、办公营业时间、人工咨询固定电话、线上客服联系方式等服务信息。

业务办理指南地址：https://www.cfca.com.cn/help/

本机构地址、咨询电话详见第 1.2 章节。

（5）电子认证服务协议

本机构公示 CFCA 电子认证服务协议，明确订户的权利与义务、本机构与订户的责任划分、电子签名认证证书及电子签名的使用条件、订户签名私钥的存储方式及安全要求等事项。

电子认证服务协议地址：

https://www.cfca.com.cn/zhengshuzizhu/cfcaszzsfwxy/

（6）依赖方协议

本机构公示 CFCA 电子认证服务依赖方协议，明确依赖方权利、义务、使用规范、风险责任划分，保障依赖方合法合规使用数字证书。

依赖方协议地址：

https://www.cfca.com.cn/zhengshuzizhu/cfcaszzsfwxy/

（7）投诉处理服务信息

本机构提供标准化投诉处理政策及投诉渠道，接受订户及社会监督。订户投诉由本机构运营中心统一受理，投诉电话：010-87549600。

（8）不公开信息

本 CPS 中引用的属于本机构内部管理制度及相关控制规则的，不在本机构官方网站发布。

2.2. 信息管理

（1）信息更新

为保障公开信息时效性，本机构建立信息动态更新机制。本 CPS 第 2.1 章节所有公示内容，若发生规则修订、信息变更、业务调整、网点变动、联系方式更新等情况，相关变更内容正式生效后 1 个工作日内完成官方网站信息同步更新。

（2）监管备案

本机构按照行业主管部门要求进行备案，接受行业主管部门监督管理。

（3）证书信息对接

本机构按照行业主管部门要求完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表等功能。

证书信息查询地址：https://cs.cfca.com.cn/

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

订户向本机构申请证书时，应当提供真实、完整和准确的信息。

本机构在受理订户证书申请时，对订户和/或受托人依法履行相关事项告知义务，严格开展身份真实性查验，完整留存申办意愿记录，依规签署电子认证服务协议。

本机构身份查验义务未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

本机构受理订户证书申请时，通过《CFCA 电子认证服务协议》向订户明确告知以下内容:

（1）订户的权利和义务;

（2）服务收费的项目和标准;

（3）电子签名认证证书、电子签名的使用条件;

（4）信息安全保障措施;

（5）本机构和订户的责任划分;

（6）订户签名私钥的存储方式及安全要求;

（7）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。

《CFCA 电子认证服务协议》在本机构官方网站公示，链接如下:

https://www.cfca.com.cn/zhengshuzizhu/cfcaszzsfwxy/

订户接受《CFCA 电子认证服务协议》或本 CPS，即视为订户知晓并同意上述全部事项。

3.1.2.2. 告知方式

本机构通过下列方式，告知订户第 3.1.2.1 章节内容:

（1）现场面对面告知;

（2）电话告知;

（3）视频告知;

（4）页面强制阅读;

（5）短信告知;

（6）邮件告知;

（7）微信告知;

（8）主管部门认可的其他方式告知。

3.1.2.3. 高等级电子签名认证证书订户告知

订户申请高等级电子签名认证证书，本机构可采用第 3.1.2.2 章节第（1）（2）（3）（8）项任一方式予以告知，并保留告知记录。

3.1.2.4. 基础级电子签名认证证书订户告知

订户申请基础级电子签名认证证书，本机构可采用第 3.1.2.2 章节第（1）（2）（3）（4）（5）（6）（7）（8）项任一方式予以告知，并保留告知记录。

3.1.2.5. 其他类型证书订户告知

订户申请其他类型证书，本机构可采用任一安全有效方式予以告

知。

3.2. 初始身份确认

3.2.1. 证明拥有私钥的方法

订户电子签名认证证书的密钥对，可通过以下方式生成:

（1）由订户持有的符合国家安全标准的密码设备或密码模块生成;

（2）订户委托本机构在安全环境中生成;

（3）订户采用经主管部门认可的其他创新性方式生成。

订户加密证书的密钥对，由本机构的密钥管理系统（KM）生成，并通过安全的方式传输给订户。本机构的密钥管理系统通过国家密码管理部门安全审查，负责为订户提供产生、备份、恢复加密证书密钥等服务。

其他类型证书的密钥对，订户可参考上述方式，或者采用其他安全方式生成。

为了证明订户拥有与注册公钥对应的私钥，订户的证书请求文件（Certificate Signing Request，简称 CSR）中应包含私钥的数字签名。本机构在为订户签发证书前，使用订户的公钥验证其私钥签名的有效性及申请数据的完整性，以此判定订户拥有私钥。

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

订户申请个人证书，应当提供订户本人有效身份证件或有效身份证件信息; 订户委托其他机构或个人代为办理时，受托人还应当提供

订户本人签署的有效授权证明，以及受托人有效身份证件或有效身份证件信息。

个人有效证件类型仅限法律法规和国家有关文件规定的身份证件，包括：居民身份证、护照、港澳居民来往内地通行证、港澳居民居住证、台湾居民来往大陆通行证、台湾居民居住证、外国人永久居留身份证等。详见《CFCA 数字证书数据构成规则》。

本机构通过证件机读工具、权威数据库或主管部门认可的其他方式查验订户及受托人身份证件的真实性、准确性、有效性。

3.2.2.2. 个人订户实人查验方式

本机构采用下列方式开展个人订户实人查验：

（1）现场面对面查验；

（2）远程人工面对面查验；

（3）生物特征验证：运用活体人脸、指纹、声纹、掌纹、笔迹等生物识别技术进行查验；

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

（5）银行卡四要素验证：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核验；

（6）由申请人持有的有效电子签名认证证书签名验证；

（7）居民身份网络可信凭证查验；

（8）公民网络电子身份标识查验；

（9）国家网络身份认证系统查验;

（10）内地银行或支付机构提供的个人账户和身份信息对应关系验证;

（11）主管部门认可的其他查验方式。

3.2.2.3. 个人高等级证书的实人查验

订户申请个人高等级电子签名认证证书，本机构可采用第3.2.2.2章节第（1）（2）（3）（11）项任一方式进行实人查验。本机构以可追溯的方式完整记录并保存身份查验过程和结果，每张证书建立独立的身份验证记录。

3.2.2.4. 个人基础级证书的实人查验

订户申请个人基础级电子签名认证证书，本机构可采用第3.2.2.2章节第（1）（2）（3）（4）（5）（6）（7）（8）（9）（10）（11）项任一方式进行实人查验。本机构以可追溯的方式完整记录并保存身份查验过程和结果，每张证书建立独立的身份验证记录。

3.2.2.5. 个人其他类型证书的实人查验

订户申请其他类型个人证书，本机构可采用任一安全有效方式进行实人查验。

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

订户申请机构证书，应当提供机构有效身份证件或有效身份证件信息。办理人非机构法定代表人，还应当提供加盖机构公章的有效授权证明，或具备同等效力的其他材料。

由机构法定代表人申请证书，本机构按照第 3.2.2.1 章节，查验法定代表人身份。由机构授权办理人（受托人）申请证书，本机构按照第 3.2.2.1 章节，查验受托人身份，并查验机构授权材料。

机构有效证件类型仅限法律法规和国家有关文件规定的身份证件，包括营业执照、外国（地区）企业常驻代表机构登记证等。机构有效证件信息仅限法律法规和国家有关文件规定的机构编码，包括统一社会信用代码、全球法人识别编码（LEI）等。详见《CFCA 数字证书数据构成规则》。

3.2.3.2. 机构高等级证书的实人查验

订户申请机构高等级电子签名认证证书，本机构可采用下列任一方式进行实人查验。

（1）由机构法定代表人申请证书，本机构按照第 3.2.2.3 章节，对机构法定代表人进行实人查验。

（2）由机构授权办理人（受托人）申请证书，本机构按照第 3.2.2.3 章节，对受托人进行实人查验，并采用对公账户随机金额打款验证。

（3）通过主管部门认可的其他方式查验。

本机构以可追溯的方式完整记录并留存身份查验过程和结果，每张证书建立独立的身份验证记录。

3.2.3.3. 机构基础级证书的实人查验

订户申请机构基础级电子签名认证证书，本机构可采用下列任一方式进行实人查验。

（1）由机构法定代表人申请证书，本机构按照第 3.2.2.4 章节，对机构法定代表人进行实人查验。

（2）由机构授权办理人（受托人）申请证书，本机构按照第 3.2.2.4 章节，对受托人进行实人查验。

（3）由订户持有的同等级或者更高等级的有效机构证书签名验证。

（4）通过主管部门认可的其他方式查验。

本机构以可追溯的方式完整记录并保存身份查验过程和结果，每张证书建立独立的身份验证记录。

3.2.3.4. 机构其他类型证书的实人查验

订户申请其他类型机构证书，本机构可采用任一安全有效方式进行实人查验。

3.2.4. 网络应用证书订户身份查验

个人、机构申请网络应用证书，本机构依据第 3.2.2.5 章节、第 3.2.3.4 章节，参照非电子签名认证证书的查验方式对个人、机构进行实人查验。

3.2.5. 订户身份查验特别说明

境外自然人申请数字证书时，本机构对其提交的境外属地主管机关核发的身份证件资料开展形式查验。

境外法人机构申请数字证书时，本机构可依托全球法人识别编码（LEI），或对其提交的境外属地主管机关核发的身份证件资料开展形式查验。

3.3. 订户意愿记录

3.3.1. 订户意愿记录内容

订户提交申请证书时，应当充分知晓并同意下列内容:

（1）订户实名身份信息;

（2）本机构相关信息;

（3）签名私钥保存方及其保存义务;

（4）订户对电子签名的法律责任。

本机构受理证书申请时，记录订户对上述（1）（2）（3）（4）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

3.3.2.1. 个人高等级证书的意愿记录

订户申请个人高等级电子签名认证证书，本机构可采用下列任一方式确认并记录订户意愿。

（1）订户现场申请证书时，本机构通过面对面确认、手抄提示语、手写签字等方式，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。

（2）订户在线申请证书时，本机构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。

本机构保留完整、可追溯的订户意愿记录。

3.3.2.2. 个人基础级证书的意愿记录

订户申请个人基础级电子签名认证证书，本机构可采用下列任一方式确认并记录订户意愿。

（1）采用与高等级证书相同的方式;

