CFCA电子认证服务证书策略

CFCA Certificate Policy

V4.1

版权归属中金金融认证中心有限公司

（任何单位和个人不得擅自翻印）

生效日期：2026年9月12日

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

版本控制表

版本	修改状态	修改说明	修改人	审核人/批准人	修改日期
1.0	形成版本并审核通过			CFCA 安委会	2011 年 06 月
2.0	修订	根据 2013 年 4 月 7 日策略管理委员会评审结论修改相关内容	赵改侠	CFCA 安委会	2013 年 04 月
2.1	修订	依据 BR 的补充相关条款	赵改侠	CFCA 安委会	2014 年 03 月
3.0	修订	根据最新 CPS 以及政策变更修改，本 CP 适应于 CFCA 所有 CPS。	赵改侠 张　翼	CFCA 安委会	2015 年 08 月
3.1	修订	兼容京港电子认证服务项目，本 CP 适应于 CFCA 所有 CPS	孙圣男	CFCA 安委会	2018 年 11 月
4.0	修订	修订 1.1 符合的具体标准及法律法规；修订 1.2 OID 标识；优化修订了 1.4 证书应用。其他为参照标准进行的优化描述。CP 适应于 CFCA 通用型电子认证服务体系的 CPS。	编写组	CFCA 策略管理委员会	2025 年 08 月
4.1	修订	调整相关业务规则	编写组	CFCA 策略管理委员会	2026 年 09 月

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

目　　录

1 概括性描述 1
1.1 概述 1
1.2 文档名称与标识 2
1.3 电子认证活动参与者 3
1.3.1 电子认证服务机构 3
1.3.2 注册机构 3
1.3.3 订户 4
1.3.4 依赖方 4
1.3.5 其他参与者 4
1.4 证书应用 4
1.4.1 适合的证书应用 4
1.4.2 限制的证书应用 6
1.5 策略管理 7
1.5.1 策略文档管理机构 7
1.5.2 联系方式 7
1.5.3 决定 CP 符合策略的机构 7
1.5.4 CP 批准程序 8
1.6 定义和缩写 8
2 发布与信息库责任 11
2.1 信息库 11
2.2 认证信息的发布 11
2.3 发布的时间或频率 12
2.4 信息库访问控制 12
3 标识与鉴别 12
3.1 命名 12
3.1.1 名称类型 12
3.1.2 对名称意义化的要求 12
3.1.3 订户的匿名或伪名 13
3.1.4 解释不同名称形式的规则 13
3.1.5 名称唯一性 13
3.1.6 商标的识别、鉴别和角色 13
3.2 初始身份确认 14
3.2.1 证明拥有私钥的方法 14
3.2.2 订户身份的鉴别 14
3.2.3 没有验证的订户信息 15
3.2.4 授权确认 15
3.2.5 互操作准则 15
3.3 密钥更新请求的标识与鉴别 15
3.3.1 常规密钥更新的标识与鉴别 15
3.3.2 撤销后的密钥更新的标识与鉴别 16
3.4 撤销请求的标识与鉴别 16

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4 证书生命周期操作要求 17
4.1 证书申请 17
4.1.1 证书申请实体 17
4.1.2 注册过程与责任 17
4.2 证书申请处理 19
4.2.1 执行识别与鉴别功能 19
4.2.2 证书申请批准和拒绝 19
4.2.3 处理证书申请的时间 20
4.3 证书签发 20
4.3.1 证书签发中电子认证服务机构的行为 20
4.3.2 电子认证服务机构对订户的通告 20
4.4 证书接受 21
4.4.1 构成接受证书的行为 21
4.4.2 电子认证服务机构对证书的发布 21
4.4.3 电子认证服务机构对其他实体的通告 21
4.5 密钥对和证书的使用 22
4.5.1 订户私钥和证书的使用 22
4.5.2 依赖方对公钥和证书的使用 23
4.6 证书更新 23
4.7 证书密钥更新 24
4.7.1 证书密钥更新的情形 24
4.7.2 请求证书密钥更新的实体 25
4.7.3 证书密钥更新请求的处理 25
4.7.4 颁发更新证书时对订户的通告 25
4.7.5 构成接受密钥更新证书的行为 25
4.7.6 电子认证服务机构对密钥更新证书的发布 25
4.7.7 电子认证服务机构对其他实体的通告 25
4.8 证书变更 25
4.9 证书撤销和冻结 26
4.9.1 证书撤销的情形 26
4.9.2 请求证书撤销的主体 27
4.9.3 请求撤销的流程 28
4.9.4 撤销请求宽限期 29
4.9.5 电子认证服务机构处理撤销请求的时限 29
4.9.6 依赖方检查证书撤销的要求 29
4.9.7 CRL 发布频率 30
4.9.8 CRL 发布的最大滞后时间 30
4.9.9 在线证书状态查询的可用性 30
4.9.10 撤销信息的其他发布形式 30
4.9.11 对密钥遭受安全威胁的特别处理要求 30
4.9.12 证书冻结及解冻 30
4.10 证书状态服务 31
4.10.1 操作特征 31
4.10.2 服务可用性 31

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.11 服务终止 31
4.12 密钥托管与恢复 31
4.13 证书归档 32
5 认证机构设施、管理和操作控制 32
5.1 物理控制 32
5.2 程序控制 32
5.2.1 可信角色 32
5.2.2 每项任务需要的人数 33
5.2.3 每个角色的识别与鉴别 33
5.2.4 需要职责分割的角色 34
5.3 人员控制 34
5.3.1 资格、经历和无过失要求 34
5.3.2 背景审查程序 34
5.3.3 培训要求 34
5.3.4 再培训周期和要求 35
5.3.5 未授权行为的处罚 35
5.3.6 独立合约人的要求 35
5.3.7 提供给员工的文档 35
5.4 审计日志程序 36
5.4.1 审计日志记录事件的类型 36
5.4.2 处理审计日志的周期 37
5.4.3 审计日志的保存期限 37
5.4.4 审计日志的保护 37
5.4.5 审计日志备份程序 38
5.4.6 审计日志收集系统 38
5.4.7 对导致事件主体的通告 38
5.4.8 脆弱性评估 38
5.5 记录归档 38
5.5.1 归档记录的类型 38
5.5.2 归档记录的保存期限 39
5.5.3 归档文件的保护 39
5.5.4 归档文件的备份程序 39
5.5.5 记录的时间戳要求 40
5.5.6 归档收集系统 40
5.5.7 获得和检验归档信息的程序 40
5.6 电子认证服务机构密钥更替 40
5.7 损坏与灾难恢复 40
5.7.1 事故和损害处理程序 40
5.7.2 计算资源、软件或数据的损坏 41
5.7.3 实体私钥损害处理程序 41
5.7.4 灾难后的业务连续性能力 41
5.8 电子认证服务机构或注册机构的终止 41
5.9 预植证书的生产管理规程 41
6 认证系统技术安全控制 42

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.1 密钥对的生成和安装 42
6.1.1 密钥对的生成 42
6.1.2 私钥传送给订户 43
6.1.3 公钥传送给证书签发机构 43
6.1.4 CA 机构公钥传送给依赖方 43
6.1.5 密钥的长度 43
6.1.6 公钥参数的生成和质量检查 43
6.1.7 密钥使用目的 44
6.2 私钥保护和密码模块工程控制 44
6.2.1 密码模块标准和控制 44
6.2.2 私钥多人控制 44
6.2.3 私钥托管 44
6.2.4 私钥备份 45
6.2.5 私钥归档 45
6.2.6 私钥导入、导出密码模块 45
6.2.7 私钥在密码模块的存储 45
6.2.8 激活私钥的方法 46
6.2.9 解除私钥激活状态的方法 46
6.2.10 销毁私钥的方法 46
6.2.11 密码模块的评估 46
6.3 密钥对管理的其他方面 46
6.3.1 公钥归档 46
6.3.2 证书操作期和密钥对使用期限 47
6.4 激活数据 47
6.4.1 激活数据的产生和安装 47
6.4.2 激活数据的保护 47
6.4.3 激活数据的其他方面 47
6.5 数据安全控制 48
6.6 计算机安全控制 48
6.6.1 特别的计算机安全技术要求 48
6.6.2 计算机安全评估 48
6.7 CA 系统生命周期技术控制 49
6.7.1 系统开发控制 49
6.7.2 安全管理控制 49
6.7.3 生命周期的安全控制 49
6.8 网络的安全控制 50
6.9 时间戳 50
7 证书、证书撤销列表和在线证书状态协议格式 50
7.1 证书格式 50
7.1.1 证书基本项 51
7.1.2 版本号 51
7.1.3 序列号 51
7.1.4 签名算法 51
7.1.5 颁发者 52

