CFCA电子政务电子认证业务规则

CFCA E-Gov Certification Practice Statement

V3.0

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
2.0	新增	1.按照国密局要求编写	编写组	委员会	2012 年 8 月
3.0	修订	1.按照国密局 2024 年 9 月的《电子政务电子认证服务管理办法》进行修订	编写组	委员会	2024 年 12 月

目　　录

前言

《中华人民共和国电子签名法》第十四条 可靠的电子签名与手写签名或者盖章具有同等的法律效力。

CFCA 是第三方电子政务电子认证服务机构，采用商用密码技术，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。

注册是电子认证服务的一个组成部分，受理用户证书申请，审核用户申请信息，协助用户申请数字证书。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开展数字证书业务。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。

用户申请 CFCA 签发的数字证书，接受与 CFCA 之间的《数字证书服务协议》。用户应妥善保管其数字证书私钥安全（可使用智能密码钥匙或通过商用密码检测认证的密码模块），如用户委托他人代为产生签名私钥，申请、保管、使用证书等，建议用户应明确委托授权范围，并定期核查授权履行情况。用户如因故意、过失（被诈骗）等导致使用数字证书时遭受损失，订户应自行承担由此产生的责任。

CFCA 对用户的赔偿责任见 CFCA 官方网站上的《数字证书服务协议》。

版本修订说明（2024 年 12 月）

本次修订主要从结构上参照 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》，结合《电子政务电子认证业务规则规范》进行了修订。

本次修订的主要目的，对照国密局最新版的《电子政务电子认证服务管理办法》要求，增加了对注册机构的备案、培训、定期评估等内容；进一步完善在线申请证书进行身份鉴别的相关描述，明确处理时限等；完善个人信息保护的描述；对照最新的国标、行标完善了定义和术语，增加了证书格式样例等。

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，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》。在中国人民银行和中国银联的领导下，历经 20 余年积淀，CFCA 已发展成为以网络安全综合服务为核心的科技企业。

本文档《CFCA 电子政务电子认证业务规则》（以下简称 CFCA E-Gov CPS、本 CPS），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，参照 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》《电子政务电子认证业务规则规范》制定，报北京市密码管理局并报国家密码管理局报备。

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认证服务，保证电子签名的真实性和可靠性的活动。本 CPS 阐述了 CFCA 提供电子政务电子认证服务的各项操作规程，符合《CFCA 电子政务电子认证业务证书策略》最新版本。适用于 CA、RA、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 CPS 所约定的责任，承担相应的责任和义务。

本 CPS 适用的 CA 系统见附录《CFCA 电子政务电子认证业务规则约束 CA》，CFCA 的所有 CA 系统，包含子 CA，均由 CFCA 所有，由 CFCA 直接控制，CFCA 将根据业务发展需要评估是否需要对 CPS 进行更新调整。

本 CPS 在原《CFCA 电子政务电子认证业务规则》V2.0 版本的基础上完善修订。本文档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。

1.2文档名称与相关标识

本 CPS 的名称为《CFCA 电子政务电子认证业务规则》，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

本节对电子认证活动参与者不同实体的身份、角色及其责任进行描述。

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”或“CA机构”)即依法设立的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。本文中电子认证服务机构、CA机构专指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）负责标识和鉴别证书主体身份的实体,向CA提出认证请求。

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

订户是从 CA 机构获得证书的最终实体，订户在获得证书之前，称作“申请者”。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、用户、最终用户（end-user ）、证书申请者等。

1.3.4 依赖方

依赖方是指在信任 CA 机构的前提下，信任证书所标明的信息，并依赖该证书用于交易时的身份鉴别、验证交易信息的完整性、对交易信息进行加密保护等的实体。

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 证书类型及适合的证书应用

数字证书具备用户身份鉴别、交易抗抵赖性、信息完整性、信息保密性四项基本功能，用户可根据自己需要，在电子政务业务中灵活选择一种证书功能或多种证书功能。详见下表。

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。
			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。
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。
			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。
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**，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**，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**，有效期 1-3 年。

1.4.2 限制的证书应用

本 CPS 的各类证书的应用基于证书中的“证书策略”“密钥用法”域进行约束，然而基于证书扩展项约束的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本

CPS 限定的应用范围，将不受 CFCA 的保护。

本 CPS 的证书不能在如下领域使用：任何与国家或地方法律法规规定相违背的领域，以及任何不安全的环境及应用。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或破坏国家安全的情形下或危险环境下使用，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 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 CPS。

1.5.2 联系方式

用户可通过以下途径进行查询、建议或投诉：

组织机构	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 CPS 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时需对本文档进行更新时，由委员会评估后，可对本文档进行更新，更新发布后需向北京市密码管理局并报国家密码管理局报备。

1.5.4 CPS 批准程序

本 CPS 的管理机构是委员会，负责制定、评审、发布、更新、废止本 CPS。委员会编写小组制定、修订 CPS 初稿；CPS 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。

CFCA 将定期评估本 CPS 的适用性，并及时修订本 CPS，按照前述流程批准公布。公布后的版本并对生效日期之后获发证书的申请者以及订户均具约束力。订户、依赖方，需定期查阅 CFCA

官网 https://www.cfca.com.cn 发布的本 CPS 的最新版本，如在本 CPS 更新公布 1 个月后，仍继续使用 CFCA 签发的数字证书，即表明同意接受此等修订的约束。如果订户、依赖方不接受此等修订的约束，应在立即停止使用 CFCA 签发的证书。

1.6定义和缩写

见附录 A：定义与缩写。

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，证书用户操作手册、证书常见问题解答(FAQ)、售后服务流程、获得证书帮助联系方式(客户服务热线电话、办公地址、邮政编码、投诉电话等)相关的技术支持信息，证书链、证书、证书撤销列表（CRL）、证书状态信息以及其他应该发布的相关信息。

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 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。

CP、CPS、数字证书服务协议、证书链等发布在https://www.cfca.com.cn/下载专区；证书可通过CFCA证书下载平台（https://cs.cfca.com.cn）等渠道获取；已被撤销的证书的信息可从证书中的CRL分布点查询；证书的状态信息可通过OCSP等服务获得。

本CPS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

CPS、CP以及相关业务规则在完成本CPS第1.5.4章节所述的批准流程后的15个工作日内发布到CFCA网站上；数字证书服务协议、相关的技术支持信息、证书链等在确认版本后，按照网站管理办法审批流程发布；发布在官方网站上的信息库确保7*24小时可访问；CRL至少每24小时发布一次，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网站上发布的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、CRL等信息对所有人可查阅、下载；证书信息可供订户及依赖方通过指定条件查

询。

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。

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项中，用于唯一标识证书主体。DN 项以个人、机构的法定证件上的名称、证件号码明确确定证书主体身份，能够把名称与唯一一个确定的实体（个人/组织机构/设备/域名等）联系起来，且使依赖方可识别。

对于个人证书主体甄别名称中的通用名通常可包含个人的真实名称或者证件号码，作为标识订户的关键信息被认证。

机构证书主体甄别名称中的通用名通常包含组织机构名称或组织机构的证件号码，作为标识订户的关键信息被认证。

设备证书中的甄别名称的通用名可以是订户所拥有的设备

名称、设备的 MAC 地址、IP 地址等，结合该订户的其他信息一起被鉴别和认证。SSL 服务器证书的甄别名称中的通用名可以是订户所拥有的域名或者 IP，结合该订户的其他信息一起被鉴别和认证。

密钥分散型证书的甄别名称包含注册机构标识、订户名称、唯一性标识等特征。

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,一经证实立即予以吊销。

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，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，详见《CFCA 数字证书数据构成规则》最新版本。在本 CPS 服务范围内该规则具有通用性，特定应用系统或者应用领域有特殊规则的，遵从其特殊规则（比如适用于人力资源社会保障领域的 DN 规则）。

3.1.5 名称唯一性

CFCA 保证在其某一个 CA 系统签发的证书 DN 具有可辨识唯一性。对于不同的申请主体，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。

3.1.6 商标的识别、鉴别和角色

用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。如订户提交的申请信息包含商标信息，则需要订户提交有关的商标注册文件，例如由政府机构出具的合法性证明文件。CFCA 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。当发生有关争议或纠纷时，CFCA 有权在必要时驳回相关证书申请或撤销已签发证书。

3.2初始身份确认

3.2.1 证明拥有私钥的方法

订户的签名公私钥对应在智能密码或者通过 GB/T 37092《密码模块安全要求》检测的密码模块中产生，为了证明订户拥有与注册公钥对应的私钥，订户的证书申请文件（CSR）中应包含其私钥的数字签名。CFCA 在为订户签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此

来判定订户拥有私钥。

3.2.2 订户身份的审查

RA 接受订户或其委托人的证书申请时，应对申请者提供申请信息进行审查，妥善保存与身份审查有关的材料和记录。CFCA 支持线下审查和线上审查。无论采取哪种审查方式，RA 机构都应妥善保管审查记录。

3.2.2.1 个人订户身份的审查

个人订户申请者应提供以下真实材料或信息:

（1）证书申请信息，包括但不限于证书主体信息、签名算法、有效期，以及使用的证书存储介质等，如订户未提供以上信息，证书主体信息使用订户法定证件上的信息，其他信息使用 RA 系统上的配置信息;

（2）个人有效身份证件或者包含经办人有效身份信息的电子数据。

对于个人订户身份的鉴别，采取以下鉴别方式:

(1)线下审查方式。个人订户在 RA 现场办理数字证书业务。

A. 个人订户应提供法定身份证件，RA 柜台应通过第三方权威可信数据源的核验方式，核验订户身份信息的真实性、完整性、准确性。

B. 如通过权威的可信数据源不能确认达到核验订户身份信息的真实性、完整性、准确性的目的，订户应提供其他法定有效证件，RA 柜台应进一步核验。

C. RA 柜台人员应确认订户提交的身份证件影像信息清晰、内容准确。

（2）线上审查方式。订户可通过 CA 在线申请平台、RA 机构的业务 APP、RA 机构的业务平台等在线办理数字证书业务。通过线上方式申请数字证书时，应对以下信息进行核验。

A. 核验订户法定证件的真实性、完整性、准确性，如线上系统通过第三方权威信息源进行核验。

B. 通过第三方权威信源不能核验其提供法定证件的真实性、完整性、准确性的，应辅助其他方式鉴别。

C. 应具备一种能体现订户意愿性的核验，比如短信验证码、邮件验证码、口令、生物识别码、视频、小额打款等任意一种方式。

3.2.2.2 机构订户身份的鉴别

机构订户申请者应指定合法授权代表提交证书申请。机构应提供以下真实材料或信息:

（1）证书申请信息，包括但不限于证书主体信息、密钥用法、有效期，以及使用的证书存储介质等；如订户未提供以上信

息，主体信息使用订户法定身份名称，其他信息使用 RA 系统上的配置信息；

（2）机构有效证件或包含机构确认的真实有效信息的电子数据；

（3）经办人授权委托书（加盖公章）或包含真实委托授权的电子数据；

（4）经办人有效身份证件或者包含经办人有效身份信息的电子数据。

RA 机构审查订户提交的材料。根据申请方式的不同进行鉴别，具体可以有以下几种申请及鉴别模式:

（1）线下方式。机构订户授权代表在 RA 现场办理数字证书业务。

A. 机构订户代表应提供机构法定证件，RA 柜台人员应实时通过第三方权威可信数据源，核验机构订户证件信息的真实性、完整性、准确性。

B. 如通过权威的可信数据源不能确认达到真实性、完整性、准确性核验的，机构订户代表应提供其他法定有效证件，RA 柜台应进一步核验。

C. RA 柜台人员应对机构订户授权信息进行确认，如肉眼不能确认授权信息的准确性、真实性时，可通过机构电话沟通等方

式确认。

D. RA 柜台人员应对机构订户授权代表个人信息进行核验，核验方式参考个人订户身份核验。

（2）线上方式。机构订户授权代表可通过 CA 在线申请平台、RA 机构的业务 APP、RA 机构的业务平台等在线办理数字证书业务。通过线上方式申请数字证书时，应对以下信息进行核验。

A. 订户法定证件（营业执照等）的真实性、完整性、准确性核验，如可利用线上系统应通过第三方权威信息源核验。

B. 通过第三方权威信源不能核验其提供法定证件的真实性、完整性、准确性的，应要求订户提供其他法定证件，并通过第三方权威信息源进行核验。

C. 机构订户意愿性的核验，如机构法人短信验证码、法人视频、机构账户小额打款等任意一种方式。

D. 线上系统应登记机构授权代表的身份信息及联系方式，对授权代表身份信息的核验参考对个人订户身份的核验。

3.2.2.3 设备证书信息的审查

申请设备证书时，除了提交申请者身份证明资料外，订户还应提交如下材料:

（1）证书申请材料;

（2）拥有设备标识/域名/IP 的所有权或控制权证明。

CFCA 除对申请者的身份、地址信息、国家信息等进行鉴别外，还要对域名或者 IP 进行鉴别。对域名的鉴别方法初步可通过域名注册信息查询（whois）功能，得到所申请服务器证书的域名注册者资料，查看域名注册者是否和服务器证书申请者一致，初步审核确定服务器证书申请者确实拥有此域名，如无法通过该方法验证，则继续通过如下鉴别方法（任选其一完成即可）：

（1）邮件验证。通过邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认订户对域名所有权或控制权。随机值应发送到标识为域名联系人的电子邮件地址或“admin”“administrato”“r”“webmaster”“hostmaster”或“postmaster”，后面是“@”之后跟着授权域名。

（2）文件验证。通过在“/.well-known/pki-validation”目录下对约定的信息进行改动，确认订户对域名/IP 的所有权或控制权。

（3）TXT 验证。通过在 DNSCNAME、TXT 记录中是否存在已约定的随机值，以确认订户对域名的所有权或控制权。

（4）ISP 服务商为其分配 IP 的证明材料。

3.2.2.4 其他证书类型的信息鉴别

密钥分散型证书申请时的核验，参照个人订户、机构订户线

上身份鉴别方式进行核验，同时应识别密钥分散型证书所使用的设备特征码。

3.2.2.5 批量申请的鉴别

机构如需批量申请证书，则需要向 RA 机构提交如下材料;

（1）批量申请证书的申请信息，包括但不限于证书主体名称、证件号码、证件类型、证件有效期等;

（2）机构获得每个证书主体的授权证明资料，如邮件授权、短信授权、手写签名授权等;

（3）机构有效证件或包含机构确认的真实有效信息的电子数据;

（4）机构给与经办人的授权委托书（加盖公章）或包含真实委托授权的电子数据;

（5）经办人有效身份证件或者包含经办人有效身份信息的电子数据。

批量申请中所包含的主体信息由批量申请机构负责审核，RA 机构仅对提出批量申请的机构进行审核，同时审核经办人的身份信息真实性、完整性、准确性，以及对委托书进行审查。审核方式同 3.2.2.1、3.2.2.2。

3.2.3 没有验证的订户信息

CFCA 不对订户申请证书中所体现的部门信息进行核验。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某一类型证书时， RA 应审核被授权人的身份和资格，包括被授权人的身份资料和授权证明，并且有权通过电话、信函或其他方式与授权人进行核实确认，以审核该授权行为的合法性。CFCA 有权通过第三方或其他方式确认被授权人的信息，亦有权要求被授权人提供授权证明等材料。

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

3.3.1 常规密钥更新的标识与鉴别

证书设置有效期的目的是为了尽量减少与证书关联的密钥

对的暴露风险，因此证书到期或者证书受损时，需要重新产生一对新的密钥对。证书密钥更新有两种情况：补发、换发。

（1）证书补发

补发是指在证书有效期内，存在以下情况时，订户需要申请证书补发：

A. 订户证书介质丢失或损坏，例如存放证书的智能密码钥匙（U 盾）损坏；

B. 订户认为证书密钥不安全（如订户怀疑证书被盗用或密钥受到了攻击）；

C. 其他经 CFCA 认可的原因。

当订户需要补发证书时，如订户申请资料与初次申请时一致，线上鉴别方式可通过向订户的手机发送验证码以及其他能够证明意愿性的方式来鉴别；线下鉴别方式与初次申请时一致。

证书补发时新证书失效日期与原证书失效日期一致。

（2）证书换发

换发是指在证书有效期到期前三个月内或证书过期后申请证书密钥更新的操作。证书换发时，订户应明确是否需要进行换发。

证书未过期时的换发核验，如果原证书在智能密码钥匙中，或者原证书不在智能密码钥匙中但能确定订户自己控制证书，则线上鉴别方式可以利用原证书的密钥对新申请数据所作的签名

进行核验。如果原证书未在智能密码钥匙中，且不能确定订户自己控制证书，则线上鉴别方式可通过向订户初始注册手机发送验证码以及其他能够证明意愿性的方式鉴别。证书未过期时换发证书，新证书有效期起始日期为证书换发申请时间，截止日期为原证书到期日再加一个证书有效周期。

当证书已过期时换发，如申请资料与初次注册时一致，且原证书在智能密码钥匙中，则可以参考未过期时的方法验证；如果原证书不在智能密码钥匙中，则线上鉴别方式可通过向初次注册时的手机号或邮箱发送验证码等用户参与方式鉴别。已经过期的证书换发证书时，其有效期仅为证书有效周期。

除服务器证书外，在补发或者换发申请提交至 CA 系统时，通常情况下将同步撤销原证书，并按照 CRL 规则发布 CRL；特殊项目可根据项目需要配置是否同步撤销老证书。服务器证书在补发或者换发申请之日起，30 日后撤销原有证书。

3.3.2 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户申请一张新证书，其身份鉴别要求与本 CPS 第 3.2.2 章节相同。

3.4撤销请求的标识与鉴别

证书撤销请求的标识与鉴别流程详见本 CPS 第 4.9 章节。

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，均可向 RA 提出证书申请，RA 机构也可为本机构提出证书申请。

自然人申请证书时其本人或者本人授权的代表为申请者；依法设立的组织申请证书时，其授权代表为申请者；RA 机构申请证书时，其授权代表为证书申请者。

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；用户申请数字证书时，须充分阅读告知内容，理解并接受 CFCA 公布的《数字证书服务协议》，该协议通过 CFCA 官方网站发布、在线业务系统弹窗、强制阅读、核心条款提示等任意一种方式出现。用户理解并同意各项事项后，提交真实有效的证书申请资料申请证书。如用户委托他人代替产生证书密钥及下载证书，应注意委托授权范围。

2、RA 机构应遵循 CFCA《注册机构运营管理办法》处理数字证书相关事项，对订户履行告知、审查、注册、妥善保管相关资料等义务。

RA 机构应在受理证书申请时，应采取适当措施，包括但不限于当面告知、书面签字告知、录音录像告知、系统页面展示等方式，使得订户充分知晓以下内容，并协助 CA 与订户签署协议:

（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、在用户同意协议的情况下，RA 可收集用户申请信息，按照本 CPS3.2 的方式进行审查。审查通过后，注册用户的信息。审查未通过的，应告知订户未通过原因。

4、订户信息完成注册后，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。

5、CA 应校验 RA 机构权限及证书申请格式，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，将签发的证书反馈给 RA 机构，RA 机构将证书转交给申请者。

6、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证书密钥及证书申请文件（CSR），利用下载凭证，通过 CFCA 证书下载平台下载证书。

7、无论通过何种方式获得证书，RA 机构均应协助订户与 CFCA 签订《数字证书服务协议》，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。在 CFCA 需要时，RA 机构应按照 CFCA 的要求，向 CFCA 提交订户身份审查记录。

8、订户应妥善保管数字证书，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，主动修改初始密码，并妥善保管。

9、CFCA 将不定期审查 RA 证书业务的合规性。

4.2证书申请处理

4.2.1 执行识别与鉴别程序

CFCA 处理证书申请按照本 CPS 第 3.2 章节要求，对证书申请进行审查。

4.2.2 证书申请批准和拒绝

RA 机构按照本 CPS 第 3.2.2 章节的要求对订户提交的申请材料进行鉴别。鉴别通过后，RA 机构可向 CA 提交申请，CA 为订户签发数字证书或证书下载凭证，经由 RA 机构反馈给订户。若鉴别未通过，RA 机构须拒绝其申请，于 2 个工作日内通知订户并告知拒绝原因。

被拒绝的订户可重新准备正确的材料，并再次提出申请。CFCA 根据内部管理制度，不定期复核 RA 机构提交的订户申请材料，并有权拒绝不符合本 CPS 的申请。

4.2.3 处理证书申请的时间

用户提交的申请材料真实、完整、准确并符合形式要求的情况下,RA 机构和 CA 机构需在 2 个工作日内完成证书申请的处理。如有特殊情况，可适当延长证书处理时间。

RA 机构和 CA 机构能否在上述时间范围内处理完成证书申请，取决于订户提供的申请信息及鉴别材料是否真实、完整、准确，以及是否及时响应了 RA 机构提出的管理要求。

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

RA 与 CA 建立安全通道，CA 接收到 RA 的证书申请后，对 RA

权限、证书申请格式、RA 签名等进行验证，验证通过后签发证书，并按照规则将证书发布至信息库。订户也可使用下载凭证(两码)，通过 CFCA 的官网下载平台下载证书，CA 系统接收到下载申请后，对两码进行核验，并对订户提交的申请进行格式及签名进行验证，通过后签发证书，并按照脱敏规则及发布频率将证书发布至信息库。

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,RA 或 CA 将通过当面、电话、短信、电子邮件、系统提示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

订户自行下载证书、委托他人获得证书或者通过 RA 获得证书等，应对证书信息进行核对。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，1 日内无异议的，视为已确认证书无误并接受证书；订户一经使用即视为订户已经接受此证书。

如订户有异议或者拒绝接受证书时，CA、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

对于证书申请者明确表示拒绝发布证书信息的，CFCA 将不发布该证书申请者证书信息；没有明确表示拒绝的， CFCA 按照脱敏规则及发布频率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

订户的私钥和证书应用于约定的、批准的用途（见本 CPS 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

依赖方在信赖交易对方的证书时，应验证对方证书是否属于CFCA签发、核验证书中的DN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，并对证书进行以下验证。

（1）通过适当并安全的途径，取得并安装CFCA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有效，包括：检查CFCA公布的最新CRL，确认该证书未被撤销；检查该证书路径中所有出现过的证书的可靠性；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。

以上任何一个环节失败，依赖方应该拒绝信赖该公钥及证书。

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 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老证书到期或者损坏等，保持原证书其他注册信息不变的情况下，生成新密钥对，重新申请一张新证书。