（2）采用页面展示强制阅读、短信确认、邮件确认等电子方式。

本机构保留完整、可追溯的订户意愿记录。

3.3.2.3. 个人其他类型证书的意愿确认

订户申请其他类型个人证书，本机构可采用任一安全有效方式确认订户意愿。

3.3.3. 机构证书的意愿记录

3.3.3.1. 机构高等级证书的意愿记录

订户申请机构高等级电子签名认证证书，本机构可采用下列任一方式确认并记录订户意愿。

（1）由机构法定代表人申请证书，本机构按照第 3.3.2.1 章节的方式确认机构法定代表人的意愿。

（2）由机构授权办理人（受托人）申请证书，本机构查验加盖机构公章的有效授权证明或具备同等效力的其他材料，并按照第 3.3.2.1 章节的方式确认受托人的意愿。

本机构保留完整、可追溯的订户意愿记录。

3.3.3.2. 机构基础级证书的意愿记录

订户申请机构基础级电子签名认证证书，本机构可采用下列任一方式确认并记录订户意愿。

（1）由机构法定代表人申请证书，本机构按照第 3.3.2.2 章节的方式确认机构法定代表人的意愿。

（2）由机构授权办理人（受托人）申请证书，本机构查验加盖

机构公章的有效授权证明或具备同等效力的其他材料，并按照第3.3.2.2章节的方式确认受托人的意愿。

本机构保留完整、可追溯的订户意愿记录。

3.3.3.3. 机构其他类型证书的意愿确认

订户申请其他类型机构证书，本机构可采用任一安全有效方式确认订户意愿。

3.3.4. 网络应用证书的意愿确认

个人、机构申请网络应用证书，本机构依据第3.3.2.3章节、第3.3.3.3章节，参照非电子签名认证证书的方式对个人、机构进行意愿确认。

3.4. 订户协议

订户申请电子签名认证证书，应当与本机构签订《CFCA电子认证服务协议》。

《CFCA电子认证服务协议》包含第3.1.2.1章节内容。

《CFCA电子认证服务协议》在本机构官方网站公示，链接如下：

https://www.cfca.com.cn/zhengshuzizhu/cfcaszzsfwxy/

订户接受本机构电子认证服务，即视为接受《CFCA电子认证服务协议》。

3.5. 未验证的订户信息

本机构签发的电子签名认证证书，按照第3.2.2章节规定流程和方式查验个人订户身份信息，按照第3.2.3章节规定的流程和方式查验机构订户身份信息。本机构签发的电子签名认证证书中不包含未经

验证的订户信息。

订户使用匿名提交的证书申请材料不符合本机构的审核要求，将无法通过审核，也无法获得证书和服务。使用伪名或伪造材料申请的证书无效，一经证实立即予以撤销。

3.6. 互操作要求

本机构符合 GM/T 0043《数字证书互操作检测规范》要求。国家密码管理局运营的面向社会公众应用的 SM2 根证书为本机构 CFCA CS SM2 CA 签发 CA 证书。国家根与本机构 CFCA CS SM2 CA 构建信任链。

截至目前，本机构未签发其他交叉认证的证书。

3.7. 命名

3.7.1. 命名规则

本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》及其最新规范，名称采用 X.500 甄别名 DN（Distinguished Name）的格式命名。

证书 DN（Distinguished Name，甄别名）是数字证书主体名称域中用于唯一标识证书主体的名称。电子签名认证证书 DN 包含订户姓名或机构名称、证件类型、证件号码或号码的映射，能够将证书名称与唯一确定的实体（如个人、组织机构等）关联起来，使依赖方可识别该实体。证书 DN 项结构定义符合《信息技术 开放系统互连 目录 第 8 部分：公钥和属性证书框架》（GB/T 16264.8）的规定，具体规则见《CFCA 数字证书数据构成规则》。

在不影响证书使用的前提下，本机构可在证书中增加自定义的其

他内容。

3.7.2. 名称唯一性

本机构签发的数字证书，证书 DN 在签发数字证书的 CA 系统内唯一标识订户主体。同一订户持有的多张证书，通过证书序列号等唯一标识进行区别。不同的申请主体，如有相同的注册名称或者识别名称时，将在后申请者的 DN 中增加其他属性进行区分。

3.7.3. 商标权的处理策略

订户在申请数字证书时不得使用可能侵犯他人知识产权的信息。若订户提交的申请信息包含商标信息，则需要订户提交有关商标注册文件，如政府机构发放的合法性证明文件。本机构颁发数字证书时，仅对商标的合法性证明文件进行形式审查，不审查证书订户是否处于纠纷中，且无需对任何订户关于知识产权的使用行为负法律责任。当发生有关知识产权的争议或纠纷时，本机构有权在必要时驳回相关证书申请或撤销已签发的证书。

4. 证书生存周期操作要求

4.1. 通用要求

证书生存周期全过程中，本机构、证书订户等相关参与方均应严格遵照本 CPS 规则履行职责。

（一）本机构承担建立、运营和维护注册通道的责任

本机构负责建立、运营、维护电子认证注册通道，保障注册通道运行稳定、流程规范，为订户证书注册、业务办理提供合法、有效的支撑。本机构将依据国家电子认证相关标准，持续优化服务能力，保障注册业务有序开展。

（二）本机构承担与订户签订电子认证服务协议的责任

本机构作为电子认证服务提供主体，负责依法与证书订户签订电子认证服务协议，明确双方权利义务、服务范围、权责边界及合规要求，是双方开展电子认证服务合作的法定依据。

（三）订户承担提供准确信息的责任

订户在办理证书相关业务时，应提交真实、准确、完整、有效的身份信息及相关材料，并对所提交信息及材料的真实性、合法性、有效性承担全部法律责任。若因订户提供虚假、错误、残缺信息及材料引发的一切风险、纠纷及损失，均由订户自行承担。

（四）本机构承担妥善记录并保存相关信息的责任

本机构严格按照法律法规及行业标准要求妥善记录并保存订户身份信息及相关材料，保障信息的真实可溯、安全可控，并按法定保管期限保存信息。

4.2. 证书申请

4.2.1. 证书申请实体

证书申请实体包括具有民事行为能力的自然人以及具有独立法人资格的组织机构（包括事业单位、企业单位、社会团体和人民团体等）。

4.2.2. 证书申请程序

订户向本机构申请证书，应向本机构提交真实、准确、完整、有效的身份信息及相关材料。

本机构对订户提交的证书申请及相关材料进行初步核查，符合受理条件、材料齐全的申请予以正式受理；不符合受理要求的，予以驳回。

本机构按照本 CPS 第 3.1.2 章节相关规定，向订户告知电子认证服务及数字证书相关事项，保障订户的知情权。

本机构按照本 CPS 第 3.2 章节相关规定，对订户身份真实性、合法性、有效性进行严格查验，确认订户真实身份。

本机构按照本 CPS 第 3.3 章节相关规定，核实订户申请证书的真实意愿，留存订户意愿记录。

本机构按照本 CPS 第 3.4 章节相关规定，与订户签署《CFCA 电子认证服务协议》，确立合法有效的电子认证服务合同关系。

本机构结合订户身份信息及相关材料，依据本 CPS 规范及相关法律法规，依法作出核发证书或驳回申请的决定，并将审核结果告知订户；驳回申请的，说明理由。

驳回申请的订户，可重新准备符合要求的材料后提交。

本机构可依据内部管理制度，不定期复核申请资料，有权驳回不符合本 CPS 的申请。

以上程序可根据实际业务场景适当调整。

4.2.3. 证书申请处理时限

订户提交的申请材料真实、完整、准确且符合形式要求，本机构在收到订户申请后 2 个工作日内完成证书申请的处理。如有特殊情况，本机构经与订户协商一致，可适当延长证书申请处理时间。

4.3. 证书签发

4.3.1. 证书签发程序

本机构验证订户身份信息与证书请求文件（CSR）。验证通过后，按照《CFCA 数字证书数据构成规则》构造证书各项数据域形成待签名数据；使用本机构 CA 体系中级证书私钥对待签名数据进行数字签名，生成订户证书，完成证书签发。

订户加密证书密钥对由本机构密钥管理系统（KM）生成，按照上述程序完成证书签发，通过安全方式传输给订户。

4.3.2. 证书签发结果通告

证书申请签发完成后，本机构可通过下列任一方式向订户通告处理结果:

（1）通过线上业务办理系统、线上服务平台、客户端等认证应用工具通知；

（2）通过信函、站内信或电子邮件等方式通知；

（3）通过页面通知；

（4）通过短信通知；

（5）通过电话通知；

（6）面对面通知，或实时视频等相当于面对面的方式通知；

（7）通过主管部门认可的其他方式通知。

本机构不对除订户以外的其他参与证书签发的参与者进行主动通告；依赖方可自行通过信息库查询获取相关信息。

4.4. 证书接受

本机构可通过下列任一方式向订户交付证书，订户按照对应流程完成证书接受。

（1）本机构向订户发送证书下载凭证，订户在安全环境下生成证书密钥与证书请求文件（CSR），凭证书下载凭证在本机构证书下载平台获取证书。订户完成证书下载，即视为接受该证书。

（2）本机构可采用现场当面交付、物流寄送、电子传输等方式向订户交付证书，订户实际收取证书即视为接受该证书。

（3）订户委托本机构保管证书，订户签订相关协议或收到证书签发通知时，即视为接受该证书。

（4）订户使用证书开展电子签名、密码运算等业务操作时，即视为接受该证书。

订户如果拒绝接受证书，应立即停止使用证书，并在 1 个工作日内向本机构提出异议。

本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。

4.5. 证书和密钥对的使用

4.5.1. 交付前的安全保护

本机构在将证书及其密钥对交付订户保管之前，采取有效措施保障其安全性，包括但不限于以下方式:

（1）采用符合国家或行业安全标准的密码设备或密码模块中生成密钥对;

（2）证书介质（密码设备或密码模块）采用安全方式交付订户;

（3）审核订户密钥是否符合国家或行业相关安全标准要求，对于不符合要求的密码算法、密钥长度，本机构拒绝颁发证书。

4.5.2. 私钥管理服务要求

订户委托本机构保管证书及其私钥，由本机构负责保障订户证书及私钥安全。本机构采取下列措施保护订户证书及私钥安全使用。

（1）未经订户授权，本机构不保存或委托他人保存其签名私钥。

（2）经订户授权，本机构采用符合国家或行业安全标准的密码设备或密码模块中生成，并以加密形式存储订户私钥。

（3）本机构确保订户密钥符合国家或行业相关安全标准要求。

（4）由本机构受托生成的订户私钥，私钥全程仅在本机构安全环境内存储，不向任何外部传输。

（5）机构证书签名私钥的使用，本机构验证法定代表人或受托人的授权主体身份。

（6）本机构仅在获得订户明确授权的情况下使用其签名私钥。

（7）本机构对所有涉及订户签名私钥的操作，生成可追溯记录。

4.5.3. 安全事件反馈

本机构建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

4.5.4. 订户对证书及私钥的使用

订户使用证书时，应遵循第 1.5 章节所规定的用途，并履行以下与证书及密钥对使用相关义务:

（1）妥善保存证书私钥，采取合理的措施防止私钥遗失、泄露、被篡改等;

（2）在授权的应用范围内使用证书及私钥;

（3）使用证书时应验证证书及证书链的正确性、完整性、有效性;

（4）证书到期或被撤销后，须停止使用该证书及对应的私钥;

（5）使用证书执行交易数据签名、加密时，应确保自己充分了解业务情况，以及充分知晓该证书与业务之间的权利义务关系;

（6）委托本机构保管证书及私钥时，订户仍为法定责任主体，对全部操作行为承担责任。

4.5.5. 依赖方对证书及公钥的使用

依赖方在信赖交易对方的证书时，应对证书进行下列步骤验证:

（1）通过本机构官方途径获取并安装本机构的证书链，并验证对方证书是否属于本机构签发;

（2）通过安全途径获取订户公钥证书，并核验证书是否属于正

确的交易方，并甄别证书中的策略是否符合交易需要及证书的适用范围；

（3）在信赖证书所证明的信任关系前确认该证书有效性，包括：检查本机构公布的最新的证书撤销列表（CRL）或在线证书查询服务（OCSP），确认该证书未被撤销；检查证书链的可靠性；检查该证书的有效期；以及检查其他能够影响证书有效性的信息；

（4）验证证书的用途适用于对应的签名；使用该公钥证书上的公钥验证签名；

若以上任一步骤失败，依赖方应拒绝接受该签名信息。

4.6. 证书续期

证书续期是指证书有效期届满前，为订户签发新证书。本机构按照第 4.7 章节规定的方式处理。

4.7. 证书密钥更新

证书密钥更新是指订户主体信息保持不变的前提下，为订户生成新的密钥对并为其新公钥签发新证书。

证书密钥更新适用于下列情形：

（1）订户证书有效期届满前；

（2）订户证书有效期届满后；

（3）订户证书密钥遭到损坏时；

（4）订户证实或怀疑其证书密钥不安全时；

（5）其他可能导致密钥更新的情形。

符合上述情形，订户可提交证书密钥更新申请；机构证书申请密

钥更新，应由法定代表人或授权人申请办理。

本机构受理证书密钥更新申请时，若符合上述情形（1），即证书有效期届满前，且自订户上次完成身份查验之日起至本次申请日未满 3 年，本机构可使用有效的原证书进行电子签名验证的方式查验订户身份；否则，本机构按照第 3.2 章节的规定重新查验订户身份。

本机构受理证书密钥更新申请时，证书签发程序按照第 4.3 章节执行。

本机构受理证书密钥更新申请时，证书接受程序按照第 4.4 章节执行。

4.8. 证书变更

证书变更是指订户主体信息变更，而原有密钥保持不变的情况下，为订户签发新证书。本机构不受理证书变更申请。订户主体信息变更，可申请撤销原有证书，并以新的主体信息申请新证书。

4.9. 证书撤销或冻结

证书撤销，也称证书吊销，是指本机构在证书有效期内，根据特定事由提前终止证书的有效性。证书撤销后，不再具备效力。

4.9.1. 证书撤销的情形

4.9.1.1. 订户撤销证书的情形

发生下列任一情形，订户应当申请撤销证书：

（1）订户决定不再使用证书；

（2）订户无法履行《CFCA 电子认证服务协议》或本 CPS 的要求；

（3）订户证明证书申请未获得其有效授权；

（4）订户怀疑密钥不安全、存放证书的介质无法正常使用等;

（5）订户证书主体信息发生变更。

4.9.1.2. 本机构撤销证书的情形

发生下列任一情形，本机构可撤销订户证书:

（1）订户证书被使用于违反法律强制性规定的事项上;

（2）订户申请证书时，提供的资料不真实、不完整、不准确;

（3）订户证书签发错误;

（4）订户证书中所显示的信息不准确或具有误导性;

（5）订户未履行《CFCA 电子认证服务协议》中所约定的义务或本 CPS 的要求;

（6）订户未能满足证书策略中的要求和条件;

（7）订户证书被超出应用范围使用;

（8）订户已失去证书主体信息（如域名、IP 地址）的所有权或控制权;

（9）网站证书（SSL 证书）被用于验证一个欺诈性或极具误导性的域名;

（10）本机构停止电子认证业务且无其他电子认证机构承接业务，本机构将撤销所有已签发证书，仅保留 CRL 和 OCSP 服务的运行;

（11）本机构电子认证服务资质被吊销且无其他电子认证机构承接业务，本机构将撤销所有已签发的证书，仅保留 CRL 和 OCSP 服务的运行;

（12）本机构的根证书、中级证书私钥泄露时，本机构根据签名

私钥泄漏紧急预案撤销所有已签发的证书;

（13）证书的关键参数被国际或国内权威标准认定存在重大安全风险;

（14）法律、行政法规规定的其他情形。

4.9.1.3. 其他参与者撤销证书的情形

依赖方或其他参与者如发现证书问题，可向本机构提出撤销申请，并说明合理理由。

4.9.2. 证书撤销程序

4.9.2.1. 订户撤销证书程序

符合第 4.9.1.1 章节的情形，订户可提交证书撤销申请；机构证书申请撤销，应由法定代表人或授权人申请办理。

订户申请撤销证书，通过本机构提供的热线电话、电子邮箱等便捷渠道，向本机构提交有效身份证明文件、拟撤销证书信息或证书撤销申请表、撤销原因等相关材料。

本机构在收到订户提交的撤销申请材料后，对申请材料进行核验，对涉及证书或私钥安全的事件（如密钥遗失、泄露等）进行记录。

本机构对订户身份进行查验；机构证书对机构授权人权限进行验证；通过后，本机构撤销订户证书。

证书撤销生效后，本机构按照证书撤销列表（CRL）发布策略更新证书撤销列表，并同步更新在线证书状态协议（OCSP）中的证书状态。本机构通过电话、短信、电子邮件、证书撤销列表（CRL）、在线证书状态协议（OCSP）等任一种或多种方式告知订户。

本机构保留证书撤销处理流程相关信息。

4.9.2.2. 本机构撤销证书程序

符合第 4.9.1.2 章节的情形，本机构执行证书撤销，并通过电话、短信、电子邮件、证书撤销列表（CRL）、在线证书状态协议（OCSP）等一种或多种方式告知订户。

本机构保留证书撤销处理流程相关信息。

4.9.2.3. 其他参与者撤销证书程序

符合第 4.9.1.3 章节的情形，本机构根据其他参与者提交的证书撤销材料及理由，做出是否撤销证书的决定。决定撤销的，按照第 4.9.2.2 章节执行。

4.9.3. 依赖方检查证书撤销的要求

依赖方在信任该证书前，应验证证书有效性，确认证书是否已被撤销。依赖方可通过下列任一方式获取证书状态信息。

（1）依赖方可解析证书域“CRL 分发点”，获取证书撤销列表（CRL），通过比对证书序列号，确认证书是否已被撤销。

（2）依赖方可使用本机构提供的在线证书状态协议（OCSP）服务，实时验证证书状态，确认证书是否已被撤销。

依赖方是否执行在线证书状态查询，取决于其自身的安全要求。对于安全保障要求高且依赖数字证书进行身份鉴别与授权的应用，依赖方在信任证书前可通过本机构提供的在线证书状态协议（OCSP）服务检查该证书的状态。

4.9.4. 证书冻结及解冻

证书冻结是指订户察觉证书面临安全威胁时，申请将证书设置为冻结状态。证书解冻是指相关安全威胁解除后，订户申请恢复证书正常状态。

4.9.4.1. 证书冻结程序

订户怀疑证书受到威胁且希望暂停使用证书时，可发起证书冻结申请。证书冻结程序参照第 4.9.2.1 章节执行。

订户违反本 CPS 相关规定，本机构认为有必要暂停订户证书使用时，本机构可执行证书冻结。证书冻结程序参照第 4.9.2.2 章节执行。

4.9.4.2. 证书解冻程序

订户认为证书受到的威胁解除后，希望继续使用该证书且该证书在有效期范围内，订户可向本机构发起证书解冻申请。本机构收到申请后，对订户身份进行查验；机构证书对机构授权人权限进行验证；通过后，将该证书恢复正常状态。

订户恢复遵守本 CPS 相关规定，本机构认为有必要恢复订户证书使用时，本机构可执行证书解冻，将该证书恢复正常状态。

4.9.5. 其他说明

订户怀疑证书私钥存在安全隐患，应在知晓该安全隐患的 24 小时内，向本机构提交证书撤销或冻结申请。本机构在收到订户证书撤销或冻结请求后，24 小时内完成处理。

证书撤销或冻结生效后，订户应立即停止使用该证书，并通知相关依赖方停止信任该证书。

未取得订户授权，擅自使用订户身份信息代为办理证书撤销或冻

结的，由此引发的全部法律责任（包括但不限于订户因此遭受的直接或间接损失、依赖方损失、行政责任等）由代办者自行承担。

4.10. 证书状态信息服务

本机构提供 7×24 小时在线证书状态协议（OCSP）服务，实时发布证书状态。在线证书状态协议（OCSP）服务为连续不间断服务，服务可用率不低于 99.95%。

本机构发布证书撤销列表（CRL），发布频率为每 24 小时至少一次。证书撤销后，写入证书撤销列表（CRL）的最大滞后时间为 24 小时。证书有效期届满后，不再在证书撤销列表（CRL）中发布。

4.11. 停止使用认证服务

发生下列任一情形，视为订户停止使用本机构电子认证服务:

（1）订户证书有效期届满后不再续期;

（2）订户证书撤销;