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

7.1.6 有效期 52
7.1.7 主体 52
7.1.8 主体公钥信息 53
7.1.9 证书扩展项 53
7.2 证书撤销列表格式 56
7.2.1 版本号 56
7.2.2 CRL 和 CRL 条目扩展项 57
7.3 在线证书状态协议格式 57
7.3.1 版本号 57
7.3.2 OCSP 扩展项 58
8 一致性审计和其他评估 58
8.1 评估者的情形及其频率 58
8.2 评估者的资质 58
8.3 评估者与被评估者的关系 59
8.4 评估内容 59
8.5 对问题与不足采取的措施 59
8.6 评估结果的传达与发布 59
8.7 其他评估 60
9 法律责任和其他业务条款 60
9.1 费用 60
9.2 财务责任 60
9.3 业务信息保密 61
9.4 个人信息保护 61
9.5 知识产权 61
9.6 陈述与保证 61
9.6.1 电子认证服务机构的陈述与保证 61
9.6.2 注册机构的陈述与保证 62
9.6.3 订户的陈述、保证及义务 62
9.6.4 依赖方的陈述与保证及义务 63
9.6.5 其他参与者的陈述与保证 63
9.7 保证免责 63
9.8 承担赔偿责任的限制 63
9.9 有效期限与终止 64
9.9.1 有效期限 64
9.9.2 终止 64
9.9.3 终止后的存续条款 64
9.10 通告与沟通 64
9.11 修订 65
9.11.1 修订程序 65
9.11.2 通知机制和期限 65
9.11.3 必须修改业务规则的情形 65
9.12 争议解决 66
9.13 管辖法律 66
9.14 与适用法律的符合性 66

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

9.15 一般条款 66
9.15.1 本 CP 的完整性 66
9.15.2 转让 67
9.15.3 分割性 67
9.15.4 强制执行 67
9.15.5 不可抗力 67
9.16 最终解释权 67
附录 A: CFCA 电子认证服务业务规则 V5.0 约束 CA 系统 68

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

1 概括性描述

1.1 概述

中金金融认证中心有限公司(即 China Financial Certification Authority，以下简称“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服务机构，具有《电子认证服务许可证》及《电子认证服务使用密码许可证》资质。

本文档《CFCA 电子认证业务证书策略》(以下简称“CFCA CP”、“本 CP”)，按照工业和信息化部发布的《电子认证服务管理办法》的要求，报工业和信息化部备案。

CFCA 作为专业的电子认证服务机构，基于公钥基础设施(PKI)技术，向公众(包括政府机关、企事业单位、其他组织及个人)提供电子认证服务，保证电子签名的真实性和可靠性。本 CP 阐述了提供电子认证服务各参与方所应满足的安全要求及各项操作规范。适用于电子认证服务机构、注册机构、订户、依赖方等电子认证活动参与者，各方应充分理解本文档所约定的责任，并承担相应的责任和义务。

本 CP 目录结构与 GB/T 26855-2011《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》基本保持一致，本 CP 中如有“应”相关要求的，均是相关各方需要满足的要求，如 CPS 声称符合本 CP，则需要在CPS中说明是否满足该策略要求,说明如何实现该策略要求。

中金金融认证中心有限公司(CFCA)版权所有
https://www.cfca.com.cn

证书策略（CP，Certificate Policy）是一个指定的规则集，它指出证书对于具有普遍安全需求的一个特定团体和（或）具体应用类的适用性。本 CP 是 CFCA 依据以下标准规范制定的通用型电子认证服务体系下的技术政策文件。凡是注日期的引用文件，仅注日期的版本适用于本 CP；凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本 CP。主要引用文件如下：

（1）《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》《电子认证服务使用密码管理办法》；

（2）GB/T 26855-2011《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》；

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

（4）GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》。

1.2 文档名称与标识

本文档的名称为《CFCA 电子认证服务证书策略》，本文档对应的识别码 OID（Object Identifier，对象标识符，指 CFCA 在 http://www.china-oid.org.cn 官方网站注册的 OID 号）如下表：

OID	说明
2.16.156.112554.10	本文档标识（CFCA 电子认证服务证书策略（CFCA CP）

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

1.3 电子认证活动参与者

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

1.3.1 电子认证服务机构

电子认证服务机构（Certificate Authority，以下简称“CA”、“CA 机构”）即依法设立的电子认证服务提供者，负责证书签发、更新、撤销等证书生命周期管理，提供证书查询、证书撤销列表（Certificate Revocation List，以下简称“CRL”）发布以及密钥管理等服务。本 CP 电子认证服务机构仅指 CFCA，有关 CFCA 产品及服务的详细信息，请访问官网 https://www.cfca.com.cn 查阅。

1.3.2 注册机构

注册机构（Registration Authority，以下简称“RA”、“RA 机构”）是受理数字证书的申请、更新、恢复和撤销申请的实体，同时也是标识和鉴别主体身份的实体。

CFCA 在履行 CA 机构职责角色的同时，若直接受理订户证书申请，也履行 RA 机构职责。当 CFCA 履行 RA 机构职责时，在本 CP 中也称为 RA 机构。CFCA 可授权其他机构为 RA 机构。被授权的 RA 机构应与 CFCA 签署数字证书合作协议，并按照协议内容及本 CP 中关于 RA 机构的职责要求，依据 CFCA《注册机构运营规范》，在协议约定的授权范围内，

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

以 CFCA 注册机构的名义开展证书注册业务，不得将相关业务再次委托给其他机构或个人。CFCA 对 RA 机构开展证书注册业务的行为进行监督，并对该行为的后果承担法律责任。

1.3.3 订户

订户是指向电子认证服务机构申请证书的实体。

1.3.4 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实体。

1.3.5 其他参与者

其他参与者是指除 CA、RA、订户和依赖方以外的电子认证服务相关的参与者。

1.4 证书应用

1.4.1 适合的证书应用

本 CP 下的证书适用于网络场景确认参与方身份，保障数据完整性，防止数据被篡改；提供过程防抵赖性，防止参与方事后否认其行为；同时支持对网络传输信息进行加密，确保信息的安全性。

本 CP 下的证书类型可从不同维度进行分类，各维度分类可互相

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

交叉，如个人证书，可以存在个人普通证书、个人高级证书、个人复合证书、个人预植证书、个人密钥分散型证书等。本版本涉及的证书类型详见下表:

分类维度	证书类型	适用场景描述
证书主体	个人证书	用于在网络环境下标识个人身份，代表个人对电子信息进行电子签名，利用数字签名防止个人交易信息被篡改，利用数字加密技术保证个人交易信息的保密性。
	机构证书	用于在网络环境下标识机构身份，代表机构对电子信息进行电子签名，利用数字签名防止机构交易信息被篡改，利用数字加密技术保证机构交易信息的保密性。
	设备证书	用于在网络环境下标识设备，在通信过程中，对通信数据进行电子签名，确保交易信息的完整性，同时可用于通信过程中密钥加密、数据加密、密钥协商等。
证书密钥用途及证书数量	普通证书	单证书，指签名证书，即证书密钥用途可包含数字签名、防抵赖。
	高级证书	双证书，指一次签发两张证书，一张签名证书，一张加密证书。签名证书密钥用途可包含数字签名、防抵赖。加密证书密钥用途包含密钥加密、数据加密、密钥协商；加密证书不单独签发，订户申请数字证书时，信息系统无特别要求的情况下，应同时签发签名证书和加密证书。
	复合型证书	多证书，指一次发放多种密码算法的证书。证书用于一些需要兼顾多种密码算法（RSA、SM2）的信息系统应用项目。
证书应用场景	安全邮件证书	用于表明邮件地址拥有者的身份，以及对邮件传输中信息的加解密、签名等操作。
	SSL 网站证书	用于表明网站身份，与浏览器客户建立安全通道，也称作服务器证书，仅受理机构申请。
	VPN 证书	用于鉴别 VPN 设备身份，建立安全通道，确保通信安全，仅受理机构申请。
	代码签名证书	用于机构保护软件等知识产权，标识代码的所有者，确保代码传输、使用过程的完整性。仅受理机构申请。
密钥生成方式	预植证书	CFCA 按照一定规则及安全控制措施，预先在智能密码钥匙中签发的一种证书。订户通常在柜面办理业务时申请证书，注册机构对订户身份鉴别通过后，将订户身份信息与预先生成的证书进行绑定，并将绑定信息发往 CFCA 预植证书服务系统，CFCA 预植证书服务系统收到信息并对注册机构的签名验证通过后，预植证书才能被订户激活。可应用于大额交易等高风险业务。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

	密钥分散证书	基于密钥分散技术，将证书密钥分散存储于多个设备或环境中。面向移动互联网或云服务等特定业务场景，适用于通过终端设备处理重大事项、大额交易等高风险事项。
	软存储证书	证书密钥由获得商用密码产品认证证书的软件产品产生，适用于风险低的业务场景，比如发送安全邮件等。
	硬存储证书	证书密钥由获得商用密码产品认证证书的硬件产品产生，比如智能密码钥匙，适用于大额交易等高风险业务场景。

1.4.2 限制的证书应用

本 CP 下的各类证书，应在证书策略标识范围内使用，证书应用时应检查是否超范围使用，对超出本 CP 限定的应用范围使用证书，将不受保护。

本 CP 下的证书禁止在如下领域使用：任何违反国家或地方法律法规及行政规章的领域，以及任何未经安全检测的环境和应用。具体包含但不限于如下情形：

（1）《中华人民共和国电子签名法》第三条规定的情形；

（2）CFCA 与 CFCA 授权的 RA 机构或订户约定的证书应用范围之外的情形；

（3）禁止在任何违反国家或地方法律法规、行政规章或破坏国家安全的情形下使用，否则由此造成的法律后果由订户自行承担。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

1.5 策略管理

1.5.1 策略文档管理机构

本CP的管理机构是“中金金融认证中心有限公司电子认证业务策略管理委员会”（以下简称“策略管理委员会”），由策略管理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、发布本CP。