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 CFCA 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 CPS 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 CPS 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 CPS 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 CPS 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 CPS 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 CPS 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签发证书的订户以及与订户有关的RA可请求证书撤销。RA 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 CPS 第 4.9.1 章节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 CRL 发布策略即时发布 CRL。

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 CFCA 或 RA 判断出现本 CPS 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

当订户有撤销需要时，可立即发起撤销申请；如发现证书密钥泄露或怀疑证书不安全，应在知晓该安全隐患的 24 小时内向 RA 或者 CFCA 申请撤销。

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

CA、RA 将在收到撤销请求的 24 小时内进行响应，如果因密钥安全问题申请撤销证书，CFCA 将在 24 小时内完成处理，并按照规则发布 CRL、更新 OCSP 状态。

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

依赖方在信任此证书前应检查证书的有效性，检查证书是否被撤销。依赖方可通过以下两种方式获得证书状态:

（1）CRL 方式，依赖方通过解析证书域“CRL 分发点”获得 CRL 的发布地址，并在该地址下载 CRL 后，核验证书是否被撤销。

（2）OCSP 方式，依赖方可以利用 CFCA 提供的 OCSP 服务，实时验证证书的状态。

4.9.7 CRL 发布频率

本 CPS 所含系统发布的证书 CRL 信息，24 小时内至少更新一次。

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 提供在线证书状态查询（OCSP）服务，服务 7*24 小时可用。CFCA 至少每 12 个月更新一次根 CA 证书、中级 CA 证书的状态；如果根 CA 证书、中级 CA 证书被撤销，则将在 24 小时内更新 CA 证书状态。

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查询系统检查该证书的状态。

CFCA 的 OCSP 响应符合 RFC6960 标准。

4.9.10 撤销信息的其他发布形式

订户也可通过CFCA官方网站上提供的证书查询服务下载CRL。CFCA也可单独发布来自该注册机构申请证书的CRL。

4.9.11 对密钥遭受安全威胁的特别处理要求

订户、RA发现其密钥遭受安全威胁时，处理参见本CPS第4.9.4章节、第4.9.5章节处理。

CA的签名密钥遭受威胁时，CFCA将按照应急预案处理，并按照CFCA信息安全委员会决议,撤销该CA下所签发的所有证书。

4.9.12 证书冻结及解冻

不支持冻结及解冻操作。

4.10证书状态服务

4.10.1 操作特征

证书状态可以通过CFCA提供的CRL及OCSP服务获得。对于撤销的证书，在证书有效期内，每次签发CRL均包含该证书序列号；证书过期后，已撤销的证书将不在CRL中发布。

证书撤销后，也可通过OCSP服务查询其状态。

4.10.2 服务可用性

CFCA 提供 7*24 小时不间断证书在线状态查询服务及 CRL 下载服务。

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 依据国家密码管理部门的相关规定，为订户提供加密证书密钥的集中产生、保存和恢复。

密钥恢复是指加密密钥的恢复，CFCA 不提供签名密钥的恢复。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 CPS 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 数字证书支持服务

5.1集成支持服务

5.1.1 证书应用接口程序

CFCA 提供证书应用接口程序供应用系统集成和调用。证书应用接口程序符合《电子政务数字证书应用接口规范》，提供证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能。

证书应用接口程序支持 Windows、AIX、Solaris、Linux、麒麟、统信等多种系统平台，并提供 C、C#、Java 等多种接口形态，可通过 COM 组件、JAVA 组件、ActiveX 控件、Applet 插件等多种形态提供服务。

5.1.2 证书应用方案支持

CFCA 具备针对电子政务信息系统的电子认证安全需求分析的能力、电子认证法律法规、技术体系的咨询能力以及设计满足业务要求的电子认证及电子签名服务方案设计能力。

数字证书应用方案设计可包括：证书格式设计、证书交付、支持服务、信息服务、集成方案、建设方案、介质选型等。

5.1.3 证书应用接口集成

CFCA 具备面向各类政务应用提供证书应用接口集成能力，并达到以下要求:

具备在多种应用环境下进行系统集成的技术能力,包括基于 Java、.NET 等

B／S 应用模式和基于 C、VC 等 C／S 应用模式的系统集成能力。

提供满足不同应用系统平台的证书应用接口组件包，包括 COM 组件、JAVA 组件、ActiveX 控件、Applet 插件等。

提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示 DEMO 等。

证书应用接口为上层提供简洁、易用的调用接口，其主要包括密码设备接口和通用密码服务接口。

（1）密码设备调用接口

密码设备调用接口包括服务器端密码设备的底层应用接口和客户端证书介质(如: USBkey)的底层应用接口。

服务器端密码设备的底层应用接口符合《公钥密码基础设施应用技术体系密码设备应用接口规范》; 客户端证书介质的底层应用接口符合《智能 IC 卡及智能密码钥匙密码应用接口规范》。

（2）通用密码服务接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《电子政务电子认证服务应用接口规范》。

其主要包括服务器端组件接口和客户端控件接口。服务器端组件和客户端控件应支持不同电子认证服务机构所签发的符合《电子政务数字证书格式规范》的数字证书。

CFCA为电子政务应用单位提供证书应用接口程序集成工作。集成工作提供以下服务:

（1）证书应用接口的开发包(包括客户端和服务器端);

（2）接口说明文档;

（3）集成演示 Demo;

（4）集成手册;

（5）证书应用接口开发培训和集成技术支持;

（6）协助应用系统开发商完成联调测试工作。

5.2信息服务

信息服务是面向证书应用单位提供证书发放和应用情况信息汇总及统计分析的信息管理服务。根据证书应用单位对证书应

用信息的管理及决策需求，CFCA 为证书应用单位提供相应的信息服务，为其实现科学管理和领导决策提供可靠依据。本项是在第 2 章节基础上，进行的更详细的描述。

5.2.1 服务内容

CFCA 提供的信息服务包括:

（1）证书信息服务

CA 系统中签发、更新、重签发的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。

（2）CRL 信息服务

CA 系统签发 CRL 信息后，可实现将 CRL 实时发布到指定的电子政务信息系统中。CFCA 提交的数据包括业务类型、电子认证服务机构身份标识、CRL 文件、同步时间等。

（3）服务支持信息服务

CFCA 面向电子政务用户、应用系统集成商、应用系统发布与之相关的服务信息，包括 CPS、常见问题解答、证书应用接口软件包等。

（4）决策支持信息服务

CFCA 面向电子政务应用单位、政府监管机构提供决策支持

信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

5.2.2 服务管理规则

CFCA 在提供信息服务时，有相应的信息隐私保障机制，确保用户的私有信息不被泄漏。具体参见 9.4 章节个人信息保护。除个人敏感信息需要保护外，政府部门的敏感信息和工作秘密也将按照保密制度进行保护。

所有载明在证书里的涉及个人敏感信息的，CFCA 将进行脱敏处理。

允许的私有信息采集：CFCA 仅在进行证书发行和管理时才能收集私有信息。除了有特殊要求目的外，CFCA 不会收集更多私有信息。

允许的私有信息使用：CFCA 只使用 CA 或者 RA 收集的私有信息。

允许的个人信息发布：CFCA 及其 RA 仅在获得订户同意的情况下，向电子政务证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。

在特别紧急情况下，CFCA 经具有执法权力的相关管理机构的同意，可以发布私有信息。但任何特定的私有信息程序的发布遵照相关的法律和政策实行。

所有者纠正私有信息的机会：CFCA 允许用户在其证书生命周期内对其私有信息进行更正。

证书应用单位访问信息的限定：对证书应用单位的管理员设定信息访问权限，限定其仅能访问来自本应用申请所签发的证书信息。应用单位管理员对非授权信息的访问，须依照政策管理规定，经上级主管部门批准后方可进行。

对司法及监管机构发布私有信息：CFCA 或者注册机构在收到以下命令时，可以执行将私有信息发给获得相应授权的人员：

（1）司法程序；

（2）经私有信息所有者同意；

（3）按照明确的法定权限的要求或许可。

对问责程序需要进行的信息访问，CFCA 将严格审核相应的问责人员身份及授权文件，无误后方可进行问责举证。对监管部门应管理需求进行的信息访问，CFCA 将按照相关的管理规定和调取程序，为其提供信息访问权限。

5.2.3 服务方式

CFCA 的信息服务以网站（https://www.cfca.com.cn）或接口的形式面向应用系统或证书用户提供服务，包括证书信息同步服务、CRL 信息同步服务等，以接口形式提供的服务符合《电子政务数字证书应用接口规范》的要求。

（1）服务支持信息服务

CFCA 通过网站（https://www.cfca.com.cn）向电子政务用户提供 2.1 所示的信息服务；面向电子政务应用系统集成商，CFCA 直接提供如下信息：

数字证书应用接口软件包；

数字证书应用接口实施指南

证书常见问题解答(FAQ)

获得证书帮助联系方式(客户服务热线电话、办公地址、邮政编码、投诉电话等)

其他应该发布的相关信息。

面向电子政务应用系统，CFCA 提供如下信息服务：

时间戳服务数据接口；

HTTPS 协议的 CRL 发布服务接口：

OCSP 服务接口。

（2）决策支持信息服务

CFCA 向应用提供方以服务报告方式提供如下信息服务：

用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务。

投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析。

客户满意度信息：提供面向业务的客户满意度调查信息。

服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

5.3使用支持服务

5.3.1 服务内容

CFCA向用户及证书应用客户提供的使用技术支持服务包括：数字证书管理、数字证书使用、证书存储介质硬件设备使用、电子认证软件系统使用、电子认证服务支撑平台使用以及各类数字证书应用(如证书登录、证书加密、数字签名)等贯穿证书使用和应用过程中的所有问题。

面向订户的服务支持

（1）数字证书管理

数字证书的导入、导出、客户端证书管理工具的安装、使用、卸载等。

（2）数字证书应用

数字证书用于身份认证、电子签名、加解密等应用出现的证书无法读取、签名失败、证书验证失败等应用问题。

（3）证书存储介质硬件设备使用

证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

（4）电子认证服务支撑平台使用

数字证书在线服务平台应用问题，如：证书更新失败、下载异常、无法提交注销申请等。

面向应用提供方的服务支持

（1）电子认证软件系统使用

提供受理点系统、注册中心系统、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

（2）电子签名服务中间件的应用

解决服务中间件在集成时出现的诸如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

5.3.2 服务方式

（1）座席服务

CFCA 提供 7*24 热线服务：400-880-9888。

（2）在线服务

CFCA 提供自助信息查询系统、网络实时通讯系统、远程终端帮助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

自助信息查询系统

将知识库信息、按照不同的类型、属性、层次等方式、结构进行分类存储，用户可以按照咨询问题或者已知条件在信息系统上进行启发式的检索，查找目标问题的答案。

网络实时通讯系统

用户可通过网络实时通讯工具与 CFCA 支持帮助人员取得联系，进行交流。

远程终端协助系统

用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软硬件环境，通过同屏显示指导、帮助用户解决应用故障。

在线帮助与传统模式的结合

将在线服务系统与电话服务结合，方便客户既可以打电话，也可自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