（3）法律法规、监管部门要求终止订户电子认证服务的其他法定情形。

本机构保存订户停止使用电子认证服务的相关操作记录。

订户停止使用电子认证服务后，本机构将对受托保管的订户证书进行处置，安全销毁订户签名私钥。

订户停止使用电子认证服务后，本机构依法保存订户身份信息、证书公钥等电子认证服务相关数据，保存期限为证书有效期届满或证书撤销后至少 5 年。

本机构对订户终止电子认证服务后所作出的电子签名，不承担任

何责任。对于服务终止前、且处于证书有效期内生成的合法有效电子签名，本机构将在法定数据留存期限内持续提供签名有效性验证服务，直至法定数据留存期限届满。

4.12. 密钥托管与恢复

本机构根证书私钥不委托任何第三方机构及个人保管。本机构所有电子认证系统根证书及私钥均安全存储于符合国家及行业相关安全标准的专用密码设备内。

本机构具备根证书密钥备份与恢复相关制度及安全策略，本机构对根证书密钥进行安全备份。

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

本机构 CA 系统的运营机房位于北京市海淀区中关村软件园区 22 号楼（中国银联北京信息中心）内，机房具备抗震、防火、防水、恒湿温控、双路供电、备用发电、不间断电源（UPS）、电磁屏蔽、门禁控制、视频监控等功能，确保业务的可靠性。

网络通信设施采用多运营商线路架构，运营商链路实现至少双路由冗余部署；通信报文全程加密传输，可支撑互联网、专线、VPN 等多类接入场景。

5.1.2. 分区管理与访问控制

本机构机房划分为多个功能区域，分为公共区、服务区、管理区和核心区。

运营机房的入口处外的办公区域属于公共区。人员进入楼内时需先经过安保人员核验身份，使用门禁卡控制出入。

服务区位于屏蔽机房内，是部署从目录服务器、OCSP 服务器等服务器的区域，访问需使用门禁卡加生物识别认证。

管理区是电子认证系统的运行监控和运维管理操作的区域，访问需使用门禁卡加生物识别认证。

核心区是部署电子系统服务器、密钥管理系统（KM）、离线根服务器的区域。核心区的访问需两位授权人员通过门禁卡和生物识别认证，且所有门禁的访问控制信息均有记录。

5.1.3. 电力与空调

本机构机房采用 UPS 供电，由两组每组三台 UPS 供电，在外部电力供应中断的情况下，每组 UPS 均能保证持续供电 15 分钟以上。同时配备有柴油发电机 2 台，当市电供应中断时，能够持续保障对机房的供电。机房的门禁和入侵报警系统均由 UPS 提供电力。

5.1.4. 门禁与监控

机房部署有门禁、入侵检测、视频监控等安防系统，机房区域的视频监控记录保存至少 6 个月，门禁日志记录的保存至少一年。

5.1.5. 灾备

本机构对重要数据实施同城备份和异地备份，同城和异地备份机房距离符合《JR/T 0264—2024 金融数据中心容灾建设指引》机房选址布局要求。同城备份机房位于北京市朝阳区容达路 7 号，与生产机房直线距离超过 16 公里。异地备份机房位于上海市浦东区日阪路 91 号，与生产机房直线距离超过 1000 公里。

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℃范围内。

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灭火系统，包含温度和烟雾检测功能，并定期进行消防安全检测。

5.1.8. 设备管理

本机构建立了设备台账和资产管理制度，设备台账包含每台设备

的责任人、使用状态、维保周期等信息，资产管理制度包含报废标准等要求。本机构定期进行设备盘点和核对，设备实际情况与设备台账相符。

5.1.9. 存储媒体管理

本机构制定了存储媒体管理规定，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。

5.2. 操作过程控制

5.2.1. 可信角色

本机构在电子认证服务开展过程中，参与证书认证系统操作、运维及管理的人员统称为可信角色，具体分类及岗位职责如下：

（1）系统管理方向：负责系统策略、账号权限管理；记录系统登录、权限使用等行为，分析各类安全异常事件。

任职要求：熟悉证书认证系统整体架构、权限管控规范与安全管理策略，掌握操作系统安全配置、账号风险排查方法，熟知电子认证行业安全合规要求及内部操作管理制度，无安全违规从业记录。

（2）技术运维方向：负责物理环境、网络、服务器及系统软件运维；处置网络安全告警与攻击事件，定期更新网络拓扑图。

任职要求：精通机房物理环境运维、网络设备及服务器运维技能，具备网络攻击研判、安全应急处置能力，熟悉网络拓扑搭建规范，掌握电子认证系统基础设施运维安全红线要求。

（3）数据库管理方向：承担数据库运维、优化、备份工作；管控账号权限、排查安全漏洞，维护数据库架构。

任职要求：精通主流数据库运维、备份恢复与性能调优技术，具备数据库安全漏洞检测、SQL 风险语句排查能力，熟知证书业务敏感数据存储安全规范，严格遵守数据访问最小权限原则。

（4）系统审计方向：负责系统及网络日志审计、报告编制；核查系统操作、组件运维及敏感信息调取行为。

任职要求：熟悉各类系统日志、网络日志字段含义，掌握异常操作行为识别方法，了解电子认证审计合规标准，具备独立编制审计报告、追溯违规操作的能力，岗位独立于运维及系统管理岗位。

（5）密钥管理方向：统筹根证书密钥全生命周期管理；监管密钥全流程操作，规范密码设备使用与处置。

任职要求：具备商用密码从业资质，精通密码设备运维、密钥生成、分发、备份、销毁全流程规范，熟知国家密码管理局相关合规要求，掌握密钥风险防控及应急处置流程。

（6）业务操作方向：受理、审核证书申请，核验订户信息；记录证书全生命周期业务操作。

任职要求：熟悉电子证书签发、更新、撤销、解冻全流程业务规范，掌握订户身份资料核验标准，知晓个人及企业证书业务合规风控要求，能够精准识别虚假申请材料。

（7）客户档案管理方向：负责客户证书档案归档与保密管理。

任职要求：熟知电子认证客户档案保密管理制度、档案保管及销毁规范，掌握纸质档案与电子档案分类归档要求，严格遵守客户隐私数据保密合规条款。

（8）运营审计方向：对核心业务、安全管控、人员权限开展内部审计，排查风险。

任职要求：熟悉电子认证全业务运营流程、内部风控规则及监管审计要求，具备权限风控、业务合规核查能力，岗位独立于所有一线运营及技术岗位，保证审计公正性。

（9）运营管理方向：统筹电子认证整体运营、技术管理、合规风控等工作。

任职要求：精通电子认证法律法规、行业监管政策及公司整体管理制度，具备整体运营统筹、风险决策、合规整改管理能力，熟悉全链条岗位工作流程与权责边界。

可信人员采用账号密码及硬件 USB Key 数字证书双因素强身份认证，全程留存登录及操作实名日志。

各类可信角色配置不少于 3 人的可信人员，实行岗位互备、权限分离制衡机制。

5.2.2. 职责分离

本机构遵循职责分离原则，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人员冗余，在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，以下角色禁止相互兼任：

（1）系统管理方向不与技术运维方向、数据库管理方向、系统

审计方向、密钥管理方向兼任。

（2）技术运维方向不与系统管理方向、数据库管理方向、系统审计方向、密钥管理方向兼任。

（3）数据库管理方向不与系统管理方向、技术运维方向、系统审计方向兼任。

（4）系统审计方向不与系统管理方向、技术运维方向、数据库管理方向兼任。

（5）密钥管理方向不与系统管理方向、技术运维方向兼任；不宜与除策略管理机构成员外的其他可信角色兼任。

（6）业务操作方向不与客户档案管理方向、运营审计方向兼任。

（7）客户档案管理方向不与业务操作方向、运营审计方向兼任。

（8）运营审计方向不与业务操作方向、客户档案管理方向兼任。

5.3. 人员控制

5.3.1. 可信人员资格要求

本机构对可信人员进行相关背景、资历调查，聘任的可信人员具备胜任其工作的相关经验，且没有不良记录。可信人员具体要求如下：

（1）完成从业经历调查和无犯罪记录核查；

（2）具备履行岗位职责所必需的专业技能要求；

（3）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；

（4）签署劳动合同。

5.3.2. 可信人员培训要求

本机构建立覆盖所有可信角色的持续培训体系，所有可信人员上岗前须完成不少于20学时的培训并通过考核；在岗可信人员每年须完成不少于20学时的培训并通过考核。培训内容主要包括：

（1）电子认证服务相关法律法规与标准；

（2）岗位通用职责要求及各角色特定的工作要求；

（3）内部管理政策、制度及流程等；

（4）公钥基础设施（PKI）和密码技术基础知识；

（5）电子认证业务规则（CPS）和证书策略（CP）；

（6）安全管理策略和机制；

（7）订户身份查验审核策略和流程；

（8）电子认证服务运营体系构成；

（9）电子认证服务技术体系构成；

（10）灾难恢复和业务连续性管理。

5.4. 审计日志程序

审计日志是CA系统在运行过程中对关键操作和事件进行记录的日志。本机构对CA系统的审计日志进行记录，并确保：

（1）准确适当地记录CA环境、密钥管理和证书管理事件；

（2）当前和归档的审计日志的机密性和完整性得到维护；

（3）根据CPS将审计日志完整、机密地归档；

（4）审计日志由授权人员审阅。

5.4.1. 记录范围

本机构记录的日志范围：持续、完整地记录关键操作与事件，包

括但不限于:

（1）CA 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;

（2）系统访问行为：包括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;

（3）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查阅等;

（4）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;

（5）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、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;

（6）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

每个事件记录包含时间、类型、内容、操作人、作用对象及结果。对系统的关键操作由操作人员进行电子签名。

5.4.3. 保存期限

系统日志保存至相关证书失效后 5 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、配置未授权变更等安全事件。

5.4.5. 审计周期

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。

5.5. 记录归档

5.5.1. 归档范围

（1）证书申请材料和订户意愿记录;

（2）所有审计日志;

（3）密码设备全生存周期管理记录;

（4）密码设备的日常操作与使用记录;

（5）根证书或密钥生存周期管理相关的全部记录;

（6）证书认证系统运行日志;

（7）已识别的安全事件及处置记录;

（8）证书认证系统关键操作日志;