1.5.2 联系方式

本CP的策略机构联系方式如下：（以官网更新为准）

组织名称	中金金融认证中心有限公司
客服机构	客服电话：400-880-9888
	投诉电话：010-80864105、010-80864106
	邮箱：cps@cfca.com.cn
地址	北京市西城区金融大街37号百盛北楼8层
	北京市西城区菜市口南大街平原里20-3
网址	https://www.cfca.com.cn

1.5.3 决定CP符合策略的机构

电子认证服务相关的法律法规、管理制度、标准规范以及CFCA的业务流程、系统环境等发生变化而需要修改本CP的，应由策略管理委员会审核决定。审核过程同本CP第1.5.4章节。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

1.5.4 CP 批准程序

本 CP 的管理机构是策略管理委员会，负责制定、评审、发布、更新、废止本 CP。策略管理委员会编写小组制定、修订 CP 初稿；CP 初稿由策略管理委员会专家组进行专家评审，形成评审稿；评审稿由公司法务进行法审，形成法审稿；经由 CFCA 总经理办公会批准后向外公布。自发布之日起三十日内向中华人民共和国工业和信息化部报备。

1.6 定义和缩写

下列定义适用于本 CP。

序号	项目	定义
1	数字证书	也称作公钥证书，由证书认证机构（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。[1]
2	电子签名认证证书	即签名证书，是指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。[2]
3	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。[3]
4	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（3.17）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。[4]
5	证书策略	一个指定的规则集，它指出证书对于具有普遍安全需求的一个特定团体和（或）具体应用类的适用性。[5]

[1] GB/T 25056-2018 3.9
[2] 参考《中华人民共和国电子签名法》第三十四条（三）
[3] GB/T 25056-2018 3.4
[4] GB/T 27913-2022 3.42
[5] GB/T 25069-2022 3.780 及 GB/T 25056-2018 3.3

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6	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。
7	密钥	控制密码变换操作的符号序列。[6]
8	签名密钥	非对称算法中专用于数字签名及验证数字签名有效性的一对密钥。
9	加密密钥	非对称算法中专用于数据加解密、密钥协商、密钥加密的一对密钥。
10	私钥	非对称密码算法中只能由拥有者控制、使用的不公开密钥。
11	签名私钥	指执行数字签名时，只能由签名人控制使用的非对称密码算法中不公开的密钥。
12	加密私钥	指执行数据加密时，只能由加密人控制使用的非对称密码算法中不公开的密钥。
13	公钥	非对称密码算法中可以公开的密钥。
14	甄别名	在数字证书的主体名称域中，用于唯一标识证书主体的 X.500 名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。
15	实体	包括法律实体（如政府机关、企事业单位、其他组织及个人）和技术实体（如服务器、网络节点、自动化系统）等具有法律认可或技术可识别的独立存在形式，能够以自身名义行使权利、履行义务或执行特定功能的主体。
16	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。[7]
17	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。[8]

[6] GB/T 25069-2022 3.389
[7] GB/T 25069-2022 3.576
[8] GB/T 25069-2022 3.119

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

18	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。[9]
19	电子签章	使用电子印章签署电子文件的过程。[10]
20	撤销	因错误签发、密钥泄露、不再使用等原因停止使用证书。本文的撤销仅对撤销后的结果负责。历史版本中的吊销、注销与本文中的撤销意思一致。
21	证书主体	证书中的“主体”项指明的、持有与证书中载明公钥相对应之私钥的实体。注：证书主体可以是订户自己，也可以是订户全权控制的设备、账号、域名、IP 地址等。当订户是法人机构时，证书主体还可以是该法人机构下下属机构、下属职员、签约人和设备等。[11]
22	身份核验	重点在于证明“自己就是自己”，是对身份信息的真实性和一致性进行验证。例如云平台的身份证核验服务，通过调用权威机关提供的身份证信息，对用户上传的身份证号、姓名和头像进行核验，确认其是否一致，以此证明用户身份的真实性。
23	身份鉴别	主要是用来回答“自己是谁”的问题。就像在网络登录中输入用户名，是表明自己身份的一个标识动作。可结合生物特征（人脸、指纹）和所拥有物品（UKEY、手机）等来进行身份鉴别。
24	独立合约人	非电子认证服务机构（CA）内部的工作人员，但从事 CA 有关业务的独立签约人员。
25	CA 证书	由 CA 机构自身签发的数字证书，包含了 CA 的公钥、CA 机构名称（DN）、有效期等以及 CA 对自身信息的数字签名。
26	主体	身份能够被鉴别的、具有法律意义的实体。

下列缩写适用于本 CP。

序号	项目	缩写定义
1	CA	电子认证服务机构（Certificate Authority）

[9] GB/T 25069-2022 3.121
[10] GB/T 25069-2022 3.120
[11] GB/T 31508-2015 3.6

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

2	RA	注册机构（Registration Authority）
3	KM	密钥管理（Key Management）
4	CRL	证书撤销列表（Certificate Revocation List）
5	OCSP	在线证书状态协议（Online Certificate Status Protocol）
6	CP	证书策略（Certificate Policy）
7	CPS	电子认证业务规则（Certificate Practice Statement）
8	CSR	证书签名请求（Certificate Signature Request）
9	DN	甄别名（Distinguished Name）
10	PKI	公钥基础设施（Public Key Infrastructure）
11	OID	对象标识符（Object Identifier）
12	URL	统一资源定位符（Uniform Resource Locator）

2 发布与信息库责任

2.1 信息库

CFCA 的信息库包括但不限于：CP、CPS 的最新版本及历史版本，《CFCA 电子认证服务协议》、相关的技术支持信息，证书链、证书、证书撤销列表、证书状态信息等。

2.2 认证信息的发布

CFCA 的 CP、CPS 经总经理办公会批准后发布，其他信息的发布按照官方网站管理制度的批准程序进行发布。CFCA 将在其官方网站 https://www.cfca.com.cn 上公布信息库。CFCA 的信息库将按照公司的相关管理措施，确保提供信息库的准确性、完整性及可用性。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

本 CP 中引用的属于公司内部管理制度及相关控制规则的，不在信息库中发布。订户如需获取，可通过本 CP 第 1.5.2 章节公布的联系方式获取。

2.3 发布的时间或频率

本 CP 在完成第 1.5.4 章节所述的批准流程后的三十个工作日内发布到 CFCA 官方网站上，并可确保 7*24 小时可访问。CRL 的发布频率参见本 CP 第 4.9.7 章节（CRL 发布频率）。

2.4 信息库访问控制

CFCA 采取适当的安全措施，防止信息被篡改或破坏，并仅授权指定人员对信息库进行更新。用户可通过 CFCA 官方网站访问相关信息库。

3 标识与鉴别

3.1 命名

3.1.1 名称类型

CA 机构签发的数字证书使用 X.500 甄别名称。

3.1.2 对名称意义化的要求

证书 DN（Distinguished Name,甄别名）是数字证书主体名称域

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

中用于唯一标识证书主体的 X.500 名称。除 CFCA 预植证书外，该字段反映证书主体真实身份、具有实际意义且不违反法律法规的内容。具体甄别名规则见《CFCA 数字证书数据构成规则》最新版本。

3.1.3 订户的匿名或伪名

使用匿名的订户提交的证书申请材料不符合CA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。

3.1.4 解释不同名称形式的规则

证书主体的名称依据 X.500 甄别名命名规则解释，具体甄别名规则见《CFCA 数字证书数据构成规则》最新版本。

3.1.5 名称唯一性

CA 机构签发给某个实体的数字证书，其主体甄别名（DN）在签发数字证书的 CA 系统内必须唯一标识该主体。同一实体持有的多张证书，需通过证书序列号等唯一标识进行区别。

3.1.6 商标的识别、鉴别和角色

订户不应在其证书申请中使用侵害他人知识产权（如商标权、著作权、专利权等）的名称，CA 机构不承担对订户是否涉及商标纠纷等知识产权争议的实质审查法律责任。若发生此类争议，CA 机构有权拒

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

绝证书申请或撤销已发放的证书。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户申请证书时，可用其私钥对申请信息进行签名，CA 机构收到证书申请，验证申请文件里的签名，以确定订户拥有私钥。

3.2.2 订户身份的鉴别

对于个人订户，订户或其授权代表应仔细阅读 CFCA 数字证书相关条款，并同意承担相应的责任。RA 机构受理申请后，将严格核验订户提交的个人身份证明文件、证书申请文件和申请信息等申请材料，核实个人订户身份的真实性并确认其意愿。

对于机构订户，订户或其授权代表应仔细阅读 CFCA 数字证书相关条款，并同意承担相应的责任。RA 机构受理申请后，将严格核验订户提交的机构身份证明文件、机构授予经办人的授权证明和经办人的个人身份证明文件等申请材料，核实机构订户是合法存在的实体并确认其意愿。

订户申请设备证书，可向 RA 机构提交申请。RA 机构会根据申请的证书类型对订户进行身份鉴别。当域名等信息被作为证书主题内容申请证书时，还需要合理验证该订户是否拥有该权利。

RA 机构对申请材料及核验记录进行存档管理。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

3.2.3 没有验证的订户信息

CA 机构不对订户在申请过程中提供的机构所属的非法人分支机构及机构部门信息进行核实。对于未列入核实范围的信息，CA 机构不对其真实性作出承诺，亦不承担由此产生的法律责任。

3.2.4 授权确认

当订户授权第三方代理申请证书时，CA 机构除应对被授权人进行身份鉴别外，还应对授权人进行身份核验。核验方式包括查验授权文书、电话确认、发送短信或电子邮件等方式。

3.2.5 互操作准则

CFCA 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社会公众应用根证书（SM2）为 CFCA 的 CFCA CS SM2 CA 成功签发 CA 证书，这使得 CFCA 与国家根之间成功构建起信任链。