（3）现场服务

根据政务客户系统的实际情况，必要时由技术支持工程师现场为用户处理数字证书应用中存在的问题。

（4）满意度调查

CFCA 通过多种用户可接受的多种调查方式进行客户回访，包括电话、WEB 网站、邮件系统、短信、传真等，并每月出具用户满意度调查报告。

CFCA 将用户回访中产生的相关文档进行归档、保存。

（5）投诉受理

用户可通过 400-880-9888 客户热线、专用投诉电话（010-80864105）、电子邮件、即时通讯工具等方式进行投诉，CFCA 将在投诉受理过程中记录投诉问题，将投诉受理中产生的相关文档进行归档、保存，并将结果及时反馈给用户。

（6）培训

培训方式可以由 CFCA 与客户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答(FAQ)、操作手册等。

5.3.3 服务质量

CFCA 的热线服务（400-880-9888）为 7*24 小时热线服务；

在线服务、现场服务为 5*8 小时服务;

在有应急服务需求的特殊情况下，CFCA 提供及时的服务。

CFCA 对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定了响应处理流程和机制，确保服务的及时性和连续性。技术支持响应时间以最大程度不影响客户使用为准则。

6 认证机构设施、管理和操作控制

6.1物理控制

6.1.1 场地位置与建筑

CFCA 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、电磁屏蔽、门禁控制、视频监控等功能，可禁止未经授权的访问并保证基础设施的物理安全性。

6.1.2 物理访问

外来人员进入楼内，需经过中国银联自有物业、CFCA 的两道审核，进入 CFCA 办公区域要经过两道门禁系统，需要有 CFCA 工作人员陪同进入。

CFCA 的 CA 机房及办公场地所有人员均持有标识身份的工牌。进出 CA 机房人员的门禁权限由 CFCA 安全管理人员根据安全策略批准授权。

授权人员进入 CFCA 综合机房，须经过指纹加门禁卡身份认证，并有 7*24 小时视频监控设备进行监控。授权人员进入安全区机房，须经过三道双人指纹加门禁卡身份认证，所有门禁的访问信息均有记录。

6.1.3 电力与空调

CFCA 机房采用 UPS 供电，由两组每组三台 UPS 线路供电，每组 UPS 均能保证系统持续运行 15 分钟以上；门禁和入侵报警系统的 UPS 供电可持续运行 8 小时。为了保证系统的可靠运行，还备有柴油发电机，当外部供电中断时，能够继续对机房实施供电。

CFCA 机房采用多台机房精密空调，保证机房内温度和湿度按照国家标准（GBJ19-87《采暖通风与空气调节设计规范》、GB50174-2008《电子信息系统机房设计规范》、GB50174-93《电子计算机机房设计规范》）。

6.1.4 水患防治

CFCA 有专门的技术措施防止、检测漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

6.1.5 火灾防护

CFCA 机房采用防火材料建设，安装有中央防火监控和自动气体消防系统，并通过了国家权威部门的消防功能验收，能有效地避免火灾威胁。

6.1.6 介质存储

对于存放重要数据的存储介质，CFCA 制定了专门的管理控制制度，以防止重要信息的泄露与人为故意产生的危害和破坏。

6.1.7 废物处理

敏感的文件资料（包括纸介质、光盘或软盘等）抛弃前要进行粉碎处理；对于存储或传输信息的介质，在抛弃前要做不可读取处理；涉密介质在抛弃前要根据生产商的指导做归零处理。加密机等重要设备废弃根据《加密机管理办法》销毁；本项下的所有废物处理均留存处理记录。

6.1.8 灾备中心

根据 GB/T 20988《信息安全技术信息系统灾难恢复规范》定义的灾难恢复等级第 5 级（实时数据传输及完整设备支持）的要求，建立了同城灾备中心，采用远程数据复制技术，并利用专线实时复制到灾备中心。

6.2程序控制

6.2.1 可信角色

CFCA 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角色及影响 CA 密钥安全管理职责的视为可信角色，包括:

（1）审查与客户服务人员，负责客户证书业务相关的支持服务以及订户申请信息鉴别操作;

（2）安全管理人员，负责物理场地安全、日常安全管理以及安全策略管理、安全审计工作的人员;

（3）密钥与密码设备管理人员，负责密钥管理、密码设备管理的人员;

（4）系统维护人员，负责对 CA 系统进行日常操作、维护的人员;

（5）人力资源管理人员，负责可信角色审查的人员。

6.2.2 每项任务需要的人数

CFCA 制定了规范的策略，严格控制任务和职责的分割，对于最敏感的操作，例如访问和管理 CA 的加密设备及其密钥，需要 3 个可信角色。

其他操作，例如对 CA 系统的任何操作，需要至少 2 个可信

角色。

CFCA 对于人员有明确的分工，贯彻互相牵制、互相监督的安全机制。

6.2.3 每个角色的识别与鉴别

CFCA 在雇用一个可信角色之前将按照本 CPS 第 6.3.2 章节的规定对其进行背景审查。

对于物理访问控制，CFCA 通过门禁卡、指纹识别鉴别不同人员，并确定相应的权限。

CFCA使用数字证书认证和订户名/口令方式对可信角色进行识别与鉴别，系统将独立完整地记录所有操作行为。

6.2.4 需要身份分离的角色

要求身份分离的角色包括（但不限于）以下几种:

安全管理员、系统和应用管理员、数据库管理员、网络管理员、操作员、订户信息收集人员、订户身份及信息核验人员、制证人员。

6.3人员控制

CFCA 按照以下要求进行人员管理及控制。

6.3.1 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。

6.3.2 背景审查程序

CFCA 在开始一个可信任角色的雇佣关系前会依据以下流程对其进行审查:

（1）应聘者应提交的个人资料

履历、最高学历毕业证书、学位证书、资格证及身份证等相关的有效证明。

（2）应聘者个人身份的确认

CFCA 人力资源部门通过电话、信函、网络、走访、调阅档案等形式对其提供材料进行审查。

（3）三个月的试用期考核

通过现场考试、日常观察、情景考验等方式对其考察。

以上三方面的审查结果应符合本 CPS 第 6.3.1 章节中规定的要求。

（4）签署保密协议

与到岗人员签署保密协议。

（5）上岗工作

6.3.3 培训要求

CFCA 建立有培训制度，每年按照制度制定培训计划，培训包含 CFCA 从事电子认证服务的人员以及注册机构。培训内容包括：PKI 的相关知识、本 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。按照管理体系要求，规范记录培训考核及培训资料。

6.3.4 再培训周期和要求

CFCA 每年至少向员工提供一次业务培训机会以不断提高其职业技能，以保持其完成工作所需要的职业水平。同时，当本 CPS 进行更新、CA 系统更新升级后，也将安排对相关员工进行相应的培训。

CFCA 根据对注册机构的评估情况，灵活安排对注册机构的培训周期。

6.3.5 未授权行为的处罚

一旦发现员工执行了未经授权的操作时，将被立即中止工作并受到纪律惩戒，其处理办法根据 CFCA 相关的管理制度执行。

6.3.6 独立合约人的要求

CFCA 在雇用独立合约人时，会要求提供身份证、学历证书、资格证书等有效证明，并需与 CFCA 签署保密协议，执行与 CFCA 正式员工同等的培训政策。

6.3.7 提供给员工的文档

CFCA 向其员工提供完成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。

6.4审计日志程序

6.4.1 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(如终端、端口、地点、客户等);

5) 生成日志条目的实体身份。

CFCA 记录的日志信息包括但不限于以下类型:

（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）新系统上线工单、系统变更工单、业务操作工单、网络变更工单、数据提取工单、故障处理记录；

（6）人员访问控制记录、监控记录；

以上记录均包含日期、时间、记录实体、记录号等。

6.4.2 处理日志的周期

CFCA 对上条中类型（1）的日志由密钥管理员收集并管理；类型（2）的日志保存在数据库，每日进行一次增量备份，每周进行一次全备份；类型（3）和类型（4）的日志每日自动保存在备份设备上；类型（5）的日志保存在工单系统；类型（6）的日志保存在文档共享管理系统。

CFCA 按照内部管理措施，定期核查记录的完整性。对警告、故障等进行及时处理，并保持处理记录。

6.4.3 审计日志的保存期限

本 CPS6.4.1 中的事件记录类型（1）的日志保存至 CA 密钥失效后 5 年；类型（2）的日志至少保存到证书失效后 5 年，其他日志至少保存至一个评估周期（1 年）后。

6.4.4 审计日志的保护

CFCA 建立了相应的管理制度，并采取物理和逻辑的控制方法确保只有经 CFCA 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。

6.4.5 审计日志备份程序

CFCA 将按照其《日志管理办法》及《数据备份管理办法》执行备份操作。

6.4.6 审计收集系统

日志收集系统涉及 RA、CA、KM 系统、数据库、堡垒机、备份系统等。

6.4.7 对导致事件主体的通告

对于审计收集系统中记录的事件，对导致该事件的个人、机构等主体，CFCA 不进行通告。

当 CFCA 发现被攻击时，将记录攻击者的行为，并在法律许

可的范围内追溯攻击者。CFCA 保留采取相应对策措施的权利。CFCA 有权决定是否对导致事件的相关实体进行通告。

6.4.8 脆弱性评估

CFCA 在系统变更时应对变更操作进行安全评估，同时按照规则定期进行系统、物理设施、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

6.5记录归档

6.5.1 归档记录的类型

CFCA 的归档记录包含以下类型:

（1）电子认证服务机构接收外部评审的资料，包括等级保护测评、信息安全体系认证等外部评审资料;

（2）电子认证服务机构的 CPS、CP 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。

6.5.2 归档记录的保存期限

CFCA 针对证书相关的归档记录将保存至证书失效后 5 年。

6.5.3 归档文件的保护

CFCA 对归档文件有相应的管理制度。

对于电子形式的归档记录文件，确保只有被授权的可信任人员才允许访问存档数据，并通过适当的物理和逻辑访问控制防止对电子归档记录进行未授权的访问、修改、删除或其他操作。CFCA 将使用可靠的归档数据存储介质和归档数据处理应用软件，确保归档数据在其归档期限内只有被授权的可信任人员才能成功访问。

对于纸质书面形式的归档记录文件，CFCA 制定了相应的档案管理办法，并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。

6.5.4 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。

数据库备份：采用本地备份和异地备份、增量备份与全备份相结合的方式进行备份。

操作系统日志的备份：每日自动进行一次备份，保存到集中备份服务器。

应用日志的备份：每日自动进行一次备份，保存到集中备份服务器。

6.5.5 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。

6.5.6 归档收集系统

CFCA 有自动的电子归档信息的存放系统。

6.5.7 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。

6.6电子认证服务机构密钥更替

当 CA 密钥对的寿命即将超过本 CPS 第 6.3.2 章节中规定的最大有效期时，CFCA 将启动密钥更新流程，替换即将过期的 CA 密钥对。CFCA 密钥变更按如下方式进行:

（1）一个上级 CA 应在其私钥到期时间小于下级 CA 的有效期之前停止签发新的下级 CA 证书（“停止签发日期”）;

（2）产生新的密钥对，签发新的上级 CA 证书;

（3）在“停止签发日期”之后，对于批准的下级 CA 或最终订户的证书请求，将采用新的 CA 密钥签发证书;

（4）用于签发订户证书的 CA 在其私钥到期时间小于订户证书最长有效期时停止签发订户证书，产生新的密钥对，生产新的子 CA 证书。

CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

6.7损坏与灾难恢复

6.7.1 事故和损害处理流程

当 CFCA 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，CFCA 将根据其制订的业务连续性计划等相关规章制度采取合理措施。

