CFCA电子政务电子认证业务证书策略

CFCA E-Gov Certificate Policy

V1.0

生效日期：2025年1月15日

版本控制表

版本	修订状态	修订说明	修订人	审核人/批准人	修订日期
1.0	形成版本	按照管理办法要求形成第一版本	编写组	委员会	2024 年 12 月 31 日

目　　录

1 概括性描述 1
1.1 概述 2
1.2 文档名称与标识 3
1.3 电子认证活动参与者 3
1.3.1 电子政务电子认证服务机构 3
1.3.2 注册机构 4
1.3.3 订户 4
1.3.4 依赖方 5
1.3.5 其他参与者 5
1.4 证书应用 5
1.4.1 适合的证书应用 5
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 16
3.3.2 撤销之后的密钥更新的标识与鉴证 16

3.4 撤销请求的标识与鉴别 16
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知 20
4.4 证书接受 20
4.4.1 构成接受证书的行为 20
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 21
4.5.1 订户私钥和证书的使用 21
4.5.2 依赖方对公钥和证书的使用 22
4.6 证书更新 23
4.7 证书密钥更新 23
4.7.1 证书密钥更新的情形 23
4.7.2 请求证书密钥更新的实体 23
4.7.3 证书密钥更新请求的处理 23
4.7.4 颁发更新证书时对订户的通告 24
4.7.5 构成接受密钥更新证书的行为 24
4.7.6 电子认证服务机构对密钥更新证书的发布 24
4.7.7 电子认证服务机构对其他实体的通告 24
4.8 证书变更 24
4.9 证书撤销和冻结 24
4.9.1 证书撤销的情形 24
4.9.2 请求证书撤销的实体 26
4.9.3 撤销的流程 27
4.9.4 撤销请求宽限期 27
4.9.5 CFCA 处理撤销请求的时限 28
4.9.6 依赖方检查证书撤销的要求 28
4.9.7 CRL 发布频率 28
4.9.8 CRL 发布的最大滞后时间 29
4.9.9 在线证书状态查询的可用性 29
4.9.10 撤销信息的其他发布形式 29
4.9.11 对密钥遭受安全威胁的特别处理要求 29
4.9.12 证书冻结及解冻 29
4.10 证书状态服务 30
4.10.1 操作特征 30

4.10.2 服务可用性 30
4.11 订购结束 30
4.12 密钥托管与恢复 30
4.13 证书归档 31
5 认证机构设施、管理和操作控制 31
5.1 物理控制 31
5.2 程序控制 31
5.2.1 可信角色 31
5.2.2 每项任务需要的人数 31
5.2.3 每个角色的识别与鉴别 32
5.2.4 需要职责分割的角色 32
5.3 人员控制 33
5.3.1 资格、经历和无过失要求 33
5.3.2 背景审查程序 33
5.3.3 培训要求 33
5.3.4 再培训周期和要求 33
5.3.5 未授权行为的处罚 33
5.3.6 独立合约人的要求 34
5.3.7 提供给员工的文档 34
5.4 审计日志程序 34
5.4.1 记录事件的类型 34
5.4.2 处理日志的周期 35
5.4.3 审计日志的保存期限 36
5.4.4 审计日志的保护 36
5.4.5 审计日志备份程序 36
5.4.6 对导致事件主体的通告 36
5.4.7 脆弱性评估 37
5.5 记录归档 37
5.5.1 归档记录的类型 37
5.5.2 归档记录的保存期限 37
5.5.3 归档文件的保护 38
5.5.4 归档文件的备份程序 38
5.5.5 记录的时间戳要求 38
5.5.6 归档收集系统 38
5.5.7 获得和检验归档信息的程序 38
5.6 电子认证服务机构密钥更替 38
5.7 损坏与灾难恢复 39
5.7.1 事故和损害处理流程 39
5.7.2 计算资源、软件或数据的损坏 39
5.7.3 实体私钥损害处理程序 39
5.7.4 灾难后的业务连续性能力 39
5.8 电子认证服务机构或注册机构的终止 40
6 认证系统技术安全控制 40
6.1 密钥对的生成和安装 40

6.1.1 密钥对的生成 40
6.1.2 私钥传送给订户 41
6.1.3 公钥传送给证书签发机构 41
6.1.4 CA 公钥传送给依赖方 41
6.1.5 密钥的长度 41
6.1.6 公钥参数的生成和质量检查 42
6.1.7 密钥使用目的 42
6.2 私钥保护和密码模块工程控制 42
6.2.1 密码模块标准和控制 42
6.2.2 私钥多人控制 42
6.2.3 私钥托管 42
6.2.4 私钥备份 43
6.2.5 私钥归档 43
6.2.6 私钥导入、导出密码模块 43
6.2.7 私钥在密码模块的存储 44
6.2.8 激活私钥的方法 44
6.2.9 解除私钥激活状态的方法 44
6.2.10 销毁私钥的方法 44
6.2.11 密码模块的评估 44
6.3 密钥对管理的其他方面 45
6.3.1 公钥归档 45
6.3.2 证书操作期和密钥对使用期限 45
6.4 激活数据 45
6.4.1 激活数据的产生和安装 45
6.4.2 激活数据的保护 46
6.4.3 激活数据的其他方面 46
6.5 计算机安全控制 46
6.5.1 特别的计算机安全技术要求 46
6.5.2 计算机安全评估 46
6.6 生命周期技术控制 47
6.6.1 系统开发控制 47
6.6.2 安全管理控制 47
6.6.3 生命期安全控制 48
6.7 网络的安全控制 48
6.8 时间戳 48
7 证书、证书撤销列表和在线证书状态协议 48
7.1 证书 48
7.1.1 证书基本项 49
7.1.2 版本 49
7.1.3 序列号 49
7.1.4 算法对象标识符 49
7.1.5 名称形式 49
7.1.6 有效期 50
7.1.7 证书扩展项 51