3.3 密钥更新请求的标识与鉴别

密钥更新是指订户证书 DN 信息不变、生成新证书密钥，为订户重新签发一张新证书。密钥更新分证书补发和证书换发两种（定义参考本 CP 第 4 章节）。

3.3.1 常规密钥更新的标识与鉴别

常规密钥更新的标识和鉴别机制支持线上和线下两种方式。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

线上方式。如证书未失效且证书当前还能使用的情况下，订户通过在线系统证书自助申请补发和证书换发时，在线系统可通过验证订户原证书的有效性来鉴别订户身份；如证书已失效且证书存放在智能密码钥匙里的情况下，订户通过在线系统自助申请证书换发时，因其签名需要用户输入智能密码钥匙里的口令，可不对申请的签名数据有效性进行验证，仅验证是否为订户原证书私钥进行的签名即可；其他情况下，订户通过在线系统自助申请证书补发和证书换发操作，系统可通过向订户初次注册时预留的手机号、邮箱发送验证码或人脸识别等方式来鉴别订户身份。其他市面上符合监管要求的且能确保是订户本人参与的身份鉴别方式，同样适用于本 CP。

线下方式，若订户选择临柜申请更新密钥，其身份鉴别方式可参考本 CP 3.2.2 的规定。

3.3.2 撤销后的密钥更新的标识与鉴别

证书撤销后，必须重新以本 CP 第 3.2 章节规定的方式进行身份鉴别，重新申请一张证书。

3.4 撤销请求的标识与鉴别

订户提出撤销请求，CA 机构或者 RA 机构应对该订户身份进行鉴别，鉴别同本 CP 第 3.2 章节的规定；如订户违反相关规则，CA 机构或者 RA 机构按规则执行撤销时，可不经过鉴别程序。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

具有民事行为能力的自然人、依法成立的法人或其他组织，可申请数字证书；申请须由订户或其授权人提交。非订户代表组织机构批量证书申请的，应取得该组织机构的书面授权。

4.1.2 注册过程与责任

1、订户或其授权代表可通过 RA 机构提出证书申请，通过安全渠道提交真实有效的身份证明文件、证书申请材料及相关信息；订户或其授权代表应仔细阅读 CFCA 数字证书相关条款，并同意承担相应的责任。

2、RA 机构应向订户明确告知以下事项：

（1）申请人的权利和义务；

（2）数字证书和电子签名的使用条件；

（3）服务收费的项目和标准；

（4）保存和使用证书持有人信息的权限和责任；

（5）电子认证服务机构的责任范围；

（6）证书持有人的责任范围；

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

（7）其他需要事先告知的事项。

3、RA 机构收到申请后，依据本 CP 第 3.2 章节的规定对订户及申请资料进行审核。审核通过的，在系统中注册订户的信息；审核未通过的，需向订户说明未通过的原因。

4、订户信息注册完成后，若 RA 机构为订户提供智能密码钥匙，则可以使用智能密码钥匙为订户产生证书签名密钥对，向 CA 提交证书申请。CA 机构验证 RA 机构权限及证书申请格式，审核通过后签发数字证书，并将证书发送给 RA 机构，由 RA 机构将证书转交给订户。

订户信息注册完成后，若 RA 机构向订户提供预植证书，则通过 RA 机构的预植前置系统，将订户信息与预植证书绑定，将绑定后的信息在预植前置系统签名后发送给 CFCA 的预植服务系统。RA 机构在预植证书未交付给订户之前，应安全保管预植证书。

订户信息注册完成后，若订户自行下载证书，则 RA 机构向 CA 机构提交证书申请，获得证书下载凭证，RA 机构将证书下载凭证以安全方式（密码信封或者安全邮件等）反馈给订户。订户自行在安全环境下产生签名密钥对，利用下载凭证，通过 CFCA 证书下载平台下载证书。

RA 机构如在其业务系统中代替订户产生证书密钥、使用订户证书的，应与订户签署授权委托协议。

5、RA 机构应协助订户与 CA 机构签订《CFCA 电子认证服务协议》;

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

若 RA 机构向订户提供智能密码钥匙，应提示订户修改智能密码钥匙的初始口令。RA 机构应妥善保管订户的证书申请资料及身份核验记录，当 CA 机构需要这些资料时，RA 机构应根据 CA 机构要求，向 CA 机构提交相关的订户身份核验记录。

6、订户应与 CA 机构签署《CFCA 电子认证服务协议》，该协议可采用纸质签署、线上签署或其他符合法律规定的形式进行签署，不同形式的协议文本具有同等法律效力；如数字证书保存在智能密码钥匙中，订户应在申领到智能密码钥匙后，主动修改初始密码，并妥善保管；订户应妥善保管数字证书，并合法合规使用数字证书。

CA 机构数字证书注册过程须符合 GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 12 章证书操作流程的规定。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

RA 机构处理证书申请按照本 CP 第 3.2 章节要求，对证书申请进行鉴别。

4.2.2 证书申请批准和拒绝

RA 机构完成本 CP 第 4.2.1 章节的规定后，视为批准证书申请，如未完成应拒绝，并告知拒绝理由。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.2.3 处理证书申请的时间

RA 机构和 CA 机构处理证书请求的最长响应时间不超过两个工作日。如有特殊情况，可适当延长证书处理时间。

4.3 证书签发

4.3.1 证书签发中电子认证服务机构的行为

在执行完本 CP 第 3.2 章节的流程后，RA 机构与 CA 机构在建立安全通道的基础上，CA 机构接收 RA 机构的证书申请请求，对 RA 机构的权限、数据格式、RA 机构的签名等进行验证，验证通过后，CA 机构按照 GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 12 章证书操作流程签发数字证书，按照信息库发布规则发布信息。

对于预植证书，CA 机构按照事先设定的规则，在安全控制环境下，由智能密码钥匙产生证书密钥对，并按照预植证书规则签发数字证书；签发的预植证书，经检验合格后，通过安全途径交付给 RA 机构。由 RA 机构对订户身份核验完成后，将核验后的订户身份通过安全通道反馈给 CA 机构，预植证书激活成功。预植证书的激活意味着 CA 机构正式批准了证书申请。

4.3.2 电子认证服务机构对订户的通告

无论是拒绝还是批准订户的证书申请，RA 机构应当通过电话、短

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

信、电子邮件、线上系统提示等方式中的一种，告知订户申请结果。

4.4 证书接受

4.4.1 构成接受证书的行为

订户在收到证书后，应仔细核对证书内容与申请信息是否一致，确认无误后方可启用。本 CP 认可以下接受证书行为：订户自接收到证书起，或订户在收到证书签发成功的系统提示、短信、邮件等提示信息后，24 小时内无异议的，视为已确认证书无误并接受证书；证书一经使用，即视为订户已接受该证书。预植证书一旦绑定并激活，即视为订户已接受该证书。

若订户对证书持有异议或拒绝接受时，RA 机构应协助其撤销证书或重新签发证书。

订户一经接受证书，即视为已与 CA 机构签署《CFCA 电子认证服务协议》。

4.4.2 电子认证服务机构对证书的发布

证书签发完成后，CA 机构将证书发布至信息库。

4.4.3 电子认证服务机构对其他实体的通告

CA 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。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在完成证书申请并接受 CA 机构签发的证书后，即视为同意遵守与 CA 机构及依赖方之间的权利义务条款。订户在使用证书时，应遵循本 CP 第 1.4.1 章节所规定的用途，并履行以下与私钥及证书使用相关的义务:

（1）妥善保存其私钥，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私钥及证书;

（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）使用证书执行交易信息签名、加密时，订户应确定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）订户委托第三方保管或使用私钥及证书时，订户仍为法定责任主体，应对受托方的全部操作行为承担连带责任，须定期核实授权范围及使用记录。

（7）预植证书必须在绑定激活后方可使用，且仅用于绑定的应用。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.5.2 依赖方对公钥和证书的使用

依赖方信赖 CA 机构签发的证书所证明的信任关系时应执行以下步骤:

（1）从 CA 机构官方途径获取并安装 CA 机构的证书链;

（2）通过安全途径获取订户公钥证书;

（3）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 CRL 或 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;

（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;

（5）确认该公钥证书上的信息是自己交易的对象，使用该公钥证书加密信息。

若以上任一步骤失败，依赖方应拒绝接受该签名信息。

当依赖方需向接收方发送加密信息时，应首先通过安全通道获取接收方的加密证书，并使用该证书中的公钥对信息进行加密。

4.6 证书更新

证书更新即证书延期（renewal），是指在订户证书 DN 信息不变、

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

保持证书密钥不变的情况下，为订户重新签发一张新证书。CA 机构不直接提供该项服务。

4.7 证书密钥更新

证书密钥更新是指订户证书 DN 信息不变、生成新证书密钥，为订户重新签发一张新证书。

4.7.1 证书密钥更新的情形

证书密钥更新主要包含以下两种情形:

证书补发是指在证书有效期内，因订户证书密钥损坏或泄露、订户证实或怀疑其证书密钥存在安全隐患或其他需进行证书密钥更新等情况，为订户进行证书密钥更新操作。证书补发时，CA 系统撤销原证书，同时为订户签发一张新证书。新证书的到期日与旧证书一致。

