CFCA 电子认证服务业务规则（CPS）

CFCA Certification Practice Statement

V5.0

生效日期：2025年8月15日

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
3.0	修改	1.声明了 J-01 系统下线策略; 2.增加了 CS 体系的说明; 3.增加了场景证书及复合证书等的说明，将原电子认证业务规则版本升级为 V3.0	CP/CPS 编写组	CFCA 安委会	2015 年 08 月
3.1	修改	补充了 ACSCA 系统的说明	CP/CPS 编写组	CFCA 安委会	2015 年 10 月
3.2	增加内容	补充了云证通证书等说明	CP/CPS 编写组	CFCA 安委会	2016 年 06 月
3.3	修改	对该体系涉及的新建子 CA 系统进行了补充，对 GT 系统下的 OCA21 CPS 变更调整进行了说明	CP/CPS 编写组	CFCA 安委会	2017 年 10 月
3.4	修改	增加了对《粤港电子签名证书互认证书策略》适应性扩展项，以及相关算法适应性描述	CP/CPS 编写组	CFCA 安委会	2018 年 11 月
4.0	修订文档内容错误修订	1.增加关于 CFCA 证书分级的策略及 OID 说明; 2.增加了关于证书中含有商标标识时的处理办法; 3.OCSP 遵从的标准修改为 RFC6960; 4.DN 描述及组成规则从 CPS 中删除，将在 DN 规则中统一描述; 5.增加附录 B（本 CPS 下 CA 说明）; 6.文档内容错误修订;	CP/CPS 编写组	CFCA 安委会	2019 年 05 月
5.0	修订	本文档对 4.0 版本进行了修订：1.明确了遵循的法律法规及标准规范；2.对 4.0 版本进行补充完善，如 1.4.1 证书类型及适用的证书应用等；3.进一步健全 4.0 版本，补充其应有的附件内容。	CP/CP 编写组	CFCA 策略管理委员会	2025 年 08 月

目　　录

前言

《中华人民共和国电子签名法》第十四条规定：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 作为第三方电子认证服务机构，面向各类实体签发数字证书并提供电子认证服务。用户可依托 CFCA 签发的数字证书实现身份核验，保障信息完整性、防篡改和防抵赖等功能。本文档《CFCA 电子认证服务业务规则》（以下简称 CFCA CPS、本 CPS）所涵盖的用户数字证书符合可靠电子签名条件。

注册是电子认证服务的重要组成部分。CFCA 通过协议授权合作机构作为注册机构（以下简称“RA”、“RA 机构”），注册机构受理用户证书申请，审核用户申请信息，协助用户申请数字证书。

用户在申请 CFCA 签发的数字证书时，须接受《CFCA 电子认证服务协议》的相关条款。用户应妥善保管其数字证书私钥安全。如用户委托他人代为生成签名私钥，或申请、保管与使用证书，建议明确委托授权范围，并定期对授权执行情况进行核查。若因用户故意、过失（如受骗）等原因导致在使用数字证书过程中遭受损失，相关责任由用户自行承担。

CFCA 对用户的赔偿责任依照 CFCA 官方网站上公布的《CFCA 电子认证服务协议》中的相关条款执行。

版本修订说明（2025 年 7 月）

本次修订主要参照 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》对文档结构进行了调整和完善。

本次修订的主要内容：基于“电子认证业务策略管理委员会”的设立，对相关批准程序和流程进行了架构调整与优化；对 CP、CPS 的报备流程进行了梳理和完善，并明确要求在业务流程中签署《CFCA 电子认证服务协议》；优化了对信息库功能的描述，新增部分证书类型，并完善了对特定应用场景下证书的说明；新增对 RA 机构的备案管理、人员培训及定期评估要求，进一步强化对 RA 机构的全流程监管；完善了在线申请证书时的身份鉴别流程，明确处理时限要求；完善关于个人信息保护的描述；参照最新的国家标准与行业标准，完善了部分术语定义并新增了数字证书格式样例；补充了 RA 机构在受理用户证书申请过程中应履行的相关职责；根据国家法律法规和主管部门要求，调整了证书发布的相关规定，优化了特殊场景（如紧急撤销）下的发布频率及 OCSP 查询服务等内容。