业务持续计划由 CFCA 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、发布业务持续计划，根据实际情况决定启动灾难恢复等各项职能。

业务中断事件分普通紧急事件和灾难事件。当服务中断发生后，该中断对客户服务产生重大影响，但恢复服务不受外界因素的影响，短时间内即可恢复服务，这类事件称为普通紧急事件；当服务中断因不可抗力因素造成，比如自然灾害、传染病、政治暴动等因素引起的事件称为灾难事件。

CFCA 针对不同事件制定了相应的应急处理机制。

当发生普通紧急事件后，CFCA 信息安全委员会负责人召集 CFCA 信息安全委员会成员举行会议，对事件进行评估。相关职能部门按照 CFCA 信息安全委员会确定的处理措施进行处置。在普通紧急事件应急处置后，CFCA 将评估已有风险防范措施的有效性并加以改进。

当发生灾难事件时，按照本 CPS 第 5.7.4 章节的规定进行。

对于灾难性事件，在主运营场地出现灾难事故或不可抗力事故而不能正常运营时，CFCA 将在 48 小时内，利用备份数据和设备在灾备数据备份中心恢复电子认证服务。

CFCA 具有专门的问题报告和响应机制：CFCA 向订户、依赖方、软件开发商和其他的第三方提供 7*24 服务热线（400-880-9888），说明如何向 CFCA 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。

CFCA 将在接收到问题报告的 24 小时内开始进行调查，并至少根据以下的条件来判断是否采取撤销或其他相应手段:

1）问题的性质;

2）收到的对特定证书或网站问题报告数量;

3）投诉人的身份;

4）相关的法规。

CFCA 可确保全天候（7*24 小时），对高优先级的问题报告首先在 CFCA 内部进行响应，在有必要时将这些问题提交给法律机构解决或执行证书的撤销。

6.7.2 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，将依据本 CPS 第 5.7.1 章节中的规定区分是普通紧急事件还是灾难事件，按照不同的事件类型分类根据相应的处理流程进行处理。

6.7.3 实体私钥损害处理程序

CFCA 制定了 CA 私钥泄露的应急预案，其中明确规定了 CA 私钥泄露的内部处理流程、人员分工及对外通知处理流程。

当 CFCA 证实 CA 私钥发生泄露时，将会立即上报行业主管部门，说明发生 CA 私钥泄露的时间、原因以及采取的应急处理措

施。

CFCA 一旦证实 CA 私钥泄露时，会立即通过官网等方式通知订户及依赖方，对所有证书进行撤销，并不再签发新的证书。

6.7.4 灾难后的业务连续性能力

在主运营场地出现灾难事故或不可抗力事故而不能正常运营时，CFCA 将在 48 小时内，利用备份数据和设备在灾备数据备份中心恢复电子认证服务。CFCA 每年按照计划进行演练。

6.8电子认证服务机构或注册机构的终止

CFCA 授权的注册机构终止服务时，将按照《注册机构运营管理规范》执行下线操作，并合理安排注册机构承接事务。

CFCA 拟暂停或终止电子认证服务时，将在暂停或终止电子认证服务 90 日前，就业务承接及其他有关事项通知订户、依赖方、注册机构等有关各方。

CFCA 将在暂停或终止电子认证服务 60 日前向行业主管部门报告，办理电子认证服务资质的注销手续，并与其他电子认证服务机构就业务承接进行协商，做出妥善安排。

若 CFCA 未能就业务承接事项与其他电子认证服务机构达成协议，将申请行业主管部门安排其他电子认证服务机构承接相关业务。

行业主管部门对此有其他相关要求的，CFCA 将严格按照行业主管部门的要求进行。

7 认证系统技术安全控制

7.1密钥对的生成和安装

7.1.1 密钥对的生成

（1）CA 密钥对的生成

CA 的密钥对在加密机内部产生，加密机通过 GB/T 37092《密码模块安全要求》标准三级及以上等级商用密码产品认证。CA 密钥的生成、使用、存储、备份、销毁等全生命周期安全管理符合 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 8.2.4 章节的要求。

对于证书根密钥生成需要有独立审计人员的现场参加，现场见证 CA 根密钥生成的过程，对以下内容发表意见:

制定根密钥生成计划描述详细的根密钥生成流程和步骤;

根密钥生成和密钥安全保护流程符合 CPS 和 CP 的要求;

根密钥生成过程中执行了计划要求的所有流程和步骤;

根密钥的生成过程需要用录像记录，作为今后的审核证据。其他 CA 的密钥控制参照上述要求进行。

（2）订户密钥对的生成

订户密钥包含订户签名证书密钥对及订户加密证书密钥对。

订户的签名证书密钥对的生成由订户负责，订户可通过智能密码钥匙（如 USBkey）或通过 GB/T 37092《密码模块安全要求》检测的其他密码模块生成签名证书密钥对。订户应确保其密钥产生的可靠性，并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。

订户的加密证书密钥对由 CFCA 的密钥管理系统生成，并通过安全的方式传输给订户。CFCA 的密钥管理系统通过国家密码管理局安全审查，负责为电子认证服务订户提供产生、备份、恢复加密证书密钥等服务。

密钥分散证书的签名密钥对由订户终端和云服务端协同运算生成。云服务端和订户终端的密钥因子由通过商用密码产品检测认证的密码模块中生成，订户终端的密钥因子可由终端设备信息、用户知晓的信息（例如用户设置的 PIN）、随机数等运算生成。

CFCA 可在订户需要时提供相应的技术支持帮助订户按照正确的流程生成密钥，CFCA 将拒绝弱密钥申请数字证书。

7.1.2 私钥传送给订户

订户的签名私钥由订户自己生成时将不会进行传送，由 CFC

A 生成时将离线或者在线安全方式传递。订户委托其他产生私钥时，受托方需确保私钥在交付给订户前未被使用。订户委托其他主体产生、保管、使用私钥时，应定期关注受托方是否按照委托范围执行操作。

7.1.3 公钥传送给证书签发机构

订户可通过 CFCA 提供的下载服务建立的安全通道将公钥证书发送给 CFCA，或者通过 RA 系统发送给 CA 系统。

7.1.4 电子认证服务机构公钥传送给依赖方

用于验证 CFCA 签名的验证公钥（证书链）以及证书状态等信息可从 CFCA 的信息库获得。

7.1.5 密钥的长度

密码算法及长度符合国家密码管理部门的相关规定；CFCA 将根据国家相关部门及政策要求，拒绝弱密钥长度数字证书的申请。

CA 证书密钥长度为 SM2-256；订户证书密钥长度应小于等于 CA 的密钥长度，通常为 SM2-256。

7.1.6 公钥参数的生成和质量检查

公钥参数由通过密码认证的密码设备生成，CFCA 在采购这

类设备时，需要供货方设备具备相应等级的密码认证证书。对生成的公钥参数的质量检查标准，CFCA 认可这些设备内置的协议、算法等均已达到标称的安全等级要求。

7.1.7 密钥使用目的

证书密钥使用的目的，通过 X.509 证书域“Key Usage”密钥用法来体现。根 CA 私钥用于签发自身证书、下级 CA 证书和 CA 的撤销列表，OCA 证书用于签发订户证书和 CRL，证书的公钥用于验证私钥签名。

订户证书依据用途配置密钥用法（KU）及增强密钥用法（EKU），即，用于数字签名（包括身份验证）的证书将设置数字签名及/或抗抵赖的密钥用法，用于密钥或数据加密的证书将设置密钥加密及/或数据加密的密钥用法，用于密钥协商的证书将设置密钥协商的密钥用法。

当订户需要同时使用签名及加密的密钥用法时，CFCA 将为订户颁发双证书（签名证书、加密证书）。

根 CA 私钥不得用于签署订户证书。

7.2私钥保护和密码模块工程控制

7.2.1 密码模块标准和控制

CFCA CA 系统生成密钥的密码模块（加密机）安置在 CFCA

核心区域，使用通过商用密码产品认证的加密机，且至少符合 GB/T 37092《信息安全技术 密码模块安全要求》三级及以上。

CFCA 制定有专门的《加密机管理办法》，从采购、验收、进入机房、初始化、激活使用、备份、维护、销毁等环节进行了规范化审批管理。加密机仅与对应系统连接，存放在屏蔽机房内。

7.2.2 私钥多人控制

CFCA CA 密钥由加密机产生并存放，产生过程有成型的操作脚本，且操作脚本通过相关领导的审批。加密机的激活数据由 5 人分持管理，且激活数据存储在智能密码钥匙或智能 IC 卡中。智能密码钥匙分别由 5 位经过授权的安全管理员掌握，并保存在屏蔽机房内最安全区的保险箱中。当激活 CA 私钥时，应由 5 个安全管理员中的 3 个人员同时在场方可使用，从技术及制度上保证了敏感加密操作的安全性。

7.2.3 私钥托管

CFCA CA 私钥均未在其他地方托管，CFCA 密钥管理系统不提供订户签名私钥托管服务。订户加密证书私钥由 CFCA 密钥管理系统产生保管，密钥管理系统符合商用密码管理规定。

7.2.4 私钥备份

CA 的私钥由 5 选 3 名安全管理人员操作备份，备份操作与

密钥产生具备相同的操作脚本，备份保存在机房最安全区的保险柜内。

7.2.5 私钥归档

当 CFCA 的 CA 密钥对到期后，将至少保存 5 年。归档的 CA 密钥对按照本 CPS 第 6.2.4 章节所述的措施进行保管。CFCA 的密钥管理策略和流程确保归档后的 CA 密钥对不会被再次用于生产系统中。当归档 CA 密钥对达到归档保存期限之后，CFCA 将按照本 CPS 第 6.2.10 章节所述的方法进行安全销毁。

CFCA 为订户产生的加密私钥的归档由密钥管理系统按照策略执行归档，归档至少保存至证书过期后 5 年。

7.2.6 私钥导入、导出密码模块

CA 私钥由加密产生，为保证服务的可靠性，CA 私钥在产生后同时需要导出、导入备份加密机内，导入导出操作按照 5 选 3 机制由多人操作完成，操作与产生一样按照既定的脚本操作，并保持操作记录。

7.2.7 私钥在密码模块的存储

CA 私钥以密文的方式存放在通过商用密码认证的密码模块中。

7.2.8 激活私钥的方法

CFCA 采用硬件设备（加密机）产生、保存 CA 私钥，其激活应由具有权限的，5 选 3 人使用其 IC 卡或者智能密码钥匙操作激活。一旦 CA 私钥被激活，激活状态将保持到 CA 离线。

7.2.9 解除私钥激活状态的方法

对于 CA 私钥，当硬件密码模块断电或重新初始化时，私钥进入非激活状态。其他情况下的非激活状态，需要 5 选 3 安全管理员操作解除私钥激活状态。

7.2.10 销毁私钥的方法

当 CA 的生命周期结束后，CFCA 将根据本 CPS 第 6.2.5 章节相关规定将 CA 私钥归档，其他的 CA 私钥备份将被安全销毁。归档的私钥在其归档期结束后，需要在 3 名以上可信人员参与下进行安全销毁，并保持安全销毁记录。