证书换发是指证书即将失效（到期日前三个月内）或已失效的情况下，为订户进行证书密钥更新操作。若在证书有效期内申请换发，CA 系统应先撤销原证书，同时为订户签发一张新证书。新证书的有效期自换发申请之日起计算。若原证书仍在有效期内，其到期日为原证书到期日基础上顺延一个完整有效期周期；若原证书已失效，则系统将直接签发新证书，新证书的到期日为其生效日期基础上顺延一个原证书的有效期周期。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.7.2 请求证书密钥更新的实体

已经申请过证书的订户可申请证书密钥更新。

4.7.3 证书密钥更新请求的处理

同本 CP 第 3.3 章节。

4.7.4 颁发更新证书时对订户的通告

同本 CP 第 4.3.2 章节的规定。

4.7.5 构成接受密钥更新证书的行为

同本 CP 第 4.4.1 章节的规定。

4.7.6 电子认证服务机构对密钥更新证书的发布

同本 CP 第 4.4.2 章节的规定。

4.7.7 电子认证服务机构对其他实体的通告

同本 CP 第 4.4.3 章节的规定。

4.8 证书变更

证书变更是指订户证书 DN 信息发生变化、保持证书密钥不变的情况下，为订户重新签发一张新证书。CA 机构不直接提供该项服务。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.9 证书撤销和冻结

4.9.1 证书撤销的情形

如有下列情形中的任何一种情形发生，订户可主动发起证书撤销申请:

（1）订户决定不再使用证书，并书面申请撤销数字证书;

（2）订户提供证明，确认证书申请未获得有效授权;

（3）订户怀疑密钥不安全，或存放证书的介质无法正常使用等;

（4）订户证书主体信息发生重大变更，需要撤销证书。

如有下列情形中的任何一种情形发生，订户证书将会被动地撤销:

（1）订户证书被使用于违反法律强制性规定的事项上;

（2）订户证书被超范围使用;

（3）订户未履行本 CP 或其与 CA 机构签署的服务协议中所约定的义务;

（4）订户已失去证书主体信息（如域名、IP）所有权或控制权;

（5）SSL 网站证书被用于验证一个欺诈性或极具误导的域名;

（6）订户申请证书时，提供的资料不真实、不完整、不准确;

（7）订户证书中所显示的信息不准确或具有误导性;

（8）订户未能满足证书策略中的要求和条件;

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

（9）CA 机构停止业务且没有安排其他 CA 机构承接业务;

（10）在 CA 机构的电子认证服务资质被撤销且无其他 CA 机构承接业务的情况下，CA 机构将撤销所有已签发的证书，并仅保留 CRL 和 OCSP 服务的运行。

（11）CA 机构的 CA 签名证书私钥被泄露时，根据签名私钥泄漏紧急预案撤销所有已签发的证书;

（12）订户证书签发错误;

（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）仅限于某 RA 机构应用范围内使用的证书，如该 RA 机构申请停用该证书，可向 CA 机构提出撤销申请;

（15）法律、行政法规规定的其他情形。

4.9.2 请求证书撤销的主体

（1）主动撤销

已申请 CA 机构证书的订户可主动提出证书撤销申请。

（2）被动撤销

RA 机构可提出证书撤销申请。

依赖方或其他参与者如发现证书问题，可向 CA 机构提出撤销申

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

请，并说明合理的撤销理由。

CA 机构可在本 CP 第 4.9.1 章节所述的情形下撤销订户的证书。

4.9.3 请求撤销的流程

（1）主动撤销

订户申请撤销证书时，可按照申请证书时的流程，向 RA 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。

RA 机构在收到订户提交的撤销申请材料后，应按照订户申请证书的核验方式，对其身份及撤销申请信息进行核验，审核通过后向 CA 机构发起证书撤销请求。

CA 机构收到撤销请求后，需验证发起请求的 RA 机构权限及撤销请求数据格式，确认无误后执行证书撤销操作，并将撤销结果反馈至 RA 机构。在证书撤销后，按照 CRL 发布策略更新 CRL，并同步更新 OCSP 状态。

RA 机构收到证书撤销结果后，反馈给订户撤销结果。

（2）被动撤销

当 RA 机构判断存在本 CP 第 4.9.1 章节所述可能导致订户证书被动撤销的情形时，可向 CA 机构提交证书撤销申请，CA 机构将依据内部控制流程处理该撤销申请。对于被动撤销的证书，CA 机构将通过适

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

当的方式通知订户；在证书撤销后，CA 机构将按照 CRL 发布策略发布 CRL，更新 OCSP 状态。若 RA 机构需批量撤销证书，应提交批量撤销证书申请材料，经 CA 机构审核通过后，由 CA 机构执行撤销操作。

依赖方或其他相关方如发现证书问题，可向 CA 机构提出撤销申请，并说明合理的撤销理由。CA 机构将对情况进行调查核实，并根据调查结果决定是否撤销证书或采取其他适当的处理措施。

4.9.4 撤销请求宽限期

若订户怀疑其证书密钥存在安全隐患，订户应在知晓该安全隐患的 24 小时内，向 RA 机构或者 CA 机构提交证书撤销申请。CA 机构可根据订户申请延长撤销请求时间至 48 小时。

4.9.5 电子认证服务机构处理撤销请求的时限

订户申请撤销证书，CA 机构应在收到请求后，24 小时内处理该请求。

若 CA 机构收到关于证书签发错误的报告，应在 24 小时内启动调查程序，并在调查处理完成后向报告人反馈结果。

4.9.6 依赖方检查证书撤销的要求

依赖方应根据自身的风险承受能力、责任范围及可能产生的影响，自行判断并确定检查证书撤销信息的时间间隔。依赖方在信赖证书前，应验证其有效性，确保证书未被撤销。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.9.7 CRL 发布频率

CRL 的发布频率应每 24 小时至少一次。

4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大滞后时间为 24 小时。

4.9.9 在线证书状态查询的可用性

CA 机构提供 7*24 小时不间断的 OCSP 服务。

4.9.10 撤销信息的其他发布形式

订户可通过 CA 机构官方网站上提供的证书查询服务下载 CRL。CA 机构也可单独发布来自该 RA 机构申请证书的 CRL。

4.9.11 对密钥遭受安全威胁的特别处理要求

订户、RA 机构发现其密钥遭受安全威胁时，应于 24 小时内提出证书撤销请求。

CA 机构的签名密钥遭受威胁时，按照签名私钥泄露应急预案处理。

4.9.12 证书冻结及解冻

证书冻结即订户证书面临威胁时请求将证书置为冻结状态，待威胁消失后，将证书恢复为可用状态，即取消冻结状态（解冻）。

证书处于冻结状态的最长时限为证书的有效期。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

4.10 证书状态服务

4.10.1 操作特征

证书状态服务按照本 CP 第 4.9.9 章节和第 4.9.10 章节的规定提供，CA 机构根据需要，在证书失效后将其从 CRL 中移除。

4.10.2 服务可用性

CA 机构应确保具备充足的资源，用于 CRL 及可选的 OCSP 服务的运行和维护，提供 7×24 小时可用的在线信息库，支持通过应用软件查询并验证其所签发且未失效证书的当前状态。

4.11 服务终止

以下两种情形将被视为服务终止:

（1）证书到期后不续订即视为服务终止;

（2）证书撤销即视为服务终止。

4.12 密钥托管与恢复

CA 机构自身密钥不托管给第三方。CA 机构仅按照相关规则为订户提供加密密钥托管与恢复服务。

密钥恢复包含两种类型: 订户密钥恢复和司法密钥恢复。订户或司法机构根据实际情况可向 CA 机构申请密钥恢复。经 CA 机构审核后，

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

可恢复密钥并存储于特定载体中。

4.13 证书归档

本 CP 中，证书失效（证书过期或撤销）后 CA 机构对失效证书进行归档，证书及证书归档记录自证书到期日起保留五年。

5 认证机构设施、管理和操作控制

CA 机构依据 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》的要求建设、维护、管理基础设施。

5.1 物理控制

CA 机构的物理安全应符合 GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 8.5 章节的各项要求。

5.2 程序控制

5.2.1 可信角色

CA 机构提供电子认证服务过程中，将能从本质上影响证书生命周期管理的操作人员及影响 CA 密钥安全的管理人员视为可信角色。CA 机构的可信角色至少包含：

（1）系统管理员：仅负责技术运维（如数据库备份与恢复、性能监控、存储管理等），不具备操作业务数据权限（如禁止直接增删改查业务数据），确保运维与业务隔离；

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

（2）安全管理员：负责统一制定安全标记策略与访问控制规则，管理数字证书、密钥策略，监管密钥生命周期（生成、分发、轮换、销毁）；

（3）审计管理员：负责实时监控所有操作日志（包括密钥管理行为），定期生成安全报告；拥有对审计策略的否决权（如拦截未授权操作）；

（4）密钥管理员：负责密钥的物理安全管理、加密算法的实施、紧急密钥的销毁。所有操作需执行双人复核机制，并实时记录于审计日志。

5.2.2 每项任务需要的人数

进出 CA 系统物理环境应实施双人同行准入机制，且进出人员须具备相关权限。所有进出人员需通过双因子识别机制进行控制，且应保留进出的记录，以供审计。

CA 系统的所有操作均应由经过授权的至少 2 个可信角色共同执行，登录系统应采用双因子认证方式，且所有操作应完整记录，保留审计日志以备查证。

访问和管理 CA 的加密设备及其密钥的操作应采取 5 选 3 机制。

5.2.3 每个角色的识别与鉴别

每个角色均应通过指纹（或口令）、智能密码钥匙或者 IC 卡等进行识别与鉴别。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