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 电子认证服务业务规则》（CFCA Certification Practice Statement，以下简称“本 CPS”），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（政府机关、企事业单位、其他组织及个人等）提供电子认证服务，包括对公众进行身份核验，为公众签发数字证书（简称“证书”）以及提供证书生命周期管理、验证等服务，用于网络场景确认参与方身份，保障信息机密性、防篡改性和防抵赖性。本文档阐述了 CFCA 提供电子认证服务的各项操作规程，符合《CFCA 电子认证业务证书策略（V4.0）》和广东省人民政府《粤港电子签名证书互认证书策略（1.1 版）》的相关策略。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 CPS 所约定的责任，并承担相应的责任和义务。

本 CPS 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 CPS 中如有“应”相关要求的，均是相关各方需要满足的要求。

本 CPS 适用的 CA 系统详见附录 A: CFCA 电子认证服务业务规则 V5.0 约束 CA 系统。CFCA 的 CA 系统（包括子 CA）均由 CFCA 所有并直接控制。CFCA 将根据业务发展需要评估是否需要对本 CPS 进行更新调整。

本 CPS 在《CFCA 电子认证业务规则》V4.0 版本的基础上完善修订。本 CPS 引用的所有法律法规、标准规范、内部文档等，凡是注日期的引用文件,仅注日期的版本适用于本 CPS;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 CPS。

1.2 文档名称与相关标识

本文档名称为《CFCA 电子认证业务规则》，本文档相关的识别码 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
2.16.156.112554.1	《CFCA 电子认证服务业务规则（CFCA CPS）文档标识》
2.16.156.112554.9.1	场景证书证据集合（EvidenceBundle）
2.16.156.112554.10	《CFCA 电子认证服务证书策略（CFCA CP）文档标识》
2.16.156.339.1.1.1.2.1	应用在香港特别行政区的电子签名证书互认证书中自然人证书（个人证书）
2.16.156.339.1.1.2.2.1	应用在香港特别行政区的电子签名证书互认证书中法人证书（机构证书）

1.3 电子认证活动参与者

本 CPS 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 CPS 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 CPS 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 CFCA 数字证书合作协议，并按照协议内容及本 CPS 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，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

数字证书具备网络用户身份核验、交易防抵赖性、信息完整性和信息机密性四项基本功能。用户可根据自身需求，在网上金融交易、电子商务、电子政务、公共服务、企业信息化及个人事务等多种应用场景中灵活选择一种或多种证书功能。

本 CPS 下的证书类型可从不同维度进行分类，各维度分类可互相交叉，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。详见附录 B:

证书类型。

订户通过RA机构办理业务时所申请的数字证书，通常仅适用于该RA机构的相关业务。若订户超范围使用可能带来风险。CFCA提请订户注意此类风险，且CFCA不对该风险造成的损失承担责任。若订户需要超出其当初申请证书时的应用范围使用证书，应向CFCA进行报备。

1.4.2 限制的证书应用

本CPS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CPS限定的应用范围使用证书，将不受保护。

本CPS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规定相违背的领域，以及任何未经过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。

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“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 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：（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 CPS 符合策略的机构

本 CPS 是否符合 CFCA 的 CP，由策略管理委员会审核决定。审核过程同本 CPS 第 1.5.4 章节。

1.5.4 CPS 批准程序

本 CPS 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 CPS。策略管理委员会编写小组制定、修订 CPS 初稿；CPS 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。

CFCA 将定期评估本 CPS 的适用性，根据评估结果及时进行修订，并按照前述流程批准公布。公布的本 CPS 版本自生效之日起，对所有在生效日期之后申请证书的订户均具有约束力。订户或依赖方需定期查阅 CFCA 官网 https://www.cfca.com.cn 发布的本 CPS 的最新版本。若订户或依赖方在本 CPS 最新版本公布之日起一个月后，仍继续使用 CFCA 签发的数字证书，则视为其已接受该最新版本的约束。若订户或依赖方不同意接受该最新版本的条款，应立即停止使用 CFCA 签发的数字证书。

1.5.5 定义和缩写

见附录 C: 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，《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。