（9）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 5 年。

5.5.3. 保护措施

本机构对归档文件具有相应的管理制度。

本机构对电子归档记录采取技术手段保障其完整性，并存储在安全的物理与数字环境中，建立备份机制。

对于纸质书面形式的归档记录文件，本机构设有专门的档案管理人员对书面档案进行妥善保存，设置有相应的查阅制度确保只有经批准的人员方可访问书面归档记录。

5.6. 电子认证服务机构根证书密钥更替

5.6.1. 密钥更替的时间

（1）到期更替：本机构根证书密钥有效期到期前两年，启动密钥更新程序；

（2）紧急更替：本机构发现根证书密钥泄露或存在安全隐患后，立即按照《中金金融认证中心有限公司 CA 签名私钥泄漏事件应急处置预案》处置。

5.6.2. 密钥更替程序

（1）密钥生成：在颁发或更换根证书时，在本机构屏蔽机房离线安全区中生成新密钥对。

（2）根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方。

（3）旧密钥处理：在完成签名密钥更替后，按照 GB/T25056-2018 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。

5.7. 损害与灾难恢复

5.7.1. 业务连续性目标

灾难恢复的时间目标（RTO）为 60 分钟，恢复点目标（RPO）为 5 分钟。

5.7.2. 恢复流程

当本机构遭到攻击、发生通讯网络故障、计算机设备不能正常提

供服务、软件遭破坏、数据库被篡改等情况时，本机构将根据制定的业务连续计划等相关规章制度采取合理措施。

业务连续计划由本机构信息安全委员会总负责，其职能包括指导和管理信息安全工作，批准、发布业务连续计划，根据实际情况决定启动灾难恢复等各项职能。

本机构针对不同事件制定了相应的应急处理机制。

本机构具有专门的问题报告和响应机制：本机构向订户、依赖方、软件开发商和其他的第三方提供服务电话，说明如何向本机构报告证书的投诉、私钥泄漏、证书使用不当、其他形式的欺诈、泄漏、使用不当或行为不当等。

5.7.3. 根私钥泄露应急处理

本机构制定了《中金金融认证中心有限公司 CA 签名私钥泄漏事件应急处置预案》，其中明确规定根私钥泄露的内部处理流程、人员分工及对外通知处理流程，每年进行一次应急演练。

5.7.4. 事件报告

详见第 5.9 章节。

5.7.5. 定期验证

定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，每半年至少进行一次灾难恢复演练。

5.8. 电子认证服务机构终止

本机构因技术性原因或商业原因暂停或终止电子认证服务，本机构起草并发布电子认证服务暂停或终止声明，至少提前 90 日就业务

承接及其他有关事项通知证书订户、依赖方等有关各方，并在暂停或终止电子认证服务 60 日前向行业主管部门报告。

本机构与其他具备资质的电子认证服务机构就业务承接进行协商，签署承接协议，明确约定承接机构的工作范围与责任。

业务承接按照下列程序执行:

（1）本机构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;

（2）本机构停止证书状态服务并归档相关数据;

（3）本机构停止其他电子认证相关服务并归档相关数据;

（4）本机构停止密码设备并归档相关密钥数据;

（5）本机构撤销或冻结业务管理员和业务操作员的操作权限;

（6）本机构对所有存档文件记录进行整理和封存;

（7）本机构对所有敏感文档和数据进行安全处理和封存;

（8）本机构清除主机和密码硬件设备中的敏感数据;

（9）本机构清除其他涉及运营的数据、安全密钥等。

与订户证书签发、管理相关的外部合作机构，应在 CPS 中明确描述合作机构终止服务和通告相关的过程

如果未能就业务承接事项与其他具备资质的电子认证服务机构达成协议，本机构将申请行业主管部门安排电子认证服务机构承接相关业务。

如果本机构被依法吊销电子认证服务许可，本机构业务承接事项按照行业主管部门的规定处理。

行业主管部门对此有其他相关要求的，本机构将严格按照行业主管部门的要求进行。

5.9. 重大事项报告

5.9.1. 重大安全事件

重大安全事件是指导致电子认证服务系统无法正常运行或数据安全性受到严重威胁的各类事件，包括但不限于：

（一）证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变等，符合下列任一情形：

（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、更改或者删除用于签发电子签名认证证书的证书链；

（4）其他对电子认证服务安全、用户资料安全有影响的改变。

（二）重大安全事故：包括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，符合下列任一情形：

（1）证书签发及验证服务连续停机时间 30 分钟及以上，有计划的扩容、升级、维护时间除外；

（2）发生根证书和中级证书签名私钥泄露；

（3）发生本机构保存的订户私钥泄露 1000 万条及以上；

（4）电子认证服务系统遭遇病毒入侵，存在异常业务操作。

（三）订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等，符合下列任一情形：

（1）涉及《个人信息保护法》所界定的个人敏感信息1000万条及以上;

（2）个人信息1亿条及以上;

（3）因订户信息泄露造成500万元以上直接经济损失，或100家及以上依赖方投诉;

（4）数据丢失导致无法恢复证书状态信息超过4小时;

（5）法律、行政法规约定的其他情形。

（四）合规性事件：包括不符合相关法律法规、标准或监管要求的事件，符合下列任一情形：

（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。

（五）人力资源类事件：包括1个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等，符合下列任一情形：

（1）涉及2名及以上管理层人员或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。

5.9.2. 重大安全事件报告程序

发生重大安全事故及订户信息泄露事件，本机构在8小时内将事发简要报告报送至安全策略委员会，以及工业和信息化部、国家密码管理局等监管单位。本机构在48小时内将事发报告报送至安全策略委员会，以及工业和信息化部、国家密码管理局等监管单位。事发报告内容包括事件发生时间、事件描述、影响范围和程度、已采取的应

急措施和效果。

应在事件处置完成后 10 个工作日内将事后总结报告报送至安全策略委员会，以及工业和信息化部、国家密码管理局等监管单位。事后总结报告内容包括事件基本情况、事件影响、影响损失评估、根源分析、责任认定、整改措施。

6. 认证系统技术安全控制

6.1. 技术安全管理制度要求

本机构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，并由安全策略委员会定期开展评审，评审频率不少于每年一次。

6.2. 密钥对的生成和安装

6.2.1. 根证书密钥对的生成和安装

本机构根证书密钥对包含根 CA 密钥对、中级 CA 密钥对。本机构根证书密钥对在 CA 机房离线安全区，采用通过国家密码管理部门认可的硬件密码设备生成。

根证书密钥对的生成、备份、恢复、销毁过程实施 5 选 3 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 10 年。

6.2.2. 订户密钥对的生成和交付

订户签名证书密钥对的生成、交付及控制方式，符合下列任一要求。

（1）订户签名证书密钥对由订户负责生成。订户可使用符合国家安全标准的智能密码钥匙（USB Key）或密码模块产生和存储签名证书密钥对。订户应确保其密钥产生的可靠性，负有保护其私钥安全的责任和义务，并承担由此带来的法律责任。

（2）订户委托本机构生成、保存签名证书及密钥对，由本机构提供技术措施确保订户对证书及签名私钥的独占控制权，并完整记录

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 5 年。

（3）采用通过主管部门认可的其他创新性保护方案。

订户加密证书密钥对由本机构的密钥管理系统（KM）生成，并通过安全的方式传输给订户。本机构的密钥管理系统（KM）通过国家密码管理部门安全审查，负责为订户提供产生、备份、恢复加密证书密钥等服务。

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

本机构采用经国家密码主管部门认可的密码机对根证书私钥进行安全保护。本机构 CA 系统密钥生成所使用的密码机部署在本单位机房核心区域，根证书私钥以密文形式存储于密码机内，符合国家标准《信息安全技术 密码模块安全要求》（GB/T 37092—2018）第 5 章相关规定。

本机构根证书私钥实施严格的分割保护机制。本机构存储根证书私钥的密码机激活数据存储在智能密码钥匙或智能 IC 卡，保存在屏蔽机房内最安全区的保险箱中。密码机激活数据分别由 5 位经过授权的密钥持卡人掌握，由 5 位密钥持卡人中的 3 位人员同时在场方可使用，单人无法获取完整私钥。

本机构根证书私钥备份由密钥管理员分别保存在有防盗措施的安全场所。

本机构制定专门的密码机管理办法，从采购、验收、备份、维护、

销毁等环节进行了规范化管理。

6.3.2. 订户私钥保护和密码模块工程控制

订户持有签名私钥，订户应使用符合国家安全标准的密码设备或密码模块中生成并存储私钥，订户应采取有效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。

订户委托本机构保管签名私钥，本机构采取下列措施保护私钥安全：

（1）订户签名私钥在符合国家安全标准的密码设备或密码模块内生成，并以密文形式安全存储；

（2）电子签名模式采用符合国家安全标准，或经主管部门认可的其他合规形式；

（3）订户签名私钥每次调用，本机构均需获得订户明确授权，并对所有涉及订户签名私钥的操作生成可追溯的记录；或采用符合国家安全标准或经主管部门认可其他控制措施；

（4）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；

（5）采取完善的安全管控措施，并定期开展安全评估。

6.4. 密钥对管理的其他方面

6.4.1. 公钥归档

本机构在证书有效期届满后对公钥证书进行归档，证书归档记录自证书有效期届满之日起保留 5 年。

6.4.2. 证书操作期和密钥对使用期限

本机构根证书、中级证书有效期不超过 30 年，订户证书有效期最长不超过 5 年 3 个月。证书密钥对使用期限和证书有效期保持一致。

本机构根证书、中级证书以及订户证书，签名私钥有效期届满后不得用于电子签名；签名公钥有效期届满后可用于验证已生成的电子签名的有效性。加密证书公钥有效期届满后不得继续使用；加密证书私钥有效期届满后可以继续使用，直至密钥对存在被破解风险。

6.5. 激活数据

6.5.1. CA 私钥激活数据的保护

本机构用于保护根证书私钥、中级证书私钥的激活数据，在私钥产生时的操作脚本控制下由智能密码钥匙或智能 IC 卡产生，经授权的 5 位密钥持卡人分持，产生后保存在最安全区的保险柜内。保险柜的密钥由其他 2 位密钥持卡人分持口令管理。密钥持卡人需要使用激活数据时，经安全策略委员会审批后，由保险柜管理员按照操作脚本分发给 5 位中的 3 位密钥持卡人。保护根证书私钥、中级证书私钥激活数据的智能密码钥匙或者智能 IC 卡采用口令保护，口令具有足够长度和复杂度。

6.5.2. 订户私钥激活数据的保护

订户应履行私钥保管主体责任，对持有的激活数据采取安全防护措施，防范激活数据泄露、窃取及篡改风险。

订户私钥激活数据宜采用多种方式，具备足够长度和复杂度，以满足安全要求。

6.6. 计算机安全控制

本机构根据《信息安全技术证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）第 8.2 章节“证书认证中心 安全”相关要求，建立计算机安全控制体系，控制措施包括但不限于:

（1）每季度至少开展一次系统漏洞扫描，检查系统升级补丁，完整留存系统升级审批流程与实施记录;

（2）针对无官方补丁支持的系统，落实网络隔离、功能管控等强化防护手段，并制定系统更替方案;

（3）所有服务器及操作终端统一部署杀毒软件，每日完成病毒库更新与全盘病毒查杀。

6.7. 生存周期安全控制

本机构根据《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）第 10 章节“证书认证中心运行管理要求”、第 11 章节“密钥管理中心运行管理要求”及第 12 章节“证书操作流程”，建立并实施覆盖证书认证系统全生命周期的安全控制体系，规范岗位权限、操作流程、安全审计及文档管理，保障系统、密钥与证书业务全生命周期安全合规、全程可追溯。

6.8. 网络的安全控制

本机构根据《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）第 5.3.8 章节“安全管理系统设计”建立网络安全控制体系，包括但不限于:

（1）网络结构满足《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）附录 A 中规定的形式;

（2）对所有 Web 服务配置防火墙、Web 应用防火墙、通讯加密、入侵检测系统、内容过滤等网络安全防护措施;

（3）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;

（4）建立针对证书签发子系统及数据库的访问白名单机制，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;

（5）建立针对证书注册子系统和数据库的访问白名单机制;

（6）定期对系统日志进行分析，分析内容包括系统异常、未授权访问尝试、资源使用异常、配置异常变更等安全事件。

6.9. 时间戳

本机构时间戳服务遵循国家标准《GB/T 20520-2025 网络安全技术 公钥基础设施 时间戳规范》，兼容互联网工程任务组（IETF）发布的 RFC 3161《互联网 X.509 公钥基础设施-时间戳协议（TSP）》。用于电子认证系统、数字证书、证书撤销列表（CRL）、在线证书状态协议（OCSP）、电子签名等业务提供可信时间支撑。时间信息来源于国家的标准时间源，采用北斗系统和全球定位系统（GPS）两种时间同步方式，实现时间源的精准同步与多路热备份，确保时间戳签发时间的准确性与权威性，同时建立时间同步监测机制，及时纠正偏差，保障时间戳的稳定性。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

本机构签发的数字证书格式符合《信息安全技术 公钥基础设施数字证书格式》（GB/T 20518-2018）的要求。证书的基本结构由基本证书域、签名算法域、签名值域等三部分组成，其中基本证书域由证书基本项和证书扩展项组成。

7.1.1. 证书基本项

证书基本项由版本、序列号、签名算法、颁发者、有效期、主体、主体公钥信息等组成。

7.1.2. 版本号

证书格式是 X.509 V3 版本。

7.1.3. 序列号

证书序列号是电子认证系统分配给所签发证书的用于唯一标识该证书的一个正整数。序列号最大长度为 20 个 8 比特字节。证书更新时，重新分配序列号。

7.1.4. 签名算法

证书签名算法标识如下:

算法	OID	附加参数
SM2	1.2.840.10045.2.1	1.2.156.10197.1.301
sm3WithSM2	1.2.156.10197.1.501	
RSA	1.2.840.113549.1.1.1	

sha1WithRSA	1.2.840.113549.1.1.5	
sha256WithRSA	1.2.840.113549.1.1.11	

7.1.5. 颁发者

颁发者是签发证书的实体，通过一个非空的甄别名来表示本机构的电子认证系统名称。颁发者 DN 如下表所示:

属性	值	说明
通用名（CN）	签发证书的电子认证系统名称，如 CFCA ACS OCA31	电子认证系统名称
机构（O）	China Financial Certification Authority	本机构的英文名称
国家（C）	CN	国家

7.1.6. 有效期

证书有效期是一个时间段，在这个时间段内，本机构将对证书的状态信息进行维护。证书有效期包括证书起始时间和证书终止时间，时间精确到秒。

7.1.7. 主体

证书主体用于描述与主体公钥项中的公钥对应的实体的情况，以主体唯一甄别名 DN 表示。订户证书 DN 通常包含以下域: CN、OU[2]、OU[1]、O、C，详见《CFCA 数字证书数据构成规则》。

7.1.8. 主体公钥信息

证书主体公钥信息用来标识公钥和相应的公钥算法。

7.1.9. 证书扩展项

证书扩展项包括标准扩展项和私有扩展项。扩展项由三部分组成，

分别是扩展类型、扩展关键度和扩展项值。扩展关键度可分为“关键”或“非关键”，用于表明证书使用者是否可以选择忽略该扩展项。证书的应用系统如果不能识别关键的扩展项时，应拒绝接受该证书；如果不能识别非关键的扩展项，则可忽略该扩展项的信息。

本机构签发的证书标准扩展项包括：颁发机构密钥标识符、主体密钥标识符、证书策略及对象标识符、机构信息访问、基本限制、密钥用法、扩展密钥用途、CRL 分发点、主体替换名称等。

本机构针对某种证书类型或者特定订户，可为其签发的证书配置私有扩展项，私有扩展项为非关键扩展。

本机构签发的证书私有扩展项符合 IETF RFC 5280 标准原则。

7.1.9.1. 颁发机构密钥标识符

订户证书中包含颁发机构密钥标识符扩展项，此扩展项用于识别与颁发者证书签名私钥相对应的公钥，可辨别同一电子认证系统使用的不同密钥，该扩展项为非关键扩展项。

7.1.9.2. 主体密钥标识符

订户证书中包含主体密钥标识符扩展项，此扩展项用于识别同一主体使用的不同密钥（如证书密钥更新时），该扩展项为非关键扩展项。

7.1.9.3. 证书策略及对象标识符

本扩展项描述证书策略及对象标识符，遵循本 CPS 第 1.3 章节的规定。该扩展项为非关键扩展项。

电子签名认证证书根据不同证书类型，遵循相应等级证书策略

OID，具体如下：

证书类型	主管部门证书策略 OID	含义
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	适用于涉及生命健康、财产权益等高风险业务场景，为各类电子文件提供可靠电子签名的数字证书。
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	适用于除高等级证书规定的场景外，为各类电子文件提供可靠电子签名的数字证书。
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	适用于涉及生命健康、财产权益等高风险业务场景，为各类电子文件提供可靠电子签名的数字证书。
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	适用于除高等级证书规定的场景外，为各类电子文件提供可靠电子签名的数字证书。

7.1.9.4. 机构信息访问

本扩展项描述最终用户通过何种方式可以访问 CA 信息。包括在线验证服务和 CA 证书地址。该扩展项为非关键扩展项。

7.1.9.5. 基本限制

根证书、中级证书，基本限制扩展项中 Subject Type 为 CA，且该项必须为关键扩展项。

订户证书，基本限制扩展项中 Subject Type 为 End Entity。

7.1.9.6. 密钥用法

本扩展项指已认证的密钥用于何种用途。

根证书、中级证书的密钥用法包含证书签名（keyCertSign）、CRL 签名（cRLSign），该项为关键扩展项。

订户签名证书的密钥用法包含数字签名（digitalSignature）、不可否认（nonRepudiation）；订户加密证书的密钥用法包含密钥加密（keyEncipherment）、数据加密（dataEncipherment）、密钥协商（keyAgreement），该项为关键扩展项。

7.1.9.7. 扩展密钥用法

本扩展项指已验证的公钥可用于一种或多种用途，可作为对密钥用法扩展项中指明的基本用途的补充或替代。该扩展项为非关键扩展项。本机构签发的证书根据不同的证书类型，该项有不同的配置。

7.1.9.8. CRL 分发点

本扩展项描述电子认证系统签发的订户证书包含的 CRL 分发点。依赖方可根据该扩展项提供的地址和协议下载证书撤销列表（CRL）。该扩展项为非关键扩展项。

7.1.9.9. 主体替换名称

本扩展项包含一个或多个可选替换名称（可使用多种名称形式中的任一个）供实体使用。该扩展项的使用符合 IETF RFC 5280 的规定。该扩展项为非关键扩展项。

服务器证书必须包括该扩展项，且只能存放域名或者 IP 地址，在主体替换名称域中要求处于该域中的任何信息必须全部经过审核。其他类型的证书可不包含该域。

7.1.9.10. 关键证书策略扩展项的处理规则

如果应用系统无法识别证书中的关键扩展项或识别出包含无法处理的关键扩展项，应用系统必须拒绝使用该证书。如果应用系统无

法识别非关键扩展，则可以忽略；如果识别出非关键扩展项，则可对其进行处理。

7.2. 证书撤销列表

本机构签发的证书撤销列表(CRL)的格式符合《信息安全技术 公钥基础设施 数字证书格式》（GB/T 20518-2018）第 5.3 章节“证书认证系统 系统设计”的相关要求。

7.3. 在线证书状态协议

本机构提供在线证书状态协议（OCSP）服务符合《网络安全技术 公钥基础设施 在线证书状态协议》(GB/T 19713-2025)第 7 章节“具体语法”的相关要求，以及互联网工程任务组（IETF）《X.509 公钥基础设施中的在线证书状态协议》（RFC 6960）的相关规范。

8. 认证机构审计及相关评估

8.1. 审计评估制度

本机构制定了审计评估制度，审计评估的类型包括认证业务审计和全面符合性评估。

本机构在如下情形接受评估或自行进行评估:

（1）根据《电子认证服务管理办法》和《电子认证服务密码管理办法》的规定，接受主管部门的全面符合性评估和检查;

（2）本机构电子认证系统每年进行网络安全等级保护三级测评;

（3）本机构按照内部管理制度，定期审计认证业务。

认证业务审计人员与负责被审计被评估内容的人员的岗位职责不重叠。认证业务审计人员应具有法律或内审资格，且在日常工作中不得参与与证书签发相关的任何生产服务工作。

本机构聘请外部测评机构对本机构进行评估时，按照相关评估事项，选择具备相关测评资质的机构及人员对本机构的运营管理进行合规性审查。本机构要求测评人员事先熟悉公钥基础设施技术及相关的法律法规、标准规范要求。外部测评机构与本机构之间是相互独立的关系，双方无任何足以影响评估客观性的利害关系。

8.2. 认证业务审计

本机构统一以完整自然年度作为标准审计周期，审计周期按自然年常态化开展认证业务审计工作。

认证业务审计内容包括但不限于：证书申请、续期、密钥变更、更新、撤销、冻结等全流程业务中，订户告知、身份查验、意愿记录、

协议签署、资料保存、验签操作及 CA 对外举证等环节的真实性、关联性和合规性核查。审计人员开展工作可行使必要权限，不受干预查阅认证业务全流程各类资料、向内外部相关人员深入问询，可深入项目业务现场实地核查、参与与监管机构的交流、调取系统数据及日志并要求相关部门配合，对违规环节核查追溯、监督整改落实，如实编制审计报告并上报相关情况，对阻碍审计工作、提供虚假资料的可提出追责建议。