5.2.4 需要职责分割的角色

以下角色必须进行职责分离:

（1）安全管理员不得与系统管理员、审计管理员兼任;

（2）系统管理员不得与审计管理员兼任。

5.3 人员控制

5.3.1 资格、经历和无过失要求

CA 机构对可信角色人员实施严格背景审查,聘用人员应具备岗位所需能力及无不良从业记录。

5.3.2 背景审查程序

CA 机构制定背景调查操作规程，以满足本 CP 第 5.3.1 章节的要求。

5.3.3 培训要求

CA 机构应对从事电子认证服务的人员按照其岗位和角色安排培训。培训内容包括: PKI 的相关知识、CP、CPS、岗位职责、内部规章制度、认证系统软件、相关应用软件、操作系统与网络、信息安全、数据安全、个人信息保护等。CA 机构应制定电子认证服务使用密码安全教育培训计划，每年组织开展电子认证服务使用密码安全知识和岗位操作技能培训，相关技术人员和管理人员每年教育培训时间不少于

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

20 个小时。

如授权RA机构进行作业，应对RA机构的作业人员进行相应培训。

5.3.4 再培训周期和要求

当本 CP 第 5.3.3 章节规定的培训内容发生变更时，CA 机构应对相关人员进行培训（含 RA 机构人员），并在其 CPS 中说明教育培训计划与频率。

5.3.5 未授权行为的处罚

CA 机构具备针对未经授权行为的处罚措施。

5.3.6 独立合约人的要求

CA 机构在聘用独立合约人时，将要求其提供有效的身份证明、学历证书、资格证书等有效证明材料，并与 CFCA 签署保密协议。同时，独立合约人应接受与 CA 机构正式员工同等标准的安全与合规培训。

5.3.7 提供给员工的文档

CA机构向作业人员提供其工作所必需的文档，文档配备符合GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 10.6 章节的要求。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

5.4 审计日志程序

审计日志（Audit Log）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。CA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 审计日志记录事件的类型

无论采用纸质或电子形式的审计日志，应至少包含以下要素：

（1）条目的日期和时间；

（2）条目的序列号或顺序号（对于自动日志条目）；

（3）条目种类；

（4）条目来源（如终端、端口、地点、客户等）；

（5）生成日志条目的实体身份。

事件记录类型：

（1）CA密钥生命周期管理事件，涵盖密钥生成、备份、恢复、归档和销毁等全周期操作记录；

（2）RA、CA及KM系统应记录与证书生命周期操作相关的信息，

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

包括但不限于证书申请、密钥更新、证书撤销等事件;

（3）系统、网络安全日志记录;

（4）操作系统、CA 系统、数据库系统运行日志及配置操作日志;

（5）操作审批记录;

（6）人员访问控制记录、监控记录。

5.4.2 处理审计日志的周期

CA 机构应建立审计日志核查机制，确保日志记录的完整性，并对核查过程中发现的任何异常或警告进行深入调查。核查过程及结果须完整存档。

5.4.3 审计日志的保存期限

本 CP 第 5.4.1 章节中的事件记录类型（1），审计日志保存至关联 CA 密钥失效后五年；事件记录类型（2），审计日志至少保存至对应证书失效后五年；其他事件记录类型，审计日志至少保存一年（即一个评估周期）。

5.4.4 审计日志的保护

CA 机构应建立完善的管理制度，采用物理与逻辑控制措施，确保仅授权人员可对审计日志进行操作。审计日志应处于严格保护之下，严禁未经授权的访问或操作。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

5.4.5 审计日志备份程序

CA 机构制定日志备份程序，且关键审计日志应至少有一份异地备份，备份周期应按照法律法规要求及风险评估情况确定。

5.4.6 审计日志收集系统

日志收集可以是系统自动收集，也可以是人工按照规则收集。审计日志收集应尽可能保证所收集数据的完整性和可用性。

5.4.7 对导致事件主体的通告

当出现的事件被审计系统记录时，无需通知产生该事件的相关人员。当出现异常事件记录时，CFCA 在其 CPS 中说明通告规范。

5.4.8 脆弱性评估

CA 机构有定期脆弱性评估机制。

5.5 记录归档

5.5.1 归档记录的类型

CA 机构归档记录至少涵盖以下核心类型:

（1）CA 机构接收外部评审的资料，包括系统测评、信息安全管理体系等外部评审资料;

（2）CA 机构的 CPS、CP 及历史版本;

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

（3）与 CA 机构运营相关的合同;

（4）系统环境建设与配置相关文档;

（5）系统变更记录、故障记录、事件报告等;

（6）证书申请、签发、撤销档案;

（7）CA 密钥产生、备份、恢复、销毁、更换等相关记录;

（8）审计资料档案;

（9）可信人员档案;

（10）证书验证相关档案。

5.5.2 归档记录的保存期限

CA 机构应将与证书相关的归档记录并至少保留至证书失效后五年。

其他归档记录的保存期限，CA 机构在其 CPS 中规范。

5.5.3 归档文件的保护

归档记录应有完整性保护措施，且未经授权人员不得访问。

5.5.4 归档文件的备份程序

归档文件的备份程序，CA 机构在其 CPS 中规范。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

5.5.5 记录的时间戳要求

归档的记录都需要标注时间；系统产生的记录按照要求添加时间戳。

5.5.6 归档收集系统

归档收集系统应满足本 CP 第 5.4.1 章节的要求。

5.5.7 获得和检验归档信息的程序

仅被授权的可信人员可获得归档信息，应每年开展不少于一次的归档信息抽查检验，确保归档信息的完整性与有效性。

5.6 电子认证服务机构密钥更替

为降低 CA 密钥遭破解的风险，CA 机构定期更换密钥，已更换的密钥不得再次使用。

CA 机构在选择密钥有效期时，将考虑密钥长度、算法安全性、控制方式、政策要求等因素。

5.7 损坏与灾难恢复

5.7.1 事故和损害处理程序

CA 机构根据故障类型与级别实施差异化处理和报告。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

5.7.2 计算资源、软件或数据的损坏

当计算资源、软件或数据遭受破坏时，应立即启动恢复服务流程以保障业务连续性。

5.7.3 实体私钥损害处理程序

CA 机构私钥损害处理程序按照《签名私钥泄露紧急预案》处理。

5.7.4 灾难后的业务连续性能力

CA 机构制定业务连续性计划，保证在灾难发生后按照预定计划执行恢复。CA 机构至少每年应急演练一次，确保业务连续性计划的可执行。

5.8 电子认证服务机构或注册机构的终止

RA 机构终止服务应当依据其与 CA 机构所签署协议的约定履行相关程序。CA 机构终止服务时应严格遵守《中华人民共和国电子签名法》及监管部门的规定。

5.9 预植证书的生产管理规程

预植证书的生产管理规程，CA 机构在其 CPS 中规范。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6 认证系统技术安全控制

CA 机构按照 GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 8.2.4 章节的要求对密钥对的产生、使用、备份、恢复等进行安全控制，并在其 CPS 中说明具体控制措施。

CA 机构的 CA 系统产生密钥的设备至少应达到 GB/T 37092-2018《密码模块安全要求》中的二级要求。其密钥用法应符合 GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》附录中的要求。

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

CA 密钥对应在 CA 机构屏蔽机房的密码设备内部产生；使用的密码设备应具有商用密码产品认证证书；严格按照 CA 机构的密钥管理办法以及安全机制执行，确保密钥的生成安全。

RA 系统密钥对应在安全控制下由 RA 系统内部产生，对应系统证书由 CA 系统签发。

订户密钥对的生成可根据业务需要选择对应的密码设备或密码模块。为保障密钥生成安全，密码设备或密码模块需满足国家密码主管部门的最新要求。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.1.2 私钥传送给订户

CA 机构只为订户提供加密密钥对的生成服务，并通过安全通道传送给订户。加密密钥对传输的安全控制措施在 CPS 中说明。

6.1.3 公钥传送给证书签发机构

订户的公钥和订户信息通过安全通道传递到 CA 系统。订户公钥传送方式在 CPS 中详细说明。

6.1.4 CA 机构公钥传送给依赖方

CA 机构通过完整证书链的分发或信息库的方式提供给依赖方。依赖方可从 CFCA 官方网站（https://www.cfca.com.cn）下载证书链，进而获得 CA 机构的公钥。

6.1.5 密钥的长度

密码算法及长度应符合国家密码管理部门的相关规定。其中，CA 证书密钥算法及长度支持 RSA-4096、RSA-2048 和 SM2-256，订户证书密钥长度支持 RSA-2048 和 SM2-256。

本 CP 下的 CA 系统，应在其 CA 证书生命周期结束时，停止使用 SHA1 密码算法。

6.1.6 公钥参数的生成和质量检查

CA 机构用于产生密钥的设备须具备相应等级的密码认证证书，同

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

时对密钥算法及长度进行检查，并拒绝弱密钥的申请。

6.1.7 密钥使用目的

CA 机构在颁发证书时，应通过 X.509 证书域“Key Usage”密钥用法来设置密钥使用的目的，如数字签名、防抵赖等。

CA 私钥不得用于签发订户证书，订户证书不得用于签发证书。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