7.2 CRL 54
7.2.1 版本号 54
7.2.2 CRL 和 CRL 条目扩展项 54
7.3 在线证书状态协议 55
7.3.1 版本号 55
7.3.2 OCSP 扩展项 55
8 一致性审计和其他评估 55
8.1 评估的情形及频率 55
8.2 评估者的资质 56
8.3 评估者与被评估者的关系 56
8.4 评估内容 56
8.5 对问题与不足采取的措施 57
8.6 评估结果的传达与发布 57
8.7 其他评估 58
9 法律责任和其他业务条款 58
9.1 费用 58
9.2 财务责任 58
9.3 业务信息保密 58
9.4 个人信息保护 59
9.5 知识产权 59
9.6 陈述与担保 59
9.6.1 电子认证服务机构的陈述与担保 59
9.6.2 注册机构的陈述与担保 60
9.6.3 订户的陈述与担保及义务 60
9.6.4 依赖方的陈述与担保及义务 61
9.6.5 其他参与者的陈述与担保 61
9.7 担保免责 61
9.8 承担赔偿责任的限制 61
9.9 有效期限与终止 61
9.9.1 有效期限 61
9.9.2 终止 62
9.9.3 终止后的存续条款 62
9.10 通告与沟通 62
9.11 修订 62
9.11.1 修订程序 62
9.11.2 通知机制和期限 63
9.11.3 必须修改业务规则的情形 63
9.12 争议解决 63
9.13 管辖法律 64
9.14 与适用法律的符合性 64
9.15 一般条款 64
9.15.1 本 CP 的完整性 64
9.15.2 转让 65
9.15.3 分割性 65

9.15.4 强制执行 65
9.15.5 不可抗力 65
9.16 最终解释权 65

1 概括性描述

中金金融认证中心有限公司（即 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，具有《电子认证服务许可证》《电子认证服务使用密码许可证》《电子政务电子认证服务许可证》。

本文档《CFCA 电子政务电子认证业务证书策略》（以下简称 CFCA E-Gov CP、本 CP），按照国家密码管理局发布的《电子政务电子认证服务管理办法》的要求，报北京市密码管理局并报国家密码管理局备案。

CFCA 基于密码技术，面向政务领域的各类实体签发数字证书，为政务活动提供电子签名认证服务，保证电子签名的真实性和可靠性的活动。本 CP 阐述了在电子政务领域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。适用于电子政务电子认证服务机构、注册机构、订户、依赖方等电子政务电子认证活动参与者，各方应充分理解本 CP 所约定的责任，并承担相应的责任和义务。

本 CP 引用的所有法律法规、标准规范、内部文档如未标识版本号的，以其最新版本为准。

本 CP 目录结构与 GB/T 26855《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，如章节条目中无特别要求的，均用“无规定”表示；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 声称符合本策略，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。

1.1 概述

证书策略（CP，Certificate Policy）是一个指定的规则集，指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 依据下列标准规范制定的 CFCA 电子政务电子认证服务的技术政策文件，本文中凡未指明日期的引用文件，以其最新版本为准。

1）《中华人民共和国电子签名法》《中华人民共和国密码法》《商用密码管理条例》《电子政务电子认证服务管理办法》;

2）GB/T 26855《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《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《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 电子政务电子认证业务证书策略》（简称 CFCA E-Gov CP、本 CP），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
2.16.156.112554.21	（CFCA 电子政务电子认证业务规则）文档标识
2.16.156.112554.20	（CFCA 电子政务电子认证业务证书策略）文档标识

1.3 电子认证活动参与者

本文中所包含的电子认证活动参与者有：电子政务电子认证服务机构、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 电子政务电子认证服务机构

电子政务电子认证服务机构（Certificate Authority，以下简称“CA”或“CA 机构”）即依法设立的电子政务电子认证服务提供者，承担证书签发、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（CRL）发布以及密钥管理等服务。本文中电子政务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，简称 RA 或 RA 机构）负责受理数字证书的申请、更新、恢复和撤销申请的实体，标识和鉴别数字证书申请者主体身份后，向 CA 提出认证请求。[1]

CFCA 可以承担 CA 角色和 RA 角色。CFCA 根据业务发展情况，授权其他机构作为 RA 机构，授权的 RA 机构与 CFCA 签署《数字证书合作协议》，履行协议及本 CPS 中注册机构的职责，按照 CFCA《注册机构运营规范》，在委托范围内以 CFCA 注册机构名义开展证书注册业务，不得再委托其他机构或者个人开展证书注册业务。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。

CFCA 自委托协议签订之日起 30 日内将 RA 机构名称、负责人，证书注册业务办理地址等信息予以公告，并向 RA 机构住所地省、自治区、直辖市密码管理部门备案。备案内容发生变更的，CFCA 也将自变更之日起 30 日内向 RA 机构住所地省、自治区、直辖市密码管理部门变更备案。

1.3.3 订户

获得 CA 签发的数字证书的实体，也称为证书持有人。为便于理解，在电子签名应用中，订户也称作签名人、证书持有人、

[1] GB/T 25056-2018 3.12 有修改

用户、最终用户（end-user）、证书申请者等。订户通常需要与CA签订合约以获得证书，并承担作为证书订户的责任。

1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.3.5 其他参与者

除CA、RA、订户和依赖方以外的参与者称为其他参与者。

1.4 证书应用

1.4.1 适合的证书应用

本CP下的证书适用于需要在电子政务网络交易中确认交易方身份、确保交易防篡改（完整性）、确保交易抗抵赖、确保交易的保密性等应用场景中。证书应用清单如下:

证书类型	实体性质	密钥用途	证书应用用途	备注
个人证书	个人	签名/加密	身份鉴别、数字签名、抗抵赖、保密性，适用于处理政务业务中个人需要签名的业务、需要保密的事项，或者需要表明个人身份的事项。	**普通证书**：证书存储在智能密码钥匙中，线下审核，当面交付或者线上审核，快递交付；或者证书软存储、委托业务方存储使用，线上审核，通知交付或邮件交付等。证书有效期1-5年
			身份鉴别、数字签名、抗抵赖，保密性等，适用于通过移动终端处理政务业务中，个人需要签名的业务、需要保密的事项，或者需要表明个人身份的事项。	**密钥分散型证书，**也称作：云证通证书，应有订户控制的智能终端（如手机）与云端服务参与运算，线上鉴别或线下鉴别，可搭配CFCA提供的云证通产品使用。证书有效期1-5年