7.2.11 密码模块的评估

CFCA 使用通过商用密码产品检测认证的加密机设备，密码模块至少需要满足密码模块安全要求三级要求，并定期对密码模块的安全性进行评估。

7.3密钥对管理的其他方面

7.3.1 公钥归档

公钥归档的保存期限、保存机制、安全措施等与证书保持一致。归档要求参照本 CPS 第 5.5 章节的相关规定。

7.3.2 证书操作期和密钥对使用期限

CA 用于签发用户证书的密钥有效期不超过 30 年，订户证书有效期最长不超过 5 年 3 个月。

CA 密钥对使用期限和 CA 证书的有效期保持一致。

订户证书的密钥对使用期限和订户证书的有效期保持一致。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。加密证书的加密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，直到密钥对存在被破解的风险，如加密算法被破解。

7.4激活数据

7.4.1 激活数据的产生和安装

CFCA 用于保护 CA 私钥的激活数据，在 CA 私钥产生时的操作脚本控制下产生，由智能密码钥匙或智能 IC 卡产生，经授权的 5 名安全管理员分持，产生后保存在最安全区的保险柜内。

7.4.2 激活数据的保护

CFCA 的 CA 密钥激活数据，由 5 名可信安全管理员分持，保存在最安全区的保险柜内，保险柜的密钥由其他两位安全管理员分持口令管理。CA 密钥激活数据安全管理员需要使用激活数据时，应填写申请单经相关领导审批后，由保险柜管理员按照操作脚本分发给 5 位中的 3 位安全管理员。

存放CA激活数据的智能密码钥匙或者智能IC卡需要用口令保护，口令至少是 8 位非弱口令。

7.4.3 激活数据的其他方面

7.4.3.1 激活数据的传输

存有 CA 私钥的加密设备和相关智能密码钥匙，保存在 CFCA 最安全区机房。如在某种特殊情况下需要进行传输时（如建设灾备系统时），其传输过程需要在 CFCA 安全管理人员和密钥管理人员共同监督的情况下进行，并全程录像记录。

7.4.3.2 激活数据的销毁

CFCA 通过对设备进行初始化的方式来销毁 CA 私钥的激活数据。

7.5数据安全控制

7.5.1 制定安全方案确保数据安全目标

（1）CFCA 将采取授权访问的策略和加密签名的手段，确保对 CA 的控制和证书申请等相关数据以及证书的相关流程的机密性、完整性和可用性，确保其不受到未经授权或非法的访问、使用、披露、修改或销毁，保护其不受到意外的丢失、销毁或损坏，以及不受到可预见的威胁和破坏;

（2）确保验证“证书数据”、签发证书、维护信息库和撤销证书的密钥、软件和流程的机密性、完整性和可用性;

（3）CFCA 将确保其维护的数据符合相应法律规定的其他安全要求。

7.5.2 安全方案定期风险评估

（1）CFCA 采取定期的风险评估策略，识别可预见的使“证书数据”和“证书流程”受到未经授权的访问、错误使用、披露、修改或销毁的内部/外部威胁;

（2）风险评估将根据“证书数据”和“证书流程”的敏感程度评估所识别威胁因素发生的可能性和发生后预计造成的破坏程度;

（3）每年将定期评估 CA 用于控制这些风险的制度、流程、

信息系统、技术、人员或其他因素是否足够。

安全计划

CFCA 将根据风险评估结果制定安全计划，内容包括制定、实施并维护安全流程、措施以及为数据安全设计的产品。根据“证书数据”和“证书流程”的敏感程度以及操作流程的复杂程度和范围，合理的管理和控制所识别的风险。安全计划包括与 CA 业务、“证书数据”和“证书流程”的规模、复杂程度、性质和范围相适应的行政、组织架构、技术和物理环境的安全控制措施。制定安全控制措施时，考虑今后可用的技术和相应的成本；安全控制措施程度应与缺失该控制可能造成的破坏以及该控制所保护数据的性质相符合。

7.6计算机安全控制

7.6.1 特别的计算机安全技术要求

CFCA 的信息安全管理符合国家相关规定，主要安全技术和控制措施包括：采用安全可信任的操作系统、严格的身份识别和人员访问控制制度、多层防火墙设置、人员职责分割、双人操作控制、系统登录通过双因子认证、所有系统操作均通过堡垒机进行安全审计记录。

7.6.2 计算机安全评估

CFCA CA系统已通过国家密码管理局等有关部门的安全性审查，获得了相应资质。

每年对信息系统进行风险评估，并按照等级保护测评三级要求执行测评。

7.7生命周期技术控制

7.7.1 系统开发控制

CFCA的开发环境通过了商用密码产品的工厂检查，开发的数字证书认证系统（CA系统）获得了商用密码产品认证资质，其开发过程符合国家密码主管部门的相关要求。

CFCA开发环境与生产运营环境物理隔离，软硬件产品的开发过程、采购过程、上线过程均有授权控制、漏洞扫描等控制记录，安全管理过程符合ISO 27001的相关要求。

7.7.2 安全管理控制

CFCA CA系统的信息安全管理，严格遵循行业主管部门的规范进行操作，公司具有相关变更操作管理制度及定期的安全审计制度，系统的任何变更都经过严格的测试验证后才能进行安装和使用，任何未经授权的操作均可通过审计检查发现。

CA 系统的软硬件产品采购、上线使用等均具有相关管理办法，在系统上线前清楚缺省配置，关闭不需要的端口等。

同时，按照 ISO 9000 质量管理体系及 ISO 27001 信息安全管理体系标准建立了严格的管理制度，并每年进行监督检查及认证。

7.7.3 生命期的安全控制

CFCA 制定有日常的审计制度、年度信息安全等级保护测评、年度信息安全管理体系监督检查等多项机制，保证 CA 系统生命周期各环节的合规要求及系统可靠运行。

7.8网络的安全控制

CFCA CA系统通过以下手段来防止网络受到未授权的访问和抵御恶意攻击:

（1）由防火墙对来自外部的访问信息进行过滤控制;

（2）将功能独立的服务器放置在不同的网段;

（3）多级防火墙划分不同网段，并采用了完善的访问控制技术;

（4）通过验证和存取访问控制权限进行数据保护;

（5）在网络系统中，采用入侵检测产品，从检测与监听等

多方面对网络系统进行防护，及时发现入侵者并报警，并实施事件响应；

（6）所有终端安装防病毒软件，并定期升级；

（7）提供冗余设计。

7.9时间戳

证书、CRL、OCSP、CA、RA 系统日志均包含时间信息，该时间信息来源于国家的标准时间源。

8 证书、证书撤销列表和在线证书状态协议

8.1证书

CFCA 签发的证书格式符合 GB/T 20518《信息安全技术 公钥基础设施 数字证书格式》。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，基本证书域由基本项和扩展项组成。

8.1.1 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。

8.1.2 版本号

CFCA 签发的证书格式是 X.509 V3。

8.1.3 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。

8.1.4 签名算法

CA 签发该证书所使用的密码算法使用 sm3WithSM2 的标识符如下:

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	

8.1.5 颁发者

证书颁发的实体，通过一个非空的甄别名表示 CFCA 的 CA 名称。颁发者 DN 如下表所示:

属性	值
通用名（CN）	签发证书的 CA 系统名称，如 CFCA ACS OCA31
机构（O）	China Financial Certification Authority
国家（C）	CN

8.1.6 有效期

证书有效期是一个时间段，在这个时间段内，CA 担保它将维护关于证书状态的信息。通过不早于、不晚于时间段的 UTC Time 时间来表达有效期。

8.1.7 主体名称

本项用于描述与主体公钥项中的公钥对应的实体的情况，包含签发机构和订户证书主体唯一甄别名 DN。

订户证书 DN 通常包含以下域：从左到右，依次为 CN、OU[2]、OU[1]、O、C。

属性	值
通用名（CN）	法定证件上的名称、证件号码、证书顺序号等组成，@为分割符；设备证书该部分为 IP 地址/域名/设备 MAC 地址/设备标识符等。该项可采取脱敏技术保护隐私信息。
机构部门（OU2）	用于标识证书类型
机构部门（OU1）	用于标识 RA 机构标识
机构（O）	签发 CA 系统名称，比如 CFCA ACS OCA31
国家（C）	CN

8.1.8 主体公钥信息

本项用来标识公钥和相应的公钥算法。

8.1.9 证书扩展项

证书扩展项是一个或多个证书扩展的序列，针对某种证书类

型或者特定用户，CFCA 可为其签发的证书配置专有扩展项，专有扩展项为非关键扩展。

8.1.9.1 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。

8.1.9.2 主体密钥标识符

订户证书中包含主体密钥标识符扩展项，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。

8.1.9.3 证书策略及对象标识符

证书策略及对象标识符参考本 CPS 第 1.2 章节。该项为非关键项

8.1.9.4 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。该项为非关键项。

OCSP 响应地址：URI：https://ocsp.cfca.com.cn/ocsp

8.1.9.5 基本限制

基本限制标识证书主体身份是否为 CA，CA 证书的基本限制扩展项中 Subject Type 为 CA，本扩展设置为关键扩展。最终订户证书的基本限制扩展项中 Subject Type 为 End Entity，本项为非关键扩展。

8.1.9.6 密钥用法

密钥用法指明已认证的密钥用于何种用途。

对于 CA 证书的密钥用法，该项为关键扩展项。密钥用法：keyCertSign、cRLSign。

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。

8.1.9.7 扩展密钥用法（extKeyUsage）

此项指明已验证的公开密钥可以用于一种用途或多种用途，它们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。CFCA 签发的证书根据不同的证书类型，该项有不同的配置。该项为非关键扩展。

8.1.9.8 CRL 分发点

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，本扩展为非关键扩展。

8.1.9.9 主体替换名称

主体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。

服务器证书应包括该扩展项，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。

8.1.9.10 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或识别出包含无法处理的信息的关键扩展，应用系统应拒绝使用该证书。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，则应对其进行处理。

8.2CRL

CFCA 定期签发的证书撤销列表 CRL，CRL 可通过证书 CRL 分发点扩展中标识的地址进行下载。

8.2.1 版本号

X.509 V2。

8.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义包含以下内容:

（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（thisUpdate）;

（4）预计下一个 CRL 更新时间（nextUpdate）;

（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）。

8.3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，CFCA 可确保有足够的资源使 CRL 和 OCSP 服务在合理的时间内向用户反馈查询结果。

8.3.1 版本号

IETF RFC 6960 定义的 OCSP v1 版。

8.3.2 OCSP 扩展项

与 IETF RFC 6960 一致。

9 一致性审计和其他评估

9.1评估的情形及频率

CFCA 在如下情形中进行评估:

（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 按照内部审计管理制度，定期进行评估。

9.2评估者的资质

若需邀请外部测评机构对 CFCA 进行评估，CFCA 将选择熟悉 IT 运营管理、具有多年测评经验的测评机构对 CFCA 的运营管理进行合规性审查。在进行测评前，测评机构应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。

9.3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。

9.4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。

9.5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，对于能理解整改的问题，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。

9.6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，并与相关机构进行沟通，对审计存在问题的机构采取适当风控措施。

其他评估及审计报告不对外发布。

9.7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。

10 责任和其他业务条款

10.1费用

10.1.1 证书生命周期操作相关服务费用

CFCA 向订户提供证书签发、补发、换发等服务时，将合理收取相关服务费用，CFCA 收费标准在订户提交申请前告知。

CFCA 暂不收取证书撤销、证书查询、证书状态查询等服务费用，但保留对此项服务收费的权利。

10.1.2 其他费用

CFCA 保留收取其他服务费的权利。

10.1.3 退款策略

只有在 CFCA 违背了本 CPS 所规定的责任与义务的情况下，订户可以通过其支付费用的通道申请退回其支付未使用服务的相关费用，其他情况下不支持退款。订户申请退款时，订户的证书将同步撤销。如果因订户原因，在证书服务期内，申请退出证书服务体系，CFCA 将不退还剩余时间的服务费用。