密码模块应满足 GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》第 7.2 章节的要求。

6.2.2 私钥多人控制

CA 机构的 CA 私钥满足 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》中关于多人控制要求。

6.2.3 私钥托管

CA 机构所有 CA 系统的私钥均安全保存在公司内部，不存在其他地方托管的情形。根据国家密码主管部门要求，CA 机构会提供订户加密证书私钥托管服务，具体将在 CPS 中详细描述。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.2.4 私钥备份

CA 机构的 CA 私钥备份在符合标准要求的硬件设备内，且备份时应与原始产生时一样符合多人控制要求，备份应存放在最安全区。

RA 机构及订户的私钥备份，本 CP 不作规定。

6.2.5 私钥归档

CA 机构归档的 CA 密钥采用与当前使用的密钥同等级别或更高级别的安全控制。当 CA 密钥到达其使用寿命需要销毁时，归档的 CA 密钥同时进行销毁。

CA 机构对订户的加密密钥对归档，至少保存至证书失效后五年。

CA 机构在其 CPS 中写明密钥归档程序。

6.2.6 私钥导入、导出密码模块

CA 私钥应由符合安全要求的硬件设备生成,其导入和导出操作应遵循多人控制策略，执行过程应采用与初始操作同样的操作脚本，并记录操作日志。

6.2.7 私钥在密码模块的存储

CA 私钥应存储在符合本 CP 第 6.1.1 章节要求的密码模块，密码模块应获得商用密码产品认证证书。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.2.8 激活私钥的方法

CA 机构按照设备厂商的说明激活私钥，激活数据（如 PIN，口令或其他形式的密钥）的长度至少应达到 8 位以上。

6.2.9 解除私钥激活状态的方法

CA 机构应确保未经授权人员不得访问已激活的硬件密码模块，并在私钥不再使用时，通过密码模块将其安全销毁。

6.2.10 销毁私钥的方法

当 CA 私钥不再使用，或其对应的 CA 证书已失效时，应对私钥进行销毁。销毁操作应依据预设的操作脚本执行，确保无法通过任何残留信息推断出私钥的任何部分，并应对销毁过程进行完整记录。

6.2.11 密码模块的评估

CA 机构定期关注商用密码产品认证情况，如所使用的密码模块不符合相关政策及安全需要，应及时更新密码模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

CA 机构按照证书归档的方式归档公钥，证书归档见本 CP 第 4.13 章节的规定。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.3.2 证书操作期和密钥对使用期限

证书的有效期应与对应密钥对的有效期保持一致。私钥在有效期结束后不得继续使用，公钥在证书失效后仍可用于验证此前生成的数字签名的有效性。

6.4 激活数据

CA 机构在其 CPS 中说明 CA 密钥的激活数据保护措施,包括产生、存储、销毁等全生命周期的保护。

6.4.1 激活数据的产生和安装

CA 密钥激活数据应在智能密码钥匙或智能 IC 卡上产生，且应采取多人分持的措施，激活数据的产生过程与 CA 密钥的产生过程一样也必须具备操作脚本。

6.4.2 激活数据的保护

用于保护激活数据的口令长度至少应达到 8 位，且不能使用弱口令。激活资料应存放在最安全区，分持人不得随意携带。

6.4.3 激活数据的其他方面

激活数据的分持人应是可信角色。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.5 数据安全控制

CA 机构应制定数据安全方案和计划，定期进行数据安全风险评估，确保数据安全。CA 机构在其 CPS 中写明数据安全控制要求。

6.6 计算机安全控制

6.6.1 特别的计算机安全技术要求

CA 机构提供以下安全控制措施，确保 CA 系统的安全:

（1）操作系统安全可靠;

（2）严格的身份识别和人员访问控制制度;

（3）网络使用异构防火墙防护;

（4）人员职责分割;

（5）任何操作应双人操作控制;

（6）系统登录必须经过双因子认证身份;

（7）所有操作均保留安全审计记录。

6.6.2 计算机安全评估

CA 机构定期对 CA 系统进行安全性评估，每年应进行网络安全等级保护三级测评。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

6.7 CA 系统生命周期技术控制

6.7.1 系统开发控制

CA 机构及 CA 系统的开发管控满足以下要求:

（1）开发过程应提供完整的说明文档;

（2）应对软硬件的采购、使用和变更进行严格控制与检查，防止引入隐蔽通道或恶意代码。CA 系统在首次启用及后续运行中应定期进行恶意代码扫描;

（3）对 CA 系统的开发和维护，应具备相应授权管理机制，确保 CA 系统的完整性。

6.7.2 安全管理控制

CA 机构对 CA 系统的配置、修改或升级，应制定操作控制措施，并记录相关操作。

CA 机构有软硬件设备生命周期的管控规范,软硬件设备接收时须有核查措施。

CA 系统所使用的软硬件设备，不能安装与 CA 系统无关的应用、开放与 CA 系统无关的端口。

6.7.3 生命周期的安全控制

CA 系统安全性贯穿设计与实现的全生命周期,始终作为核心保障

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

目标。CA 机构定期开展 CA 系统全生命周期安全审查，确保安全控制措施符合法律法规要求。

6.8 网络的安全控制

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》的要求进行网络划分和安全防护。

6.9 时间戳

CA 机构涉及 CA 系统相关的系统时间使用国家标准时间源，并保存对有关时间的更改记录以供审计。

CA 机构提供时间戳服务，时间戳请求、应答、格式等符合 GB/T 20520《信息安全技术 公钥基础设施 时间戳规范》的要求。

7 证书、证书撤销列表和在线证书状态协议格式

7.1 证书格式

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。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。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

7.1.1 证书基本项

证书基本项由如下部分组成：版本、序列号、签名算法、颁发者、有效期、主体、主体公钥信息。

7.1.2 版本号

CA 机构签发的证书格式是 X.509 V3 版本。

7.1.3 序列号

证书序列号是 CA 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

证书密码算法标识如下：

算法	OID	附加参数及备注
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	

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

7.1.5 颁发者

CA 机构在本 CP 下所签发证书的主体名称采用 X.500 甄别名的形式。颁发者即 CA 证书的名称形式如下:

属性	值	说明
通用名（CN）	签发证书的 CA 系统名称，如 CFCA ACS OCA31	CA 系统名称
机构（O）	China Financial Certification Authority	CA 公司名称
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，CA 对证书状态的相关信息进行维护。证书的有效期通过起始时间（notBefore）和终止时间（notAfter）表示，时间精度应精确到秒。

CA 证书的有效期最长不超过三十年,订户证书的有效期最长不超过五年零三个月。

7.1.7 主体

主体即订户证书的名称形式如下:

属性	值	说明	示例
C	CN	国家	CN
S	省份	可选	北京
L	城市	可选	北京
O	订户所在机构信息或	必选	CFCA ACS

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

	者 CA 机构标识		OCA31
OU2	证书类型	如 O 为 CA 系统名称，则该项存在，标识证书类型，如个人普通证书（Individual-1）；如 O 为订户所在机构信息，则该项为可选，表示订户所在的部门信息	INDIVIDUAL-1
OU1	RA 机构标识	如 O 为 CA 系统名称，则该项存在，表示 RA 机构简称；如 O 为订户所在机构信息，则该项为可选，表示订户所在的部门信息	信息中心
CN	订户的法定标识	经过脱敏处理的包含个人或机构法定名称和证件号码	张三/xx 公司

7.1.8 主体公钥信息

本项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。

CA 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

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

钥用法、扩展密钥用途、CRL 分发点、主体替换名称(可选设备证书)。

CA 机构设定其私有扩展项时，私有扩展项设置为非关键扩展项。

CA 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

订户证书及 CA 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 CA 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，参考本 CP 第 1.2 章节的规定。该扩展项为非关键扩展项。

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。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

7.1.9.5 基本限制

若是 CA 证书，则基本限制扩展项中 Subject Type 为 CA，且该项必须为关键扩展项；若是订户证书，则基本限制扩展项中 Subject Type 为 End Entity，且该扩展项为非关键扩展项。

7.1.9.6 密钥用法

所有的实体证书包含本扩展项，CA 证书只能包含 KeyCertSign、CRLSign 密钥用法，该扩展项必须为关键扩展项。

对于订户证书，该项为关键扩展项。签名证书的密钥用法包含：数字签名、防抵赖；加密证书的密钥用法包含：密钥加密、数据加密、密钥协商。

7.1.9.7 扩展密钥用法

本扩展项指明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。

7.1.9.8 CRL 分发点

本扩展项描述 CA 系统签发的证书包含的 CRL 分发点，依赖方可根据该扩展项提供的地址和协议下载 CRL。该扩展项为非关键扩展项。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

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，CA 把该实体与认证的公开密钥绑定在一起。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，则可以忽略它，但如果识别出非关键扩展项，则可对其进行处理。

7.2 证书撤销列表格式

CA 机构所签发的证书撤销列表符合 X.509 V2 格式。

7.2.1 版本号

X.509 V2。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

7.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义如下:

（1）版本（Version）显示 CRL 的版本号;

（2）CRL 的签发者（Issuer）指明签发 CRL 的 CA 甄别名;

（3）CRL 发布时间（this Update）;

（4）预计下一个 CRL 更新时间（next Update）;

（5）签名算法;

（6）列出撤销的证书，包括撤销证书的序列号和撤销日期;