机构证书	企业/事业单位/政府机构等	签名/加密	身份鉴别、数字签名、抗抵赖、保密性，适用于处理政务业务需要机构签名的业务、需要保密的事项，或者需要表明机构身份的事项。	**普通证书**：证书存储在智能密码钥匙中，线下审核，当面交付或者线上审核，快递交付；或者证书软存储、委托业务方存储使用，线上审核，通知交付或邮件交付等。证书有效期 1-5 年。
			身份鉴别、数字签名、抗抵赖，适用于通过移动终端处理政务业务中，机构需要签名的业务、需要保密的事项，或者需要表明机构身份的事项。	**密钥分散型证书**，也称作：云证通证书，应有订户控制的智能终端（如手机）与云端服务参与运算，线上鉴别或线下鉴别，需要搭配 CFCA 提供的云证通产品使用。通知交付。证书有效期 1-5 年。
设备证书	web 服务器	签名/加密	身份鉴别、数字签名、抗抵赖、保密性，用于表明电子政务业务网站身份，与浏览器客户建立安全通道。	**SSL 服务器证书**，标识网站身份，有效期 1-3 年。
	VPN 网关	签名/加密	身份鉴别、数字签名、抗抵赖、保密性，用于鉴别电子政务业务中 VPN 设备身份，建立安全通道，确保通信安全。	**VPN 证书**，标识 VPN 设备身份，有效期 1-3 年。
	其他设备	签名/加密	身份鉴别、数字签名、抗抵赖、保密性，用于鉴别电子政务业务设备身份，建立安全通道，确保通信安全。	**其他设备证书**，标识其他设备身份，有效期 1-3 年。

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：任何与国家或地方法律、法规或行政规章规定相违背的领域，任何未经过安全检测的环境及应用等。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 授权的注册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、法规和行政规章或破坏国家安全的情形下使用，由此产生的法律后果由订户自行承担。

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”（以下简称委员会），由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:

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	www.cfca.com.cn

1.5.3 决定 CP 符合策略的机构

电子政务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策略的，应由委员会评估后，可对本策略进行更新，更新发布后需自公布之日起 30 日内向北京市密码管理局报备。

1.5.4 CP 批准程序

本 CP 的管理机构是委员会，负责制定、评审、发布、更新、废止本 CP。委员会编写小组制定、修订 CP 初稿；CP 初稿由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。自公布之日起 30 日内向北京市密码管理局并报国家密码管理局报备。

1.6 定义和缩写

下列定义适用于本 CP。

序号	项目	定义
1	电子政务电子认证服务	指采用商用密码技术为政务活动提供电子签名认证服务，保证电子签名的真实性和可靠性的活动。[2]
2	电子政务电子认证服务机构	具备《电子政务电子认证服务许可》的，为政务领域提供电子认证服务的第三方机构。
3	注册机构	负责受理数字证书的申请、更新、恢复和撤销申请的实体，标识和鉴别数字证书申请者主体身份后，向 CA 提出认证请求。[3]
4	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

[2] 《电子政务电子认证服务管理办法》
[3] GB/T 25056-2018 3.12 有修改

		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。[4]
5	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。[5]
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。[6]
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。[7]
8	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。[8]
9	电子认证业务规则	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。
10	订户	获得 CFCA 签发的数字证书的实体，也称为证书持有人。在电子签名应用中，也称作签名人。
11	依赖方	依赖方是指基于对数字证书或者电子签名的信赖从事有关活动的实体。[9]
12	密钥	控制密码变换操作的符号序列。[10]
13	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。
14	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。
15	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。
16	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。

[4] GB/T 25056-2018 3.9
[5] 参考《电子签名法》第十四条
[6] GB/T 25056-2018 3.4
[7] GB/T 27913-2022 3.42
[8] GB/T 25069-2022 3.789
[9] 参考《电子签名法》及 GB/T 25056-2018 3.3
[10] GB/T 25069-2022 3.389

17	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。
18	公钥	非对称密码算法中可以公开的密钥。
19	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。
20	实体	个人、合伙企业、组织或具有合法的、独立可识别存在的业务。[11]
21	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。[12]
22	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，本文仅包含利用数字证书相关技术所做的电子签名。[13]
23	电子签章	使用电子印章签署电子文件的过程。[14]
24	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。[15]
25	撤销	因错误签发、密钥泄露、不再使用等原因需要停止使用证书。历史版本中的吊销、注销与本文中的撤销意思一致。

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）
2	RA	注册机构（Registration Authority）
3	KM	密钥管理系统（Key Management）

[11] GB/T 27913-2022 3.32
[12] GB/T 25069-2022 3.576
[13] GB/T 25069-2022 3.119
[14] GB/T 25069-2022 3.120
[15] GB/T 25069-2022 3.121

4	CRL	证书撤销列表（Certificate Revocation List）
5	OCSP	在线证书状态协议（Online Certificate Status Protoc
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	唯一甄别名（Distinguished Name）
10	PKI	公钥基础设施（Public Key Infrastructure）
11	OID	对象标识符（Object Identifier）

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，数字证书服务协议、相关的技术支持信息，证书链、证书、证书撤销列表（CRL）、证书状态信息等。

2.2 认证信息的发布

CFCA 的 CP、CPS 经委员会批准后发布，其他信息的发布按照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。

本 CP 中引用的属于公司内部管理制度及相关控制规则的文档，不在信息库中发布。

2.3 发布的时间或频率

CP、CPS 在完成本 CP 第 1.5.4 章节所述的批准流程后 15 个工作日内发布到 CFCA 网站上，并确保 7*24 小时可访问。CRL 的发布频率参见本 CP4.9.7（CRL 发布频率）。CFCA 签发的 CRL 信息，根据需要，也可以人工方式实时发布。

2.4 信息库访问控制

CFCA 采取适当措施，防止信息被篡改或被破坏。用户可通过 CFCA 官网访问本公司信息库，官网对所有用户开放。证书信息可供订户及依赖方通过指定条件查询。考虑到个人无 OCSP 服务查询工具，OCSP 服务信息不直接对个人用户开放。

3 标识与鉴别

3.1 命名

3.1.1 名称类型

CFCA 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）：唯一甄别名，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。

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 CFCA 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，DN 规则由 CFCA 定义。

3.1.5 名称唯一性

CFCA 签发给某个实体的证书，其主体甄别名（DN），在该证书签发 CA 系统内应能唯一标识该主体。属于同一实体的多张证书应通过证书序列号等唯一标识区别。

3.1.6 商标的识别、鉴别和角色

证书申请者不应在其证书申请中使用侵害他人知识产权的名称，CFCA 不具有实质审查申请者是否处于商标纠纷中的法律责任。出现此类争端时，CFCA 有权拒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

订户申请电子签名认证证书时，可通过以下方式证明拥有私钥:

1) 签名私钥应在智能密码钥匙或者通过 GB/T 37092《密码模块安全要求》 检测的密码模块中产生，由证书申请者专有;

2) 证书申请者应使用其私钥对证书请求信息进行签名;