10.2财务责任

10.2.1 保险范围

CFCA 根据业务发展情况，同时考虑国内保险种类，决定其投保策略。

10.2.2 其他资产

CFCA 确保具有足够的财务实力来维持其正常经营，保证相应义务的履行，并依据本 CPS 的约定承担对订户及对依赖方的责任。

10.2.3 对最终订户的保险或担保范围

CFCA 根据业务发展情况，决定就其电子认证服务为最终订户的投保策略。无论是否投保，CFCA 对最终订户的赔偿责任，见《数字证书服务协议》。

10.3业务信息保密

10.3.1 保密信息范围

保密信息包括但不限于以下内容:

（1）CFCA 认证体系的各种配置信息，包括但不限于 CA 私钥及保护口令;

（2）认证系统的各种备份信息，包括但不限于 CA 私钥备份分割保护信息;

（3）各种测评及审计等溯源记录及审计记录等;

（4）订户证书信息以外的个人隐私信息;

（5）政府部门的敏感信息和工作秘密

（6）其他被 CFCA 标注密级的信息。

10.3.2 不属于保密的信息

不属于保密的信息包括:

（1）证书、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。

10.3.3 保密信息的保护责任

CFCA 有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。CFCA 的每个员工都要接受信息保密方面的培训。

当 CFCA 在任何法律法规、规章的要求下，或在法院的要求下必须提供本 CPS 中具有保密性质的信息时，CFCA 应按照要求，向监管部门或执法部门公布相关的保密信息，CFCA 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。

10.4个人信息保护

10.4.1 个人信息保护方案

CFCA 严格遵守《中华人民共和国个人信息保护法》，任何订户选择使用 CFCA 的证书服务，表明已经接受 CFCA 的个人信息保护制度。

CFCA 的《法律声明及个人信息保护政策》已在官网（https://www.cfca.com.cn）公布。

10.4.2 作为隐私处理的信息

订户提供的不在数字证书内容中载明的且符合法律法规有关隐私信息定义的资料被视为隐私信息。

10.4.3 不被视作隐私的信息

订户提供的用来构建数字证书内容的信息不被视作隐私信息。

10.4.4 保护隐私的责任

CFCA、注册机构、订户、依赖方等机构或个人都有义务按照本 CPS 的规定，承担相应的隐私保护责任。在法律法规要求或公共权力部门通过合法程序要求下，CFCA 可以向特定的对象提供隐私信息，CFCA 无需承担由此造成的任何责任。

10.4.5 个人信息的收集

CFCA 作为合法的第三方电子认证机构，根据我国《中华人民共和国电子签名法》《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》和《中华人民共和国数据安全法》等相关法律法规和监管要求，在受理订户申请数字证书时需要对订户身份进行核验。CFCA 遵循合法、正当、必要和诚信的原则，收集和使用订户的个人信息，包括但不限于订户个人姓名、性别、年龄、证件号码、家庭住址、联系方式等。个人信息的使用原则上都应征得订户的同意后进行，除非 CFCA 为履行法定职责或者法定义务所必需，或法律法规另有规定的其他情形。与 CFCA 建立证书服务的合作方（包括但不限于 RA），应建立收集订户个人信息的管理制度，在开展业务过程中遵循合法、正当、必要的原则，以书面形式明确告知收集订户个人信息的目的、方式和范围，并征得订户书面同意。

10.4.6 个人信息的使用

CFCA 不会在与证书服务及应用无关的情况下使用订户个人信息。除非出现下列情形:

（1）基于订户本人书面授权或同意;

（2）根据国家有关法律法规规定的其他情形。

10.4.7 个人信息的共享

CFCA不会以商业目的或未取得订户自身同意或授权情况下，与其他组织或个人共享订户的个人信息。

在遵守国家相关法律法规的前提下，CFCA 经过用户本人书面授权或同意提供订户个人信息，并有义务要求接收方采取有效手段保护上述信息。本 CPS 未尽事宜以 CFCA 官网公布的《法律声明与个人信息保护政策》为准。

10.4.8 个人信息的保护和存储

（1）CFCA 采取合适的安全措施和技术手段存储及保护订户的个人信息，以防止丢失、被误用、受到未授权访问或泄漏、被篡改或毁坏;

（2）根据我国《中华人民共和国电子签名法》及相关规定，在证书失效后仍将保存订户个人信息至少 5 年，法律法规另有规定的除外。

10.4.9 个人信息的管理

（1）个人信息的查阅：订户有权访问其个人信息，对其姓名、证件号码或数字证书数据进行查看;

（2）个人信息的更正和补充：当订户需要更正或补充其个人信息时，可以通过电子邮件或电话等联系方式联系 CA 机构，C

A 机构将在 20 个工作日内回复更正请求;

（3）个人信息的删除：CA 机构按照法律法规要求对订户个人信息进行删除。

10.4.10 其他信息披露情形

CFCA、订户、注册机构、依赖方等机构或个人都有义务按照本 CPS 的规定，承担相应的个人信息保护责任。在法律法规或公共权力部门通过合法程序或订户授权同意情况下，CFCA 可以向特定的对象提供订户个人信息，CFCA 无需承担由此造成的任何责任。

10.5知识产权

CFCA 享有并保留对证书以及 CFCA 提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权；CFCA 制订并发布的 CPS、CP、技术支持手册、发布的证书和 CRL 等的所有权和知识产权均归 CFCA 所有。

订户产生的私钥与公钥属于订户的财产，但订户的公钥经 CFCA 认证签发成数字证书，数字证书及撤销列表发布在 CFCA 的信息库中，CFCA 的信息库属于 CFCA 的财产，CFCA 只提供订户及依赖方使用的权限。

10.6陈述与担保

10.6.1 电子认证服务机构的陈述与担保

CFCA 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。

CFCA 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，CFCA 对签发的数字证书承担相应法律责任。

CFCA 保证使用的系统及密码符合国家政策与标准，保证 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

CFCA 的运营遵守 CPS 并随着业务的调整对 CPS 进行修订。

根据《电子政务电子认证服务管理办法》要求，CFCA 将不定期对其注册机构电子政务电子认证业务是否符合本 CPS 约定进行审计。CFCA 具有保存和使用证书持有人信息的权限和责任。

CFCA 不负责评估订户及依赖方是否使用数字证书的情况，不承担因订户及依赖方超范围使用证书所带来的损失的赔偿责任。

10.6.2 注册机构的陈述与担保

作为 CFCA 的注册机构，应遵守本 CPS、CFCA《注册机构运

营管理规范》和《数字证书合作协议》等，并承诺以下事项：

（1）向用户告知数字证书申请前的相关事项，使订户明确地知道并书面同意关于使用第三方数字证书的意义、数字证书的功能、使用范围、使用方式、密钥管理以及丢失数字证书的后果和处理措施、法律责任限制等注意事项；

（2）按照本 CPS 要求，审核用户申请材料的真实性、完整性、准确性，并注册用户信息；如对订户的证书申请材料审查没有通过，有及时告知订户的义务；

（3）按照本 CPS 的规定，以安全的方式向 CA 提交证书申请、撤销、更新等服务请求；

（4）注册机构向订户提供智能密码钥匙时，应告知订户修改智能密码钥匙的初始口令，以及不在公共场所使用智能密码钥匙等相关注意事项；

（5）须对订户的申请信息及与认证相关的信息妥善保存，严格遵守隐私条款及个人信息保护条款的规定，于适当的时间转交给 CFCA 归档。根据相关协议内容配合 CFCA 需要的业务合规性审计及监管部门的监督检查；

（6）注册机构有义务通知订户阅读 CFCA 发布的 CP、CPS 以及其他相关规定，在订户完全知晓并同意 CP、CPS 和《数字证书服务协议》内容的前提下，为订户办理数字证书。

10.6.3 订户的陈述与担保及义务

订户确认已经阅读和理解了本 CPS 及《数字证书服务协议》的全部内容，并同意受此 CPS 文件规定的约束。

（1）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；

（2）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 CFCA 支付相应的服务费，具体费用可与 RA 协商；

（3）订户应在上述信息、资料发生改变时及时通知 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；

（4）订户须使用经合法途径获得的相关软件，且合法使用 CFCA 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；

（5）订户用于电子签名的证书私钥，应由订户自己产生，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。如订户委托他人代为产生签名私钥、申请证书、保管证书、使用证书等，应明确授权范围并定期核查授权履行情况。

订户如因故意、过失（被诈骗）等导致使用数字证书时遭受损失，订户应自行承担由此产生的责任；

（6）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到原 RA 或 CFCA 申请撤销该数字证书。证书过期或被撤销，订户将不得继续使用该证书；

（7）如因订户原因，导致依赖方或 CFCA 遭受损失的，订户需承担相应的赔偿责任。这些情形包括但不限于：

A. 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 RA 或 CFCA，导致依赖方遭受损失需要由 CFCA 赔偿的情况；

B. 订户知道自己的私钥已经失密或者可能已经失密而未及时告知 RA 或 CFCA，并继续使用导致依赖方遭受损失需要 CFCA 赔偿的情况；

C. 订户使用失效证书（包括过期、被撤销），给依赖方造成损失，或者有其他过错或未履行本协议的相关约定，违反相关法律法规的规定。

（8）订户在发现或怀疑由 RA 或 CFCA 提供的认证服务造成订户的网上交易信息的泄漏和/或篡改时，应在 24 小时内向 RA 或 CFCA 提出争议处理请求并通知有关各方。

10.6.4 依赖方的陈述与担保及义务

依赖方声明和承诺:

（1）通过 CFCA 官方途径获取并安装 CFCA 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：检查证书链的有效性；检查最新 CRL，确认该证书未被撤销；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）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;

（4）熟悉本 CPS 的条款，了解证书的使用目的，只在符合本 CPS 规定的证书应用范围内信任该证书;

（5）同意 CPS 中关于 CFCA 责任限制的规定。

10.6.5 其他参与者的陈述与担保

未列明的其他参与者应遵循本 CPS 的规定。

10.7担保免责

（1）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 CFCA 申请签发证书，订户因此使用该证书而产生的纠纷，由订户自行承担全部法律责任，CFCA 对

此不承担任何责任或后果;

（2）由于非 CFCA 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，CFCA 给予配合，但 CFCA 不向任何方承担赔偿或补偿责任;

（3）CFCA 对各类证书的适用范围作了规定，若证书被超出范围使用或被用于其他未被 CFCA 允许的用途，CFCA 不承担任何法律责任;

（4）由于不可抗力因素或必要的机构调整导致 CFCA 暂停、终止部分或全部数字证书服务，CFCA 不承担赔偿或补偿责任;

（5）CFCA 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，CFCA 不承担任何法律责任;

（6）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，CFCA 给予配合，但 CFCA 不承担赔偿或补偿责任。

10.8CFCA 承担赔偿责任的限制

（1）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，CFCA 不向订户和/或依赖方承担任何

赔偿和/或补偿责任;