每个审计周期内，选取的审计项目业务量占当期认证业务总业务量的比例不低于 60%，通过合理的抽样规模，充分兼顾审计效率与审计质量，确保审计结论能够客观反映当期认证业务的整体合规水平。

8.3. 全面符合性评估

本机构评估周期每年一次。评估内容涵盖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及认证规则与证书策略符合性等相关事项。针对审计发现的问题，及时通知被审计部门限期整改，并全程跟踪整改进度与落实情况；同时应于每年 1 月底前，将上一年度符合性评估报告按要求报送至主管部门。

9. 法律责任和其他业务条款

9.1. 费用

本机构结合日常运营成本、服务运维标准及行业规范，开展电子认证服务成本核算，制定服务价格策略。

本机构电子认证服务收费项目包括但不限于：数字证书、身份认证、电子签名、电子数据存证、电子签名验证，以及相关软硬件产品及其他配套增值服务费用。

本机构所有收费按照既定价格策略执行，各项收费标准可联系本机构获取。

本机构仅在本机构违反本 CPS 所规定的义务时，订户可通过原支付通道申请退回已支付但未使用服务对应的费用，其他情形不予退款。若因订户自身原因，在服务有效期内终止服务的，剩余周期内的服务费用不予退还。

9.2. 财务责任

本机构建立赔付专项备用资金保障机制，作为因本机构电子认证业务过失、证书服务差错、系统运营责任等情形造成用户合法权益损失的赔付兜底保障。

本机构赔付专项备用资金保障额度严格按照上一会计年度经审计本公司财务报表列示的营业收入的 1.5%足额留存（提取金额以百万元为最小单位向上取整），每年依据年度审计结果动态核定、补足差额，持续维持合规保障额度标准。

赔付专项备用资金来源为本机构自有经营积累资金，实行专户存

储、专款专用、独立管理，与日常经营周转资金分账核算，不得挪用于经营扩张、分红、固定资产购置等支付类用途。每年配合外部审计机构对赔付备用资金的额度充足性、管理规范性、专款专用执行情况进行审计核查，并按监管要求接受主管部门监督检查。

本机构亦保留采用银行履约保函、专业责任保险、母公司连带责任担保等合规资金保障替代方式的权利，确保任何时候均具备足额损失赔付履约能力，保障电子认证服务相关各方合法权益。

9.3. 业务信息保密

9.3.1. 保密信息范围

本机构保密信息包括但不限于下列内容:

（1）本机构认证体系的各种配置信息，包括但不限于根证书、中级证书私钥及保护口令;

（2）本机构认证系统的各种备份信息，包括但不限于根证书、中级证书私钥备份分割保护信息;

（3）本机构各种测评、审计等活动的溯源记录及审计记录等;

（4）本机构订户证书信息以外的个人隐私信息;

（5）本机构标注密级的其他信息。

9.3.2. 不属于保密的信息

不属于本机构保密的信息包括:

（1）证书记载信息、证书撤销列表（CRL）信息;

（2）在提供方披露数据和信息之前，已被接受方所持有的数据和信息;

（3）在提供方披露数据和信息时或在披露数据和信息之后，非因接受方的原因而被披露的信息；

（4）经公开或通过其他途径成为公众领域的一部分数据和信息；

（5）有权披露的第三方，披露给接受方的数据和信息；

（6）其他可以通过公共、公开渠道获得的信息。

9.3.3. 保密信息的保护责任

本机构通过各种严格的管理制度、流程和技术手段来保护保密信息，包括但不限于商业机密、订户资料、客户信息等。本机构所有员工均接受信息保密方面的培训。

当本机构在法律法规、监管部门或执法部门的要求下必须依法提供本 CPS 中具有保密性质的信息时，本机构按照要求向监管部门或执法部门提供相关的保密信息，本机构无须承担任何责任。这种披露不视为违反保密的要求和义务。

9.4. 个人隐私保护

本机构严格遵循《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》相关规定，参照《信息安全技术 个人信息安全规范》（GB/T 35273-2020）制定个人隐私信息保护措施，详见本机构《法律声明及个人信息保护政策》。

9.5. 知识产权

本机构依法持有并保留数字证书、自有软件、文档资料、业务数据等全部内容的著作权、专利申请权及其他各类知识产权。本机构制定并发布的电子认证业务规则（CPS）、证书策略（CP）、技术手册、

数字证书、证书撤销列表（CRL）等文件与载体，其所有权及知识产权均归属本机构。

订户公钥经本机构核验签发为数字证书后，该证书及证书撤销列表（CRL）统一存储、发布于本机构信息数据库。该数据库所有权归本机构所有。本机构仅授予订户及依赖方使用权限。

9.6. 陈述和担保

9.6.1. 本机构的陈述与保证

本机构采用经过国家有关管理机关审批的信息安全基础设施开展电子认证服务业务。

本机构的运作遵守《中华人民共和国电子签名法》及相关法律的规定，接受行业主管部门的指导。本机构对签发的数字证书承担相应法律责任。

本机构保证使用的系统及密码符合国家政策与标准，保证根证书签名私钥在本机构内部得到安全地存放和保护，建立和执行的安全机制符合国家政策的规定。

本机构的运营遵守本 CPS，并随着业务的调整对 CPS 进行修订。

本机构依据《电子认证服务管理办法》相关规定，不定期开展内部审计，核查本机构电子认证业务执行情况是否符合本 CPS 的约定。

本机构具有保存和使用证书持有人信息的权利。

本机构不参与订户及依赖方使用数字证书的具体行为，不承担因订户及依赖方自身过错使用证书所造成的损害赔偿责任。

9.6.2. 订户的陈述、保证与义务

订户确认已经阅读和理解本 CPS 及《CFCA 电子认证服务协议》的全部内容，并同意接受本 CPS 文件规定的约束。

订户知晓利用数字证书所做的电子签名与手写签名具有同等法律效力。订户应遵循诚实、信用原则，申请数字证书时，应当提供真实、完整、准确的信息和资料。

订户可自行或委托他人申请数字证书。在申请证书时，订户应向本机构支付相应的服务费。

订户应在上述信息、资料发生改变时及时通知本机构。如因订户故意或过失提供的资料不真实、不完整、不准确或资料改变后未及时通知本机构，造成的损失由订户自行承担。

订户须使用经合法途径获得的相关软件，且合法使用本机构发放的数字证书，承诺使用数字证书前已确认证书正确。承诺使用证书的行为符合订户真实意愿或者仅为了处理已获得授权的事务，并对使用数字证书的行为负相关法律责任。

订户用于电子签名的证书私钥，应由订户产生，并应采取必要手段来保障证书的私钥或相关密码的安全存储、使用、备份等。如订户委托本机构产生，本机构采取必要手段来保障证书的私钥安全。

如订户使用的数字证书私钥、密码或口令泄漏、丢失，或者订户不希望继续使用数字证书，或者订户主体不存在时，订户或法定权利人应当立即联系本机构，申请撤销该数字证书。证书过期或被撤销后，订户将不得继续使用该证书。

如因订户原因，导致依赖方或本机构遭受损失的，订户需承担相

应的赔偿责任，包括但不限于下列情形:

（1）订户在申请数字证书时没有提供真实、完整、准确信息，或在这些信息变更时未及时通知本机构，导致依赖方遭受损失需要由本机构赔偿的情况;

（2）订户知悉自己的私钥已经失密或者可能已经失密而未及时告知本机构，并继续使用导致依赖方遭受损失需要本机构赔偿的情况;

（3）订户使用失效证书（包括证书过期、证书被撤销），给依赖方造成损失，或者有其他过错或未履行本 CPS 的相关约定，违反相关法律法规的情况。

订户一旦发现或怀疑由本机构提供的电子认证服务造成订户的网上交易信息的泄漏、篡改，应在 24 小时内向本机构提出争议处理申请，并通知有关各方。

9.6.3. 依赖方的陈述、保证与义务

依赖方应通过本机构官方途径获取并安装 CFCA 证书链。

依赖方应在信赖证书所证明的信任关系前确认该证书为有效证书，包括:检查最新的证书撤销列表(CRL)或在线证书状态协议(OCSP)，确认该证书未被撤销;检查该证书链的可靠性;检查该证书的有效期;以及检查其他能够影响证书有效性的信息。

依赖方应在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内容一致。

依赖方应熟悉本 CPS 的条款，了解证书的使用目的，在符合本 CPS 规定的证书应用范围内信任该证书。

依赖方同意本 CPS 中关于本机构责任限制的规定。

9.6.4. 其他参与者的陈述与保证

未列明的其他参与者应遵循本 CPS 的规定。

9.7. 担保免责

如果订户提供不准确、不真实、不完整的信息，或重要信息变更未及时通知，向本机构申请签发证书，订户因使用该证书而产生的纠纷，由订户自行承担全部法律责任，本机构对此不承担任何责任或后果。

由于非本机构原因造成的设备故障、网络中断导致证书报错、交易中断或其他事故造成的损失，损失方可以追究侵权方责任，本机构给予配合，但本机构不向任何一方承担赔偿或补偿责任。

本机构对各类证书的适用范围做了规定，若证书被超出范围使用或被用于其他未被本机构允许的用途，本机构不承担任何法律责任。

本机构由于不可抗力因素或必要的机构调整导致本机构暂停、终止部分或全部数字证书服务，本机构不承担赔偿或补偿责任。

本机构在法律许可的范围内，根据有关法律法规的要求，如实提供电子交易和网络交易中产生的数字签名的验证信息的验证服务，对非因该验证服务而导致的任何后果，本机构不承担任何法律责任。

本机构对于民事主体未尽必要的资质审核，如因依赖方、订户使用的应用软件未按照约定使用数字证书、未验证证书有效性等导致的依赖方、订户遭受损失的，依赖方订户可以追究侵权人的责任，本机构给予配合，但本机构不承担赔偿或补偿责任。