（7）CRL 数字（CRL number）。

7.3 在线证书状态协议格式

CA 机构提供在线证书状态查询服务，在正常的网络状态下，确保有足够的资源使 OCSP 服务在合理的时间内向用户反馈查询结果。

CA 机构提供的 OCSP 服务符合 IETF RFC 6960 及 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

IETF RFC 6960 定义的 OCSP V1 版。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

7.3.2 OCSP 扩展项

未使用 OCSP 扩展项。

8 一致性审计和其他评估

8.1 评估者的情形及其频率

CA 机构在如下情形中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，接受主管部门的评估和检查;

（2）CFCA CA 系统每年进行网络安全等级保护三级测评;

（3）CA 机构根据业务发展情况，不定期对 RA 机构进行评估;

（4）当系统发生变更时，变更前后应进行风险评估;

（5）CA 机构按照内部管理制度，定期审计实际业务及各项策略的一致性。

8.2 评估者的资质

CA 机构聘请外部测评机构对 CA 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 CA 机构的运营管理进行合规性审查。CA 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。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

8.3 评估者与被评估者的关系

内部审计人员与负责被审计被评估内容的人员的岗位职责不能重叠。外部测评机构、审计机构与 CA 机构之间应是相互独立的关系，双方无任何足以影响评估客观性的利害关系。

8.4 评估内容

评估的内容包括但不限于以下方面:

（1）CA 机构的物理环境和控制;

（2）密钥管理操作;

（3）基础 CA 控制;

（4）证书生命周期管理;

（5）CA 业务规则。

8.5 对问题与不足采取的措施

CA 机构应对评估报告中的问题进行影响评估，对于能整改的问题，立即整改，由评估者对整改结果进行确认；对于不能立即整改的问题，建立整改台账，按计划进行整改。

8.6 评估结果的传达与发布

如有法律规定或行业主管部门规定，CA 机构将向公众发布行业主管部门对 CA 机构的检查或评估结果。

当 CA 机构对 RA 机构进行抽样审计后，审计结果将只在 CA 机构

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

内部进行传达，并与相关 RA 机构进行沟通。CA 机构对审计存在问题的 RA 机构采取适当风控措施。

其他评估及审计报告不对外发布。

8.7 其他评估

CA 机构对自身的电子认证活动进行抽样审查。CA 机构对 RA 机构的活动进行抽样审查时，RA 机构的选择要充分覆盖各个地域、各个行业以及各种证书应用的场景。

9 法律责任和其他业务条款

9.1 费用

CFCA 有权针对签发、换发、补发、撤销及整个生命周期管理等相关服务收取合理费用。若直接向订户收取费用，应向订户披露费用标准及关联条款、条件。应以明确方式向订户披露。若费用由第三方代为支付，该第三方应就费用相关情况向订户作出明确说明。

9.2 财务责任

CFCA 具备保障其业务持续运营的财务能力，且拥有承担赔偿责任所需要的财力支持。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

9.3 业务信息保密

CFCA 按照相关的法律法规，在 CPS 中披露业务信息保密情况。

9.4 个人信息保护

CFCA 按照相关的法律法规，在 CPS 中披露个人信息保护情况。

9.5 知识产权

本 CP 下的知识产权归 CFCA 所有。

9.6 陈述与保证

9.6.1 电子认证服务机构的陈述与保证

（1）依据本 CP 制定电子认证服务业务规则（CPS）；

（2）公布 CPS，并确保各项操作及提供的服务符合 CPS 所公布的规范；

（3）确保提供的各项服务安全稳定，并保留适当的证明资料；

（4）公布与订户之间的服务协议，并确认其条款符合法律法规、标准规范基本要求；

（5）及时撤销违反订户义务或本 CP 及 CFCA 的 CPS 相关规定的证书；

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

（6）按照规则发布证书撤销列表，并保证订户可查询使用；

（7）提供如本 CP 第 2 章节所列信息库服务。

9.6.2 注册机构的陈述与保证

（1）依据本 CP 及 CFCA 的 CPS，审慎执行订户注册相关操作；

（2）接受订户申请，妥善留存足以核验订户申请信息的相关资料；

（3）在接受订户申请时，严格核验订户身份，并恰当作出注册决定；

（4）严格履行与 CFCA 之间的协议。

9.6.3 订户的陈述、保证及义务

（1）订户向 RA 机构提交申请时，应确保申请资料的真实性、完整性与准确性；

（2）订户须妥善保管其私钥并定期更新密码，订户委托他人保管或使用其私钥时，应当与受托方建立清晰明确的授权关系，并对受托方的行为负责；

（3）订户应充分知悉并同意遵守本 CP、CFCA 的 CPS 和证书使用要求，并在接受后使用数字证书；

（4）若密钥被盗或存在安全隐患，订户应当依据 CFCA 的 CPS 要

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

求及时向 RA 机构提出证书撤销申请;

（5）订户应在约定范围内使用数字证书;

（6）订户的重要信息、资料变更时，应及时通知 CFCA 或原 RA 机构。若因订户提供的资料不真实、不完整、不准确，或者在资料改变后未及时通知 CFCA 或原 RA 机构从而造成的损失由订户自行承担;

（7）因订户原因，导致依赖方或 CFCA 遭受损失的，订户应承担相应的赔偿责任。

9.6.4 依赖方的陈述与保证及义务

依赖方应通过正确途径（例如 CFCA 官网）获取到相应证书链，并在使用时验证证书链及证书的有效性。

9.6.5 其他参与者的陈述与保证

无规定。

9.7 保证免责

CFCA 在 CPS 中说明保证免责情况。

9.8 承担赔偿责任的限制

CFCA 在 CPS 中说明承担赔偿责任的限制。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

9.9 有效期限与终止

9.9.1 有效期限

本 CP 自 CFCA 在其官方网站（https://www.cfca.com.cn）公布的版本中标注的生效日期起生效。

9.9.2 终止

CFCA 有权终止本 CP。本 CP 自 CFCA 在其官方网站公布终止声明的三十日后终止。

自 CFCA 官方网站公布的新版本 CP 生效之日起，上一版本 CP 效力将自动终止。

9.9.3 终止后的存续条款

本 CP 中涉及审计、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 CP 终止后继续有效。

9.10 通告与沟通

如需要进一步了解任何本 CP 中提及的服务、规范、操作等信息，可以通过电话联系 CFCA，详见本 CP 第 1.5.2 章节。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

9.11 修订

CFCA 有权修订本 CP，并将修订版本进行公布。修订版本自版本中标注的生效日期起生效。

9.11.1 修订程序

当本 CP 不适用时，可按照本 CP 第 1.5.4 章节执行。审批通过后，新版《CFCA 电子认证服务证书策略》将在 CFCA 公司官方网站（https://www.cfca.com.cn）发布。

《CFCA 电子认证服务证书策略》将进行严格的版本控制。

9.11.2 通知机制和期限

CFCA 有权对本 CP 中的任何术语及条款进行修订，修订前无需事先通知任何一方，但应在修订完成后及时在 CFCA 官方网站公布修订版本。修订版本发布后七个工作日内，若订户未申请撤销该证书，即视为订户同意该修改。

9.11.3 必须修改业务规则的情形

当本 CP 描述的规则、流程和相关技术已经不能满足 CFCA 电子认证服务要求或本 CP 依据的法律法规和相关主管部门规章变更时，CFCA 必须修改业务规则。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

9.12 争议解决

CFCA 在其 CPS 中制定争议解决程序。

9.13 管辖法律

CFCA 的电子认证服务在各方面受中国法律法规的管辖,包括但不限于《中华人民共和国电子签名法》《中华人民共和国密码法》《电子认证服务管理办法》《电子认证服务密码管理办法》和《中华人民共和国民法典》等。

9.14 与适用法律的符合性

CFCA 的各项策略均应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。

9.15 一般条款

9.15.1 本 CP 的完整性

本 CP 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。

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均构成各参与者之间的完整协议。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

9.15.2 转让

CFCA、CFCA 授权的 RA 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。

9.15.3 分割性

若本 CP 中某一条款被相关主管部门认定为违法、无效或不可执行时，CFCA 将立即对该条款进行修订，直至其合法、有效和可执行为止。该条款的违法性、无效性或不可执行性，不影响本 CP 中其他条款的法律效力。

9.15.4 强制执行

无规定。

9.15.5 不可抗力

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。CFCA 对因不可抗力导致的损害不承担赔偿责任。

9.16 最终解释权

本 CP 最终解释权归 CFCA 所有，其内容由 CFCA 负责解释和修订。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn

附录 A: CFCA 电子认证服务业务规则 V5.0 约束 CA 系统

序号	根 CA	根 CA 算法	中级 CA	中级 CA 算法
1	CFCA CS CA	RSA2048/SHA1	CFCA OCA1	RSA2048/SHA1
			CFCA CS OCA11	
			CFCA GT OCA21	
2	CFCA ACS CA	RSA4096/SHA256	CFCA ACS OCA31	RSA2048/SHA256
			CFCA ACS OCA33	
			CFCA ACS OCA34	
3	CFCA CS SM2 CA	SM2/SM3	CFCA SM2 OCA1	SM2/SM3
			CFCA CS SM2 OCA11	
			CFCA GT SM2 OCA21	
			CFCA ACS SM2 OCA31	
			CFCA ACS SM2 OCA33	
			CFCA ACS SM2 OCA34	

*: CFCA CS SM2 CA 下中级 CA 与国家密码管理局国家信任根 ROOT CA 形成信任关系。

中金金融认证中心有限公司（CFCA）版权所有
https://www.cfca.com.cn