CP、CPS、《CFCA 电子认证服务协议》、证书链可至 https://www.cfca.com.cn/下载专区查阅及下载；数字证书可通过 CFCA 证书下载平台（https://cs.cfca.com.cn）等官方渠道获取；OCA32 签发的证书可通过联系 CFCA 客服获取；已撤销的证书信息可通过数字证书内的 CRL 分布点查询获取；证书状态信息可通过 OCSP 等服务获取。

本 CPS 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 CPS 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 CPS 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。CRL 的发布频率参见本 CPS 第 4.9.7 章节（CRL 发布频率）。

《CFCA 电子认证服务协议》、相关技术支持信息、证书链等在确认版本后，按照官方网站管理制度的批准程序发布。

CFCA 官方网站所发布的信息库，确保 7*24 小时可访问。

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。

CFCA 网站上发布的 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、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,甄别名）是数字证书主体名称域中用于唯一标识证书主体的 X.500 名称。证书 DN 通常根据个人或机构法定证件上的名称和证件号码来明确证书主体的身份，能够将名称与唯一一个确定的实体（如个人、组织机构、设备或域名等）关联起来，且使依赖方可识别该实体。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。

个人证书 DN 中的通用名通常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 DN 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 DN 中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认证。SSL 服务器证书 DN 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认证。

安全邮件证书 DN 中的通用名必须是真实名称，邮件地址必须是有效的地址。

代码签名证书 DN 中的组织机构名称必须是证书订户的真实名称，通用名称可以是代码标识名称或者有效证件上的真实名称。CFCA 将对有效证件进行认证。

预植证书 DN 中包含标识审核订户身份的 RA 机构相关应用系统信息标识，订户信息将与该 RA 机构应用系统中的订户标识一起被认证。

场景证书 DN 包含申办场景业务的申请者的真实名称或者申办场景的特征。

密钥分散型证书 DN 包含 RA 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 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，DN 规则由 CFCA 定义，除 CFCA 预植证书，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

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。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

订户在申请数字证书时不得使用可能侵犯他人知识产权的信息。若订户提交的申请信息包含商标信息，则需要订户提交有关的商标注册文件，如政府机构发放的合法性证明文件。CA 机构颁发数字证书时，仅对商标的合法性证明文件进行形式审查，不审查证书订户是否处于纠纷中，且无需对任何订户关于知识产权的使用行为负法律责任。当发生有关知识产权的争议或纠纷时，CA 机构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钥匙中产生，或者在通过GB/T 37092《信息安全技术 密码模块安全要求》标准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 订户身份的鉴别

订户在申请数字证书前，应仔细阅读与CFCA数字证书申请的相关事项，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的证书申请信息，接受证书申请的有关条款，并同意承担相应的责任。

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、准确性、有效性进行鉴别，对订户提交的证书申请信息进行审核，并妥善保存订户申请材料及鉴别记录。

RA机构在进行身份鉴别时，无论采用何种方式，都应妥善保管相应的鉴别记录。

3.2.2.1 个人订户身份的鉴别

个人订户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，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，可采取以下鉴别方式：

A. 线下鉴别方式。个人订户在 RA 机构现场办理数字证书业务。

（1）个人订户应提供法定身份证件，RA 机构柜台应通过第三方权威可信数据源，核验订户身份信息的真实性、准确性、有效性。

（2）若通过权威可信数据源不能满足核验订户身份信息的真实性、准确性、有效性的要求，订户应提供其他法定有效证件，RA 机构柜台应进一步核验。

（3）RA 机构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。

B. 线上鉴别方式。订户可通过 CA 机构在线申请平台、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：

（1）核验订户法定证件的真实性、准确性、有效性，如线上系统通过第三方权威可信数据源进行核验。

（2）若通过第三方权威可信数据源不能满足核验订户提供的法定证件的真实性、准确性、有效性的要求，应辅助其他方式鉴别。

（3）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、小额打款等方式。

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；若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包含经办人有效身份信息的电子数据。

RA 机构操作员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:

A. 线下方式。机构订户授权代表在 RA 机构现场办理数字证书业务。

（1）机构订户代表应提供机构法定证件，RA 机构柜台人员应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、准确性、有效性、完整性。