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

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

A. 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、失去或无法使用任何数据、无法使用任何设备、无法使用任何软件等非直接受损的情形;

B. 由上述第 A 项所述的损失相应产生或附带引起的损失或损害;

C. 非因 CFCA 的行为而导致的损失;

D. 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。

（4）无论本 CPS 是否有相反或不同规定，如果 CFCA 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，CFCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

10.9有效期限与终止

10.9.1 有效期限

本 CPS 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。

10.9.2 终止

CFCA 有权终止本 CPS（包括其修订版本），CFCA 应在本 CPS（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 CPS 效力将自动终止。

10.9.3 终止后的存续条款

本 CPS 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 CPS 终止后继续有效。

10.10通告与沟通

如需要进一步了解任何本 CPS 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。

10.11修订

CFCA 有权修订本 CPS，并将修订后的版本在官方网站上公布。修订后的版本应注明生效日期。

10.11.1 修订程序

修订程序与本 CPS 第 1.5.4 章节“CPS 批准程序”相同。

10.11.2 通知机制和期限

CFCA 有权修订本 CPS 中的任何术语和条款，修订后会及时公布在 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，将被视为同意修订后的 CPS。

10.11.3 必须修改业务规则的情形

当本 CPS 描述的规则、流程和相关技术已经不能满足 CFCA 电子认证业务要求或本 CPS 依据的法律法规和部门规章变更时，CFCA 将依照有关规定修改本 CPS 的相关内容。

10.12争议解决

订户或依赖方在发现或合理怀疑由 CFCA 提供的认证服务造成订户的电子交易信息泄漏或篡改时，订户可向 CFCA 提出争议

处理请求并通知有关各方，或向北京仲裁委申请仲裁。

任何订户或依赖方欲向 CFCA 提出索赔，应当自知道或应当知道权利受损之日起的一年内提出。超出一年的，该索赔无效。

10.13管辖法律

本 CPS 和协议中条款的制定遵守《中华人民共和国民法典》和《中华人民共和国电子签名法》《中华人民共和国密码法》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，CFCA 将会对此条款进行修改，使之符合相关法律规定。

10.14与适用法律的符合性

CFCA 的各项策略均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要求。若本 CPS 的某一条款被主管部门宣布为违法、不可执行或无效时，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。本 CPS 某一个条款违法、不可执行或无效时，不会影响其他条款的法律效力。

10.15一般条款

10.15.1 本 CPS 的完整性

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。

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。

10.15.2 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。

10.15.3 分割性

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，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 CPS 中其他条款的有效性。

10.15.4 强制执行

无规定。

10.15.5 不可抗力

不可抗力是指不能预见、不能避免且不能克服的客观情况。构成不可抗力的事件包括战争、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，但各方都有义务建立灾难恢复

和业务连续性机制。

10.16最终解释权

本 CPS 最终解释权由 CFCA 所有，由 CFCA 负责解释和修订。

附录 A：定义与缩写

下列定义适用于本 CPS。

序号	项目	定义
1	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。[1]
2	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。[2]
3	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。[3]
4	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。[4]
5	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。[5]
6	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。[6]
7	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。[7]
8	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。
9	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。

[1]《电子政务电子认证服务管理办法》
[2] GB/T 25056-2018 3.12 有修改
[3] GB/T 25056-2018 3.9
[4] 参考《电子签名法》第十四条
[5] GB/T 25056-2018 3.4
[6] GB/T 27913-2022 3.42
[7] GB/T 25069-2022 3.789

10	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。[8]
11	密钥	控制密码变换操作的符号序列。[9]
12	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。
13	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。
14	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。
15	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。
16	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。
17	公钥	非对称密码算法中可以公开的密钥。
18	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。
19	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。[10]
20	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。[11]
21	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。[12]

[8] 参考《电子签名法》及 GB/T 25056-2018 3.3
[9] GB/T 25069-2022 3.389
[10] GB/T 27913-2022 3.32
[11] GB/T 25069-2022 3.576
[12] GB/T 25069-2022 3.119

22	电子签章	使用电子印章签署电子文件的过程。[13]
23	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。[14]
24	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 CPS。

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（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	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）

附录 B：CFCA 电子政务电子认证业务规则约束 CA 系统

根 CA	中级 CA	根 CA 算法	运营 CA	中级 CA 算法
国家根	CFCA CS	SM2/SM3	CFCA SM2 OCA1	SM2/SM3

[13] GB/T 25069-2022 3.120
[14] GB/T 25069-2022 3.121

CA	SM2 CA*		CFCA CS SM2 OCA11	
			CFCA ACS SM2 OCA31	
			CFCA ACS SM2 OCA32	
			CFCA ACS SM2 OCA33	

*：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。

附录 C：各类证书格式样例

终端用户（个人证书）		
属性	值	备注或示例
版本	X.509 V3	
序列号		由 CFCA 按照各 CA 规则产生的唯一数
签名算法	1.2.156.10197.1.501	SM3withSM2
颁发者	CN = CFCA CA 系统名称 O = China Financial Certification Authority C = CN	CN 项表示 CFCA 的 CA 系统名称，参见附录 B
有效期	不早于、不晚于	初始不超过 5 年，更新后不超过 5 年+3 个月
主体名称	cn=[应用标识@个人名称@01+身份证号@顺序号] ou=[证书类型] ou=[RA 简称] o=CFCA OCA 名称 c=CN	如：cn=CITIC@张三@01101081992****3034@0000001,ou=Individual-1,ou=CITIC,o=CFCA ACS OCA31,c=CN 隔符“@”为 CFCA 保留字符且应要有 3 个@符
公钥		公钥算法、公钥
标准扩展项		

颁发者密钥标识符	用于识别与颁发者证书签名私钥相应的公钥	
主体密钥标识符	用于识别同一主体使用的不同密钥	
密钥用法	签名证书：数字签名、抗抵赖 加密证书：密钥加密、数据加密、密钥协商	（“关键”扩展）
证书策略	Policy Identifier = [证书类型 oid] Policy Qualifier ID = CPS Qualifier : [CFCA 电子政务电子认证业务规则 URL]	
基本限制	主体类型（Subject type）	最终实体
扩展密钥用法	客户端认证/服务端认证/ocsp 签名/	根据证书类型不同扩展密钥用法不同
CRL 分发点	标识证书对应的 CRL 下载地址	url:https://crl.cfca.com.cn/oca31/SM2/*.crl *表示的是具体的分发点
机构信息访问	标识 CA 机构可访问的 OCSP 服务地址	URI: https://ocsp.cfca.com.cn/ocsp
终端用户（机构证书）		
属性	值	备注
版本	X.509 V3	
序列号		由 CFCA 按照各 CA 规则产生的唯一数
签名算法	1.2.156.10197.1.501	SM3withSM2
颁发者	CN = CFCA CA 系统名称 O = China Financial Certification Authority C = CN	CN 项表示 CFCA 的 CA 系统名称，参见附录 B
有效期	不早于、不晚于	初始不超过 5 年，更新后不超过 5 年+3 个月

主体名称	cn=[应用标识@机构名称@N+统一社会信用号@顺序号，隔符（@）为 CFCA 保留字符且应有 3 个@符] ou=[证书类型] ou=[RA 简称] o=CFCA OCA 名称 c=CN	如：cn=CITIC@中金金融认证中心有限公司@N91110000759626025U@00000001, ou=Organizational-2,ou=CITIC,o=CFCA ACS OCA31,c=CN
公钥		
标准扩展项		
颁发者密钥标识符	用于识别与颁发者证书签名私钥相应的公钥	
主体密钥标识符	用于识别同一主体使用的不同密钥	
密钥用法	签名证书：数字签名、抗抵赖 加密证书：密钥加密、数据加密、密钥协商	（“关键”扩展）
证书策略	Policy Identifier = [证书类型 oid] Policy Qualifier ID = CPS Qualifier : [CFCA 电子认证业务规则 URL]	
基本限制	主体类型（Subject type）	最终实体
扩展密钥用法	客户端认证	根据证书类型不同扩展密钥用法不同
CRL 分发点	标识证书对应的 CRL 下载地址	url:https://crl.cfca.com.cn/oca31/SM2/*.crl *表示的是具体的分发点
机构信息访问	标识 CA 机构可访问的 OCSP 服务地址	URI: https://ocsp.cfca.com.cn/ocsp
终端用户（设备证书）		
属性	值	备注
版本	X.509 V3	
序列号		由 CFCA 按照各 CA 规则产生的唯一数
签名算法	1.2.156.10197.1.501	SM3withSM2

颁发者	CN = CFCA CA 系统名称 O = China Financial Certification Authority C = CN	CN 项表示 CFCA 的 CA 系统名称，参见附录 B
有效期	不早于、不晚于	初始不超过 5 年，更新后不超过 5 年+3 个月
主体名称	cn=[设备 ip 地址/mac 码/域名] ou=[组织部门名称，不一定存在] o=设备所有者机构法定名称 L = 地区（服务器证书存在） S = 省（服务器证书存在） c=CN	如：cn=192.168.120.122,ou=运行部,o=中金金融认证中心有限公司，L = 北京 ST = 北京 C = CN
公钥		
标准扩展项		
颁发者密钥标识符	用于识别与颁发者证书签名私钥相应的公钥	
主体密钥标识符	用于识别同一主体使用的不同密钥	
密钥用法	签名证书：数字签名、抗抵赖 加密证书：密钥加密、数据加密、密钥协商	（“关键”扩展）通常签发双证书
证书策略	Policy Identifier = [证书类型 oid] Policy Qualifier ID = CPS Qualifier : [CFCA 电子认证业务规则 URL]	
基本限制	主体类型（Subject type）	最终实体
主体备用名称	可与主体名称一致	
扩展密钥用法	服务端认证	根据证书类型不同扩展密钥用法不同
CRL 分发点	url:https://crl.cfca.com.cn/oca31/SM2/*.crl	*表示的是具体的分发点
机构信息访问	标识 CA 机构可访问的 OCSP 服务地址	URI: https://ocsp.cfca.com.cn/ocsp
OCA 证书（以 CFCA ACS SM2 OCA31 为例）		
属性	值	备注

版本	X.509 V3	
序列号	1000000012	
签名算法	1.2.156.10197.1.501	SM3withSM2
颁发者	CN = CFCA CS SM2 CA O = China Financial Certification Authority C = CN	上级 CA
有效期 从	2015年9月27日 9:55:11	
有效期 到	2035年7月4日 9:55:11	
主体名称	CN = CFCA ACS SM2 OCA31 O = China Financial Certification Authority C = CN	
公钥	04 27 12 c0 14 e6 68 a2 e6 b5 00 30 39 bb d9 0f e4 a4 96 96 c0 3d 37 f1 b3 5a 8d 24 24 bd 5f 71 66 e9 4b 1d 5e 9b 9a 58 7f b9 19 72 35 cb ad 1f 2d 1c 48 d9 b9 dc c2 14 4e aa 8c 57 44 dc 7c e1 31	
公钥参数	1.2.156.10197.1.301	
标准扩展项		
颁发者密钥标识符	e48eddd4a3e7b60fee1d2796cd75dc25257269dd	
主体密钥标识符	08d8d126c4487d9cecac98e9f17f62b980cea945	
密钥用法	Certificate Signing, Off-line CRL Signing, CRL Signing （06）	关键扩展
基本限制	Subject Type=CA Path Length Constraint=None	关键扩展
CRL 分发点	URL=https://crl.cfca.com.cn/csrca/SM2/crl1.crl	