3) CA 应使用证书申请者公钥验证该签名。

3.2.2 订户身份的鉴别

订户在申请 CFCA 签发的证书前，应仔细阅读申请数字证书相关事项，亲自或指定授权代表，提供有效身份证明文件、证书申请文件或以 CFCA 认可的安全方式提交真实有效信息，接受证书申请的有关条款，同意承担相应的责任。

CFCA 或者 CFCA 的 RA 机构接受订户的证书申请后，应对订户及其授权代表的身份真实性、完整性、准确性进行鉴别(核验)，对申请者提交的证书信息进行审核，妥善保存订户申请材料及鉴别记录。

3.2.3 没有验证的订户信息

CFCA 不对订户申请时的机构部门信息进行核验，对于未在核验范围内的信息，CFCA 不承诺相关信息的真实性，不承担相关的法律责任。

3.2.4 授权确认

当订户通过授权第三人代理申请证书时，注册机构应对授权进行核验。可通过核验授权文书、向授权人电话确认、向授权人发送短信、向授权人发送邮件等方式进行确认。

3.2.5 互操作准则

CFCA 通过 GM/T 0043《数字证书互操作检测规范》的检测，由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 签发 CA 证书，与国家根形成信任链。

截止目前，CFCA 未签发其他交叉认证的证书。

3.3 密钥更新请求的标识与鉴别

密钥更新是指订户初次注册时的信息不变，重新产生一对证书密钥，CA 重新为订户签发一张新的证书。密钥更新存在两种情况：“证书补发”，证书补发时新证书失效日期与原证书失效日期一致；“证书换发”是指在证书截止日期前三个月内或证书过期后申请更新证书密钥操作。

3.3.1 常规密钥更新的标识与鉴别

当订户需要更新的证书还能正常使用时，订户通过在线系统自动申请密钥更新，注册系统可通过核验订户老证书的有效性鉴别订户。

当订户需要更新的证书已不能使用，比如损坏、密钥泄露等，可以采用向初次注册时的手机号、邮箱等发送验证码验证的用户参与方式鉴别。

如订户临柜申请更新密钥，鉴别方式可参考本 CP 3.2.2 的规定。

3.3.2 撤销之后的密钥更新的标识与鉴证

证书撤销后，必须重新以本 CP 3.2 规定的方式进行鉴别，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 机构应执行鉴别，鉴别同本 CP3.2 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。

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、依法成立的组织，可以提交数字证书申请；证书申请应由证书持有者或相应的授权人提交，非证书持有者代表组织机构进行批量证书申请的还应获得该组织的授权。

4.1.2 注册过程与责任

1、证书申请者可通过在 RA 机构现场、CFCA 现场或者在线的方式，提出证书申请；申请者应事先阅读相关注意事项，理解并同意各项事项后，提交真实有效的信息，申请证书。

2、RA 机构应在受理证书申请时，告知申请者以下事项：

1）数字证书和电子签名的使用条件；

2）服务收费的项目和标准；

3）保存和使用证书持有人信息的权限和责任；

4）电子认证服务机构的责任范围；

5）证书持有人的责任范围；

6）其他需要事先告知的事项。

3、RA 机构收到申请者的申请后，对申请者以及申请信息按照本 CPS3.2 的方式进行审核。审核通过后注册申请者的信息。审核未通过的，应告知订户审核未通过的原因。

4、RA 机构审核申请者身份信息后，应协助订户与 CFCA 签订不限形式的《数字证书服务协议》。

5、订户与 CFCA 签署协议后，RA 机构对订户信息进行注册；如 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 校验 RA 机构权限及证书申请格式，签发数字证书，将签发的证书反馈给 RA 机构，RA 机构将证书转交给申请者。

订户信息注册完成后，如订户自行下载证书，则 RA 机构向 CA 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，通过指定的下载平台下载证书。

6、无论通过哪种方式获得证书，RA 应提示订户修改智能密码钥匙的初始口令。RA 机构应妥善保管证书订户申请资料及鉴别记录。

7、订户接受证书后，应妥善保管自己的证书私钥及数字证书，并合法合规使用数字证书。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，主动修改初始口令，并妥

善保管。

CFCA 数字证书注册过程须符合 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

证书申请者申请证书时，注册机构应遵循以下规范:

1）依据本 CP3.2 的规定，取得申请者申请数字证书的相关资料;

2）依据本 CP3.2 的规定，核验并记录申请数字证书申请时的相关识别资料;

3）依据本 CP3.2 的规定，取得申请者的证书请求文件，并确认公钥属于申请者所有;

4）确认将记载于数字证书中的信息是正确的。

4.2.2 证书申请批准和拒绝

完成本 CP 4.2.1 的审核后，视为批准证书申请，如未通过审核应拒绝，并应在 2 个工作日内告知拒绝理由。

4.2.3 处理证书申请的时间

处理证书请求的最长响应时间应不超过 2 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 CP3.2 章节的流程的基础上，RA 应与 CA 建立安全通道并进行双向身份鉴别，CA 对 RA 机构的权限、数据格式、RA 的签名等进行验证，验证通过后，CA 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 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。

4.3.2 电子认证服务机构对订户的通知

无论是拒绝还是批准订户的证书申请，CFCA 或 CFCA 授权的注册机构将通过电话、短信、电子邮件或其他任意一种方式告知订户申请结果。

4.4 证书接受

4.4.1 构成接受证书的行为

本 CP 认可以下接受证书的行为：

订户应将收到的证书与其申请信息进行核对，确认无误后方可使用，一经使用即视为订户已经接受此证书；如订户有异议或拒绝接受证书时，RA 应协助订户撤销证书或者重新签发证书。

4.4.2 电子认证服务机构对证书的发布

证书签发完成后，对于证书申请者明确表示拒绝发布证书信息的，CFCA 将不发布证书信息；没有明确表示拒绝的，CFCA 按照发布规则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

证书签发后，CFCA 不对其他实体进行主动通告，依赖方可在信息库上自行查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在使用证书时必须遵守本 CP 的要求，订户的私钥和证书应用于约定的、批准的用途（见本 CP 第 1.4.1 章节的规定），在使用证书私钥及证书时遵守以下事项:

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，订户应确定自己了解业务情况，以及该证书与业务之间的权利义务关系；