9.8. 偿付责任规则

除非有另外的规定或约定，对于非因本 CPS 项下的认证服务而导致的任何损失，本机构不向订户和/或依赖方承担任何赔偿和/或补偿责任。

订户或依赖方进行的民事活动因本机构提供的认证服务而遭受的损失，本机构将依据本 CPS 的相关条款给予相应的赔偿，具体赔偿见《CFCA 电子认证服务协议》。如果本机构能够证明提供的服务是按照《中华人民共和国电子签名法》《电子认证服务管理办法》等现行法律法规，以及本机构向主管部门备案的 CPS 实施的，则视为本机构不具有任何过错，本机构将不对订户或依赖方承担任何赔偿责任。

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

（1）订户和/或依赖方的任何预期损失或间接损失、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;

（2）由上述第（1）项所述的损失相应产生或附带引起的损失或损害;

（3）非因本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。

无论本 CPS 是否有相反或不同规定，如果本机构根据本 CPS 或任何法律规定，以及司法判定须承担赔偿和/或补偿责任的，本机构将按照相关法律法规的规定、仲裁机构的裁决或法院的判决承担相应的

赔偿责任。

9.9. 赔偿

本机构在电子认证服务过程中，针对因自身服务过失给证书用户及相关方造成合法权益损害的情形，建立规范的损害赔偿机制。由运营中心统一受理赔偿申请并开展初步核查；经核查情况属实的，移交法律与风控部开展责任认定及赔偿方案审核；审核通过后提交内部审批流程；审批完成后由财务部负责赔偿款项支付。赔偿全流程办理时限不超过 60 日。本机构严格依照既定流程与时限完成赔偿相关处置工作。

9.10. 有效期和终止

本 CPS 自官方网站公示版本所标注的生效日期起正式生效，另有提前终止约定的除外。

新版本规则生效当日，原版本自动废止。

本机构可终止 CPS 及其修订版本，且在终止前 30 日，于官方网站发布终止公告。

本 CPS 中有关审计、保密信息、隐私保护、知识产权以及赔偿责任的限制等条款，在本 CPS 终止后继续有效。

9.11. 对参与者的个别通告与沟通

电子认证各参与方之间开展相互通信、单方通告及业务沟通时，须执行本规则约定的通信方式，确保相关通信行为合法有效。所有正式通告、业务往来信息均通过双方确认的官方系统、预留电子信箱或书面通讯渠道传递；联络信息发生变更的，参与方应及时完成报备，

未及时报备引发的相关后果由责任方承担。

9.12. 修订和发布

本机构定期评估本 CPS 的适用性，并将修订后的版本在官方网站公布。修订后的版本自版本标注的生效日期起生效，并对各参与方具有约束力。订户、依赖方等需定期查阅 CPS 最新版本。

本 CPS 修订程序详见第 1.6.2 章节。

本机构有权修订本 CPS 中的任何术语、条款，修订后将及时在本机构官方网站公布。如订户在修订公布后 10 日内，未申请证书撤销，将被视为同意该修订。

当本 CPS 描述的规则、流程和相关技术已经不能满足本机构电子认证业务要求，或者本 CPS 依据的法律法规和相关主管部门规章变更时，本机构将依照有关规定修改本 CPS 的相关内容。

9.13. 争议处理与举证

本条款适用于本机构、订户、依赖方之间的所有争议、投诉及索赔纠纷，争议包括本机构与订户的证书服务相关争议、本机构与依赖方的信赖利益争议等相关情形。争议一方应在知晓争议或权利受损之日起 3 个月内，书面向相对方提出争议处理请求并通知其他相关方，各方在收到请求后 30 日内协商解决，协商不成可申请第三方调解；本机构设立专门投诉渠道，收到投诉后 15 日内反馈初步处理意见，复杂事项可延长 15 日并书面说明理由；协商或调解不成的，任何一方可将争议提交北京仲裁委员会按其届时有效规则仲裁，仲裁地为北京，裁决为终局。仲裁条款无效的，可向本机构所在地有管辖权的人

民法院提起诉讼。

任何订户或依赖方向本机构提出索赔诉求的，必须在其知道或者应当知道自身权利遭受损害之日起的1年内提出。一旦超出1年期限，该项索赔将不具备法律效力，本机构有权拒绝受理。

依据《民事诉讼法》相关规定，本机构对其服务合规性负有举证责任；本机构需留存证书全生命周期举证记录，涵盖签发、签名、验证签名各环节相关记录，收到有效举证请求后，30个工作日内提供相关记录副本，复杂事项的可延长30个工作日并书面说明理由。

9.14. 管辖法律

本CPS和协议中条款遵守《中华人民共和国民法典》《中华人民共和国电子签名法》《中华人民共和国密码法》《电子认证服务管理办法》及相关法律规定。如CPS中某项条款与上述法律条款或其可执行性发生抵触，本机构将会对此条款进行修改，使之符合相关法律规定。

9.15. 与适用法律的符合性

本机构的各项策略均遵守并符合中华人民共和国现行有效的法律法规及相关主管部门的监管要求，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

本CPS将替代所有以前的或同时期的、与相同主题相关的书面或

口头解释。

本 CP、CPS、订户协议、依赖方协议以及订户协议和依赖方协议的补充协议构成各参与者之间的完整协议。

本机构、订户及依赖方之间的权利义务不能通过任何形式转让给任何人。

本 CPS 的某一条款被主管部门宣布为违法、不可执行或无效时，本机构将对该不符合性条款进行修改，直至该条款合法、有效和可执行为止，但此条款的违法、不可执行或无效，不影响本 CPS 中其他条款的有效性。

不可抗力是指因无法预见、不可避免且不可克服的客观情况，导致合同一方或多方无法履行义务的情形。构成不可抗力的事件包括但不限于：战争、恐怖行动、罢工、自然灾害（如地震、洪水）、重大传染病、互联网或其他基础设施无法使用等。本机构对因不可抗力导致的损害不承担赔偿责任，但各方都有义务建立灾难恢复和业务连续性机制。

本机构与订户签订的《CFCA 电子认证服务协议》，明确标注其对应的本 CPS 具体版本号，确保协议内容与对应版本 CPS 的条款要求保持一致，便于各方查阅、执行及追溯，避免因版本混淆引发相关争议及合规风险。

9.17. 其他条款

本 CPS 最终解释权由本机构所有，由本机构负责解释和修订。

附录：CFCA 电子认证系统及证书链

CA 系统	证书 类型	证书主题	证书序列号	颁发 机构	密码 算法	证书 有效期	计划 服务时间
	根证书	O=CFCA CS CA C=CN	18255284	CFCA CS CA	RSA 2048	2011/5/20 -2041/5/12	2041/5/12
CFCA OCA1	中级 证书	O=CFCA OCA1 C=CN	1000000019	CFCA CS CA	RSA 2048	2011/5/21 -2031/5/16	2031/5/16
CFCA OCA11	中级 证书	CN=CFCA CS OCA11 O=China Financial Certification Authority C=CN	1000000024	CFCA CS CA	RSA 2048	2012/8/22 -2031/5/15	2031/5/15
CFCA GT OCA21	中级 证书	CN=CFCA GT OCA21 O=China Financial Certification Authority C=CN	1000000032	CFCA CS CA	RSA 2048	2020/10/16 -2035/7/4	2035/7/4
	根证书	CN=CFCA ACS CA O=China Financial Certification Authority C=CN	41aef3cfbe44 64544f64f89a 97f23917	CFCA ACS CA	RSA 4096	2015/9/23 -2035/9/28	2035/9/28
CFCA ACS OCA31	中级 证书	CN=CFCA ACS OCA31 O=China Financial Certification Authority C=CN	34ac474cf8f2 15698f66f4a0 f7b986bc	CFCA ACS CA	RSA 2048	2015/9/27 -2035/9/22	2035/9/22
CFCA ACS OCA32	中级 证书	CN=CFCA ACS OCA32 O=China Financial Certification Authority C=CN	35fa6b4521c6 e75270a78aee 64415e7c	CFCA ACS CA	RSA 2048	2015/9/27 -2035/9/22	2035/9/22
CFCA ACS OCA33	中级 证书	CN=CFCA ACS OCA33 O=China Financial Certification Authority C=CN	265c5c3af558 f083f6d0c594 3ff4c4aa	CFCA ACS CA	RSA 2048	2017/9/4 -2035/9/5	2035/9/5
CFCA ACS OCA34	中级 证书	CN=CFCA ACS OCA34 O=China Financial Certification Authority C=CN	75a38a83ee08 e8305d2dd177 65265ba1	CFCA ACS CA	RSA 2048	2017/9/4 -2035/9/4	2035/9/4

CA 系统	证书 类型	证书主题	证书序列号	颁发 机构	密码 算法	证书 有效期	计划 服务时间
	根证书	CN=CFCA CS SM2 CA O=China Financial Certification Authority C=CN	172f4259	CFCA CS SM2 CA	SM2 256	2012/8/31 -2042/8/24	2042/8/24
CFCA SM2 OCA1	中级证书	O=CFCA SM2 OCA1 C=CN	1000000008	CFCA CS SM2 CA	SM2 256	2013/1/24 -2033/1/19	2033/1/19
CFCA CS SM2 OCA11	中级证书	CN=CFCA CS SM2 OCA11 O=China Financial Certification Authority C=CN	1000000007	CFCA CS SM2 CA	SM2 256	2012/8/31 -2031/5/15	2031/5/15
CFCA GT SM2 OCA21	中级证书	CN=CFCA GT SM2 OCA21 O=China Financial Certification Authority C=CN	1000000034	CFCA CS SM2 CA	SM2 256	2020/10/16 -2035/7/4	2035/7/4
CFCA ACS SM2 OCA31	中级证书	CN=CFCA ACS SM2 OCA31 O=China Financial Certification Authority C=CN	1000000012	CFCA CS SM2 CA	SM2 256	2015/9/27 -2035/7/4	2035/7/4
CFCA ACS SM2 OCA32	中级证书	CN=CFCA ACS SM2 OCA32 O=China Financial Certification Authority C=CN	1000000014	CFCA CS SM2 CA	SM2 256	2015/9/27 -2035/7/4	2035/7/4
CFCA ACS SM2 OCA33	中级证书	CN=CFCA ACS SM2 OCA33 O=China Financial Certification Authority C=CN	1000000021	CFCA CS SM2 CA	SM2 256	2017/9/4 -2035/7/4	2035/7/4
CFCA ACS SM2 OCA34	中级证书	CN=CFCA ACS SM2 OCA34 O=China Financial Certification Authority C=CN	1000000022	CFCA CS SM2 CA	SM2 256	2017/9/4 -2035/7/4	2035/7/4