6）订户如委托、授权其他方保管、使用自己的私钥及证书，建议订户定期核实授权范围及使用记录。

4.5.2 依赖方对公钥和证书的使用

依赖方信赖 CFCA 签发的证书所证明的信任关系时需要：

1）获取并安装该证书对应的证书链；

2)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；

3）验证证书的用途适用于对应的签名；

4）使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。

4.6 证书更新

证书更新是指在订户证书 DN 信息不变，保持原有公钥不变的情况下为订户重新签发一张新证书。CFCA 原则上不提供该项服务。

4.7 证书密钥更新

证书密钥更新是指订户生成新密钥并为之申请新证书。

4.7.1 证书密钥更新的情形

1）当订户证书即将到期或已经到期时;

2）当订户证书密钥遭到损坏时;

3）当订户证实或怀疑其证书密钥不安全时;

4）其他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

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 章节的规定。

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

证书变更是指订户的证书 DN 信息发生变化，在不改变现有公钥的情况下重新申请一张证书。CFCA 不直接提供该项服务，通常情况下，订户的主体信息发生变化时，应重新申请一张新证书。

4.9 证书撤销和冻结

4.9.1 证书撤销的情形

如有下列情况中的任何一种情况发生，订户可发起主动撤销：

1）订户申请撤销证书;

2）订户提供证明，确认证书申请未经有效授权;

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。

以下情况下，订户证书将被动地撤销:

1）有证据表明订户证书使用于非法事项上，或 CFCA 发现订户证书超范围使用;

2）有证据表明订户未履行本 CP 或订户协议中约定的义务;

3）有证据表明订户已丧失证书主体信息（如域名/IP）所有权或控制权;

4）CFCA 获知通配符证书被用于验证一个欺诈性或极具误导的子域名;

5）CFCA 判断证书签发时未能满足证书策略或证书标准中的要求和条件，或者证书中的任何信息不准确;

6）CFCA 因某些原因停止业务，并且没有安排其他的 CA 承接业务时;

7）CFCA 电子认证服务资质被撤销后，无人承接 CFCA 业务时，CFCA 将撤销所有已签发的证书，仅维持 CRL/OCSP 服务;

8）CFCA 的 CA 签名证书私钥被泄露时，将根据应急预案撤销所有已签发的证书；

9）证书的重要参数被国际国内主流标准或被监管机构认为有重大风险时；

10）仅用于注册机构应用范围的证书，因注册机构申请停止使用该证书时，可向 CFCA 提出撤销申请；

11）政务机构的证书持有者不从事原岗位工作，政务机构可发起证书撤销申请；

12) 司法机构要求撤销证书持有者证书或法律、行政法规规定的其他情形。

4.9.2 请求证书撤销的实体

已申请 CFCA 证书的订户、CFCA 授权的注册机构可请求证书撤销。CFCA 授权的注册机构申请批量撤销证书时，需要提交相关说明材料，经 CFCA 审核通过后予以处理。依赖方、软件商或其他第三方也可提交证书问题报告，通知 CFCA 撤销证书的合理原因，CFCA 经调查核实后，根据调查结果决定是否采取撤销或其他适当方式处理。

同时，CFCA 也可在本 CP 4.9.1 所述的情形下撤销订户的证书。

4.9.3 撤销的流程

1）主动撤销

订户申请撤销证书时可与申请证书时一样，向 RA 提供包含有效身份证明文件、需要撤销的证书信息或者证书撤销申请表、撤销原因等。

RA 收到订户的撤销申请材料后，按照订户申请证书时的核验方法对订户身份及撤销申请信息进行核验，审核通过后向 CA 发起撤销请求。

CA 收到撤销请求后，验证发起撤销请求的 RA 权限以及撤销请求数据格式后，执行证书撤销，并将撤销结果反馈给 RA，同时按照信息发布策略发布 CRL、更新 OCSP 状态。

RA 收到证书撤销结果后，反馈给订户撤销结果。

2）被动撤销

当 CA 或 RA 判断出现本 CP 第 4.9.1 章节中会导致订户证书被动撤销的情形时，RA 可向 CFCA 提出撤销证书的申请，CFCA 将通过内部流程申请撤销证书。在证书撤销后，CA 将按照 CRL 发布策略发布 CRL。

4.9.4 撤销请求宽限期

如果订户怀疑其证书密钥不安全，订户应在知晓该安全隐患

的 24 小时内，向 RA 或者 CA 请求撤销证书。CFCA 可以根据具体情况延长撤销请求宽限期。

如果 CFCA 的 CA 证书密钥不安全，CFCA 应在知晓该安全隐患的 24 小时内，向 CFCA 信息安全委员会报告，按照 CFCA 信息安全委员会的决议，撤销该 CA 证书及其签发的所有证书。

4.9.5 CFCA 处理撤销请求的时限

如果订户因怀疑其证书密钥不安全，并请求撤销其证书，则 CFCA 应在收到请求后，24 小时内处理该请求。

如果其他方向 CFCA 报告签发了问题证书，则 CFCA 应在收到问题报告后，24 小时内启动调查，并将调查结果及处理情况反馈给报告者。

4.9.6 依赖方检查证书撤销的要求

依赖方应根据其风险、责任及可能导致的后果，自行判断检查撤销信息的时间间隔。依赖方在信任此证书前应检查证书的有效性，确认证书未被撤销。

4.9.7 CRL 发布频率

CRL 发布频率应为每 24 小时至少发布一次。

4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大延迟时间为 24 小时。

4.9.9 在线证书状态查询的可用性

CFCA 提供 7*24 小时不间断的 OCSP 服务。

CFCA 至少每 12 个月更新一次根 CA 证书和下级 CA 证书的状态；如果根 CA 证书或者下级 CA 证书被撤销，CFCA 将应在 24 小时内更新根 CA 证书或者下级 CA 证书状态。

4.9.10 撤销信息的其他发布形式

无规定。

4.9.11 对密钥遭受安全威胁的特别处理要求

订户、注册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 的签名密钥遭受威胁时，将会按照应急预案处理。

4.9.12 证书冻结及解冻

CFCA 在该 CP 下不支持证书冻结及解冻操作。

4.10 证书状态服务

4.10.1 操作特征

证书状态服务按照本 CP4.9.9 和 4.9.10 的规定提供，CFCA 根据需要，在证书过期后，将其从 CRL 中删除。

4.10.2 服务可用性

CFCA 保障具备足够的资源运行和维护其 CRL 和可选的 OCSP 能力，提供 7*24 小时可用的在线信息库，应用软件可以利用该信息库自动检查 CA 签发的未过期证书的当前状态。

4.11 订购结束

以下两种情形将被视为订购结束:

1）证书到期后不续订即视为订购结束;

2）证书撤销视为订购结束。

4.12 密钥托管与恢复

CFCA 自身的密钥不托管给第三方。CFCA 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 CFCA 申请密钥恢复，经审核后，

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，CFCA 对失效证书进行归档，证书归档记录保留 5 年。

5 认证机构设施、管理和操作控制

CFCA 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》的要求建设、维护、管理基础设施。

5.1 物理控制

CFCA 的物理安全应满足 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》第 8.5 章节的各项要求。

5.2 程序控制

5.2.1 可信角色

CFCA 的可信角色至少包含系统管理员、安全管理员、审计员、密钥管理员等。

5.2.2 每项任务需要的人数

进出 CA 系统所在的物理环境的人数应为两人及以上，进入

应通过双因子识别机制进行控制，且应保留进入、进出的记录以供审计。

对系统的任何操作，应是经过授权的双人操作，登入系统应采取双因子认证，任何操作应保留记录，以供审计。

对 CA 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（口令）、智能密码钥匙或者 IC 卡等进行识别与鉴别。

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和应用管理员、数据库管理员、网络管理员、操作员、制证人员兼任;

2）系统和应用管理员、数据库管理员、网络管理员不得与订户信息收集人员、订户身份及信息核验人员、操作员、制证人员兼任;

3）订户信息收集人员、订户身份及信息核验人员不得与操作员、制证人员兼任。

5.3 人员控制

5.3.1 资格、经历和无过失要求

CFCA 对可信角色的人员必须进行相关的背景、资历调查，聘任的可信人员应具有足以胜任其工作的相关经验，且没有相关的不良记录。

5.3.2 背景审查程序

CFCA 制定背景调查操作规程，以满足本 CP5.3.1 的要求。

5.3.3 培训要求

CFCA 的作业人员，应依据其职务、职责，对 CA 运作应具备的软硬件功能、作业程序、控制程序、CP、CPS 以及其他相关技术与作业规范进行培训。

如委托授权注册机构，也应对注册机构人员进行相应培训。

5.3.4 再培训周期和要求

对于本 CP5.3.3 所需培训内容发生变更时，CFCA 应再次对相关人员（包括注册机构人员）进行培训，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

CFCA 具备针对员工未经授权行为的处罚措施。

5.3.6 独立合约人的要求

CFCA 针对独立合约人的管理与本机构人员管理同等要求，且与独立合约人签订保密协议。

5.3.7 提供给员工的文档

CFCA 向作业人员提供其工作所必需的文档，文档配备满足 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》第 10.6 章节的要求。

5.4 审计日志程序

CFCA 维护控制系统以提供合理的保证,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周期性的审阅。

5.4.1 记录事件的类型

CFCA 无论其用于审计的记录是纸质的还是电子的，应至少包含以下内容:

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 IP 地址，端口，通信证书信息等);

5) 生成日志条目的实体身份。

事件记录类型:

1）CA 密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁;

2）RA、CA、KM 系统记录的与证书生命周期操作相关的记录，包括证书申请、证书密钥更新、证书撤销等事件;

3）系统、网络安全事件记录;

4）操作系统、CA 系统、数据库系统配置操作日志;

5）操作审批记录;

6）人员访问控制记录、监控记录。

5.4.2 处理日志的周期

CFCA 制定记录核查规程，核查记录的完整性、确保记录未被篡改，对不正常的或任何警告应进行谨慎调查。核查结果的应用应保持文件记录。

5.4.3 审计日志的保存期限

本 CP5.4.1 中的事件记录类型 1，保存至 CA 密钥失效后 5 年；事件记录类型 2，日志至少保存到证书失效后 5 年；其他事件记录类型，日志至少保存至一个评估周期（1 年）后。

5.4.4 审计日志的保护

CFCA 建立相应的管理制度，采取物理和逻辑的控制方法确保只有经授权的人员才能对审计日志进行操作。审计日志处于严格的保护状态，严禁未经授权的任何操作。

5.4.5 审计日志备份程序

CFCA 制定日志备份程序，且相关备份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。

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。

5.4.6 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。

5.4.7 脆弱性评估

CFCA 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

CFCA 归档的记录至少包含以下类型:

1）电子认证服务机构接收外部评审的资料;

2）电子认证服务机构的 CP、CPS 及历史版本;

3）与认证机构运营相关的合同;

4）系统环境建设与配置相关档案;

5）系统变更记录、故障记录、事件报告;

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

CFCA 保存与证书相关的归档记录，保存至证书失效后 5 年。

其他记录的归档保存期限，由电子认证服务机构在其 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

归档文件的备份内容包括：数据库的备份、CRL 文件的备份、操作系统日志的备份、应用日志的备份。

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标识。

5.5.6 归档收集系统

归档收集系统应满足本 CP5.4.1 的要求。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员才能获得归档信息，应进行不定期的抽查检验，确保归档信息有效。

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，CFCA 定期更换密钥，已更换

的密钥不得再次使用。

CFCA 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 事故和损害处理流程

CFCA 对故障类型及故障级别进行不同情况的处理和报告。

5.7.2 计算资源、软件或数据的损坏

当计算资源、软件或数据受到破坏后，必须尽快重新恢复服务。CFCA 至少每年演练一次应急处理程序。

5.7.3 实体私钥损害处理程序

CFCA 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

CFCA 制定了业务连续性计划，保证在灾难发生后按照预定计划执行恢复。CFCA 至少每年演练一次，确保业务性计划可执行。

5.8 电子认证服务机构或注册机构的终止

注册机构终止服务时，按照与 CFCA 签署的协议执行。CFCA 执行终止程序按照《电子政务电子认证服务管理办法》第二十九条要求执行。

6 认证系统技术安全控制

CFCA 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。

CFCA 的 CA 系统产生密钥的设备至少应达到 GB/T 37092《密码模块安全要求》中的三级要求。

密钥用法应符合 GB/T 20518《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 密钥对是在 CFCA 屏蔽机房的密码设备内部产生的。使用的密码设备具有商用密码产品检测认证证书。CFCA 有严格规范的密钥管理办法以及安全机制，确保密钥的生成安全。

RA 系统密钥对是在安全控制下由 RA 系统内部产生，对应系

统证书由 CFCA 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。

6.1.2 私钥传送给订户

CFCA 只为订户提供加密密钥对的生成服务，并在 CPS 中说明密钥对传输的安全控制措施。

6.1.3 公钥传送给证书签发机构

订户的公钥应和订户信息通过安全通道传递到 CA 系统。CFCA 在其 CPS 中详细说明公钥传送方式。

6.1.4 CA 公钥传送给依赖方

CFCA 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 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，根 CA 证书密钥算法及长度支持 SM2-256，订户证书密钥长度支持 SM2-256。

6.1.6 公钥参数的生成和质量检查

CFCA 采购的用于产生密钥的设备需具备相应等级的密码认证证书，同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

CFCA 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。

根 CA 私钥不得用于签署订户证书。

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《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

CFCA 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

CFCA 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，CFCA 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。

6.2.4 私钥备份

CFCA 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。

注册机构及订户的私钥备份，本策略不作规定。

6.2.5 私钥归档

CFCA 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，会同时将归档的 CA 密钥进行销毁。

CFCA 对订户的加密密钥对归档，至少保存至证书过期后 5 年。

CFCA 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 私钥必须由符合条件的硬件设备产生，导入、导出应按照多人控制策略执行，应与初始操作具备同样的操作脚本，保持操作记录。

6.2.7 私钥在密码模块的存储

CA 私钥应存储在符合本 CP 6.1.1 要求的密码模块，密码模块应获得商用密码检测认证证书。

6.2.8 激活私钥的方法

CFCA 按照设备厂商的说明激活私钥，激活数据（如 PIN，口令或手工持有的密钥分享组件）至少应达到 8 位。

6.2.9 解除私钥激活状态的方法

对于已激活的硬件密码模块，CFCA 确保访问得到授权。当不再使用私钥时，必须在密码模块中销毁私钥。

6.2.10 销毁私钥的方法

当不再使用 CA 的私钥或与之对应的 CA 证书过期、撤销时，必须销毁 CA 的私钥。销毁 CA 私钥的操作应具有操作脚本，且销毁后不能使用任何信息来推断私钥的任何部分，销毁操作应保持记录。

6.2.11 密码模块的评估

CFCA 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

CFCA 通过证书的方式归档公钥，公钥归档见本 CP 4.13 的规定。

6.3.2 证书操作期和密钥对使用期限

证书的有效期与密钥对有效期一致，签名私钥在到期后不得继续使用，签名公钥在到期后可用于验证已做的签名的有效性。加密证书的有效公钥在到期后不能继续使用，加密证书的加密私钥到期后可以继续使用。

6.4 激活数据

CFCA 在其 CPS 中说明 CA 密钥的激活数据保护措施，包括产生、储存、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者智能 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。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

CFCA 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）各层级间采取异构防火墙防护;

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。

6.5.2 计算机安全评估

CFCA 定期对 CA 系统进行安全性评估，每年应至少进行信息

系统三级等保测评。

6.6 生命周期技术控制

6.6.1 系统开发控制

CFCA 系统的开发管控满足以下要求:

1）对开发应具有详细的说明文件;

2）应控制和检查软硬件的购买、使用和修改，防止可能的隐蔽通道或恶意代码，CA 系统在初次使用及以后应定期扫描恶意代码;

3）对 CA 系统的开发和维护，应具备一定授权管理机制，确保 CA 系统的完整性。

6.6.2 安全管理控制

cFCA 对 CA 系统的配置、修改或升级，制定操作控制措施，并记录相关操作，同时应具备定期侦察未经授权的改变的机制。

CFCA 有软硬件设备生命周期的安全管控作业规范，软硬件设备接收时须有安全保护核查措施。

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

6.6.3 生命期安全控制

CFCA 定期对 CA 的生命周期进行安全审查，以确保相关措施符合相关规定。

6.7 网络的安全控制

CFCA 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》要求进行网络划分和安全防护。

6.8 时间戳

CFCA 涉及 CA 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。

CFCA 提供时间戳服务，时间戳请求、应答、格式等符合 GB/T 20520-2006《信息安全技术 公钥基础设施 时间戳规范》。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

CFCA 签发的数字证书格式，符合 IETF RFC 5280 及 GB/T 20518《信息安全技术 公钥基础设施 数字证书格式》。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

CFCA 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 算法对象标识符

证书密码算法标识如下：

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	

7.1.5 名称形式

CFCA 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

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者 CA 系统名称	必选	CFCA ACS OCA31
OU2	如 INDIVIDUAL-1	如 O 为 CA 系统名称，则该项存在，用于标识证书类型；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	如：CITIC	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		个人或机构法定名称	张三/xx 公司

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 担保对证书状态的相关信息进行维护。证书有效期的起始时间（notBefore）和证书有效期的终止时间（notAfter）来表示，时间应精确

到秒。

CA 证书的有效期最长不超过 30 年，订户证书的有效期最长不超过 5 年零 3 个月。

7.1.7 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。扩展关键度可定义成关键的或非关键的，表明一个证书的使用者是否可忽略该扩展项。证书的应用系统如果不能识别关键的扩展时，应拒绝接受该证书，如果不能识别非关键的扩展，则可忽略该扩展项的信息。

CFCA 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、密钥用法、扩展密钥用途、证书策略、主体替换名称（可选设备证书）、基本限制、CRL 分发点。

CFCA 设定其私有扩展项时，私有扩展项设置为非关键性扩展。

CFCA 签发的证书私有扩展项符合 IETF RFC 5280 标准原则。

7.1.7.1 颁发机构密钥标识符

CFCA 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，该扩展项为非关键项。

7.1.7.2 主体密钥标识符

订户证书中包含主体密钥标识符扩展项，它标识了被认证的公钥，可用于区分同一主体使用的不同密钥（如证书密钥更新时），该扩展项为非关键项。

7.1.7.3 证书策略及对象标识符

本 CP 下所签发的证书，包含证书策略项，证书策略及对象标识符，参考本 CP 第 1.2 章节的规定。该项为非关键项。

7.1.7.4 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。该项为非关键项。

7.1.7.5 基本限制

CA 证书的基本限制扩展项中 Subject Type 为 CA，则该项必须为关键扩展；最终订户证书的基本限制扩展项中 Subject Type 为 End Entity，该项为非关键扩展。

7.1.7.6 密钥用法

所有的实体证书包含本扩展，CA 证书只能包含 keyCertSign、cRLSign 密钥用法，该项必须为关键扩展。

对于订户证书，该项为关键扩展，密钥用法签名证书：数字签名、抗抵赖；加密证书：数据加密、密钥协商、密钥交换。

7.1.7.7 扩展密钥用法

本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。该项为非关键项。

7.1.7.8 CRL 分发点

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

7.1.7.9 主体替换名称

主题替换名称包含一个或多个可选替换名（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。该项为非关键项。

服务器证书必须包括该扩展，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。

7.1.7.10 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或识别出包含无

法处理的关键扩展，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，则必须对其进行处理。

7.2 CRL

CFCA 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。

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 的甄别名;

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

CFCA 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。

CFCA 提供的 OCSP 服务符合 IETF RFC 6960 及最新版本《信息安全技术 公钥基础设施 在线证书状态协议》。

7.3.1 版本号

IETF RFC 6960 定义的 OCSP v1 版。

7.3.2 OCSP 扩展项

与 IETF RFC 6960 一致。

8 一致性审计和其他评估

8.1 评估的情形及频率

CFCA 在如下情形中接受或进行评估:

1）根据《电子政务电子认证服务管理办法》的规定，接受主管部门的评估和监督检查;

2）CFCA 自行或者委托专业机构每年至少进行一次电子政务电子认证服务合规性评估，对评估中发现的问题及时进行整改，

并向北京市密码管理部门报送合规性评估报告;

3）CFCA CA 系统每年进行信息系统三级等级保护测评;

4）CFCA 根据业务发展情况，对注册机构进行评估;

5）当系统发生变更时，变更前后均应进行评估;

6）CFCA 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

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

8.3 评估者与被评估者的关系

内部审计人员与执行审计内容、评估内容的岗位职责不能重叠。外部测评机构、审计机构与 CFCA 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 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

CFCA 将对评估报告中的问题进行影响评估，对于能立即整改的问题，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决定，CFCA 将向公众发布行业主管部门对 CFCA 的检查或评估结果。

当 CFCA 对注册机构进行抽样审计后，审计结果将只在 CFCA 内部进行传达，并与相关注册机构进行沟通。CFCA 对审计存在问题的注册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

CFCA 对自身的电子认证活动进行抽样审查。CFCA 对注册机构的活动进行抽样审查，注册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 可就签发、补发证书、换发证书、撤销证书以及证书生命周期的相关服务等收取费用。有关费用的相关条款、条件应在申请数字证书时清楚说明。

9.2 财务责任

CFCA 具备维持其业务可持续发展所需要的财力支持，并具备用于承担赔偿责任而需负担的财务能力。

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 中披露个人信息保密情况。

9.5 知识产权

本 CP 下的知识产权归 CFCA 所有。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

1）依据本 CP 制定电子认证服务规则（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）公布并确认与用户约定的条款符合法律法规、标准规范基本要求；

5）对违反用户义务或 CPS 相关约定的证书及时进行撤销；

6）按照规则发布撤销列表，并保证用户可查询使用；

7）提供如本 CP 第 2 章所列信息库服务。

9.6.2 注册机构的陈述与担保

1）依据本 CP 及 CFCA 的 CPS，执行用户注册相关操作;

2）接受用户申请，留存足以核验订户申请信息的相关资料;

3）在接受用户申请时，确实了解用户，并正确执行批准与否;

4）履行与 CFCA 之间的协议。

9.6.3 订户的陈述与担保及义务

1）用户向注册机构提交申请时，必须提供详细且正确的申请资料;

2）妥善安全地保护其私钥，及时修改密码;

3）确实了解并同意接受本政策及电子政务电子认证服务机构 CPS 及使用要求，并在同意后使用数字证书;

4）密钥被盗或怀疑不安全时，必须依据电子政务电子认证服务机构的 CPS 及时向注册机构提出撤销;

5）在约定范围内使用数字证书;

6）重要信息、资料变更时应当及时通知 CFCA 或原 RA,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 CFCA 或原 RA,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，订户需承

担相应的赔偿责任。

9.6.4 依赖方的陈述与担保及义务

依赖方应通过正确途径获取到 CA 机构的证书链，并在信任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担保

无规定。

9.7 担保免责

CFCA 在 CPS 中说明担保免责情况。

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。

9.9 有效期限与终止

9.9.1 有效期限

本 CP 在发布时标注生效日期，CFCA 应在生效日期之前在其官方网站（https://www.cfca.com.cn）公布。

9.9.2 终止

CFCA 有权终止本 CP（包括其修订版本），CFCA 应在本 CP（包括其修订版本）终止日期的 30 日之前在其官方网站公布终止声明。

自新版本生效之日起，上一版本的 CP 效力将自动终止。

9.9.3 终止后的存续条款

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，联系电话：400-880-9888。

9.11 修订

CFCA 有权修订本 CP，并将修订版本在官方网站（https://www.cfca.com.cn）上公布。

9.11.1 修订程序

当本 CP 不适用时，由委员会组织编写组进行修订。

修订完成后，委员会进行审批，审批通过后将在 CFCA 公司的

网站(https://www.cfca.com.cn)上发布新的《CFCA 电子政务电子认证业务证书策略》。

《CFCA 电子政务电子认证业务证书策略》将进行严格的版本控制。

9.11.2 通知机制和期限

CFCA 有权修订本 CP 中的任何术语、条款，事前无需通知任何一方，但在修订后应及时公布在 CFCA 网站上。如在修订发布后 7 个工作日内，订户没有申请对其证书进行撤销，将视为同意该修改。

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电子政务电子认证服务业务要求或本 CP 依据的法律法规和部门规章变更时，

CFCA 必须修改本策略。

9.12 争议解决

CFCA 在其 CPS 中订定争议解决程序。

9.13 管辖法律

CFCA 的电子认证服务受《中华人民共和国电子签名法》《中华人民共和国密码法》《电子政务电子认证服务管理办法》和《中华人民共和国民法典》 等相关法律法规管辖。

CFCA 的电子政务电子认证服务在各方面遵循中国法律和法规的管制和解释。

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各项法律法规和相关主管部门的要求。若本 CP 的某一条款被主管部门宣布为违法、不可执行或无效时，CFCA 将对该条款进行修改，直至该条款合法、有效和可执行为止。本 CP 某一个条款违法、不可执行或无效时，不影响本 CP 中其他条款的法律效力。

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。

CPS、CP、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。

9.15.2 转让

CA 机构、CFCA 授权的注册机构、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

本 CP 的某一条款被主管部门宣布为违法、不可执行或无效时，CFCA 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 CP 中其他条款的有效性。

9.15.4 强制执行

无规定。

9.15.5 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。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、传染性疾病、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 最终解释权由 CFCA 所有，由 CFCA 负责解释和修订。