（2）若通过第三方权威可信数据源不能满足核验机构订户证件信息的真实性、准确性、有效性、完整性的要求，机构订户代表应

提供其他法定有效证件，RA 机构柜台人员应进一步核验。

（3）RA 机构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。

（4）RA 机构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。

B. 线上方式。机构订户授权代表可通过 CA 机构在线申请平台、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，至少应对以下信息进行核验。

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

（2）若通过第三方权威信源不能满足核验机构订户提供的法定证件的真实性、准确性、有效性的要求，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。

（3）机构订户意愿性的核验，如机构法人短信验证码、法人生物识别、机构账户小额打款等方式。

（4）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 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）机构给予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包含经办人有效身份信息的电子数据。

批量申请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、准确性、有效性、完整性，以及对委托书进行审查。审核方式同本 CPS 第 3.2.2.1 章节、第 3.2.2.2 章节。

3.2.2.4 设备证书信息的鉴别

设备证书通常应用于机构的设备标识及通信安全，RA 机构可以受理本机构的设备证证书申请，RA 机构对本机构设备证书申请时的鉴别仅需要确保设备信息属于本机构，且信息准确有效。其他机构的设备证书申请由 CA 机构负责核验。

机构订户申请设备证书时，除了提交身份证明资料外，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。

CA 机构除对订户的身份、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。对域名的初步鉴别方法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订户一致，初步审核确定服务器证书订户确实拥有此域名，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，确认订户对域名的所有权或控制权。随机值应发送到标识为域名联系人的电子邮件地址或'admin','administrator','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。

3.2.2.5 其他证书类型的信息鉴别

针对安全邮件证书，CA 机构将只受理可在域名注册信息查询（whois）功能里查询到的域名邮件申请，并通过适当的途径鉴别该邮件地址是否合法、有效，同时鉴别证书订户的身份信息、地址、国家等信息。对电子邮箱的鉴别只会验证电子邮件是否属于订户使

用，并不会验证订户是否用实名注册此邮箱。

预植证书在证书绑定时，参照个人订户、机构订户线下身份鉴别方式进行核验。

场景证书按照场景中涉及到的实体，参照个人订户、机构订户线上身份鉴别方式进行核验。

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。

3.2.3 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

当订户通过授权第三方代理申请某一类型证书时，RA 机构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。CA 机构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 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 CFCACS 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。

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。

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，建议重新产生一对新的密钥对。证书密钥更新有两种情况：证书补发、证书换发。

（1）证书补发

补发是指在证书有效期内，存在以下情形时，订户需要申请证书补发：

A. 订户证书介质丢失或损坏，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 CA 机构认可的原因。

当订户需要补发证书时，若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

愿性的方式进行鉴别；线下鉴别方式与初次申请证书要求一致。

证书补发时新证书到期日与原证书到期日一致。

（2）证书换发

换发是指在证书到期日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。若原证书在智能密码钥匙中，或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。若原证书不在智能密码钥匙中，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或邮箱发送验证码以及其他能够证明意愿性的方式进行鉴别。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，到期日为原证书到期日再加一个证书有效周期。

证书已过期时的换发核验。若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；若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、邮箱等发送验证码等订户参与方式鉴别。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 SSL 服务器证书外，在证书补发或者证书换发申请提交至 CA 系统时，若原证书还在有效期内，CA 系统将同步撤销原证书，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原证书。SSL 服务器证书在证书补发或者证书换发申请之日起三十日后，如原证书依然在有效期内，则 CA 系统可撤销原证书。

场景证书不涉及密钥更新。

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、订户可通过现场或在线方式向 RA 机构提交数字证书申请。在申请前，订户应认真阅读并充分理解相关告知内容，接受 RA 机构公布的《CFCA 电子认证服务协议》。在确认知悉并同意所有事项后，订户应提交真实有效的身份证明文件、证书申请材料及相关信息。若订户委托他人代为申请，应明确委托授权范围，并对授权行为负

责。

2、RA 机构应遵守 CFCA《注册机构运营管理办法》的规定，处理与数字证书相关的各项事务，并切实履行对订户的告知、审查、注册以及相关资料的妥善保管等义务。

RA 机构在受理证书申请时，应采取适当措施确保订户充分知晓以下内容。这些措施包括但不限于当面告知、书面签字告知、录音录像告知以及系统页面展示等方式。RA 机构还应协助 CA 机构与订户签署相关协议:

（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;

（7）其他需要事先告知的事项。

3、在订户同意协议的情况下，RA 机构应收集订户证书申请信息，并按照本 CPS 第 3.2 章节规定的方式进行身份核验。身份核验通过后，RA 机构应完成订户信息的注册；若身份核验未通过，应告知订户未通过的原因。

4、订户信息完成注册后，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 机构提交证书申请。CA 机构应校验 RA 机构的权限及证书申请格式，并依

据 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 章证书操作流程的要求签发数字证书。签发完成后，CA 机构应将证书发送至 RA 机构，由 RA 机构转交订户。

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 CA 机构的预植服务系统。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证书密钥及证书申请文件（CSR），利用下载凭证，通过 CA 机构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》；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。

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。

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。

7、CA 机构应不定期审查证书业务的合规性。

4.2 证书申请处理

4.2.1 执行识别与鉴别程序

RA 机构处理证书申请按照本 CPS 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。若鉴别通过后，RA 机构可向 CA 机构提交申请，CA 机构为订户签发数字证书或证书下载凭证，由 RA 机构反馈给订户。若鉴别未通过，RA 机构应拒绝其申请，于两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符合要求的材料后再次提交申请。CA 机构将根据其内部管理制度，不定期对 RA 机构提交的订户申请材料进行复核，并有权拒绝不符合本 CPS 要求的申请。

4.2.3 处理证书申请的时间

订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 机构需在两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。

场景证书通常为即时处理。

4.3 证书签发

4.3.1 证书签发中 CA 机构和 RA 机构的行为

RA 机构与 CA 机构建立安全通道，CA 机构接收到 RA 机构的证书申请后，对 RA 机构权限、证书申请格式、RA 机构签名等进行验证，验证通过后按照脱敏规则签发证书。订户也可使用下载凭证（两码），通过 CFCA 官方网站下载平台下载证书。CA 系统接收到下载申请后，对两码进行核验，并对订户提交的证书申请格式及签名进行验证，通过后按照脱敏规则签发证书。

对于预植证书，CA 机构操作人员在全方位监控环境下，按照规则预先将证书签发并下载在智能密码钥匙中，并按照规则将证书发布至信息库。预植证书生产后，操作人员应执行检验程序，检验通过后可交付给 RA 机构，检验未通过的应按照《不合格品处理规范》处理。当订户身份信息与其关联（绑定）的预植证书信息反馈至 CA 机构的预植服务系统后，视为预植证书签发完成。

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 机构通过电话、短信、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。订户可通过 CFCA 官方网站查询证书签发结果。

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通过 RA 机构获得证书等，应对证书信息进行核对无误后方可启用。本 CPS 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，一日内无异议的，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；预植证书一旦绑定激活，即视为订户已经接受此证书；场景证书一旦签发，即视为订户已经接受此证书。

若订户对证书有异议或者拒绝接受证书时，RA 机构应协助订户撤销证书或者重新签发证书。

订户接受证书后，即视为订户接受本 CPS 准则、与 CA 机构签署了《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

若订户明确表示拒绝发布证书信息的，CA 机构将不发布该证书申请者证书信息；没有明确表示拒绝的，CA 机构按照信息库发布规则将证书发布至信息库。场景证书不发布证书撤销信息。

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。

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 CPS 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。

（8）场景证书只能在申请证书时的场景中使用。

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CA机构签发、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，并对证书进行以下步骤:

（1）通过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有效，包括:检查CA机构公布的最新CRL或OCSP，确认该证书未被撤销；检查证书链的可靠性；检查该证书的有效期；以及检查其他能够影响证书有效性的信息;

（4）验证证书的用途适用于对应的签名；使用该公钥证书上的公钥验证签名;

（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、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

证书密钥更新适用于以下情况:

（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。

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过期（到期日前三个月内）或已过期的

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；若原证书已过期，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。

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。

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。

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 CPS 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;

（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 机构提出撤销申请，并说明合理的撤销理由。

CA 机构可在本 CPS 第 4.9.1 章节所述的情形下撤销订户的证书。

4.9.3 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 CPS 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。

场景证书不支持证书撤销。

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

依赖方在信任该证书前，应验证其有效性，并确认证书是否已被撤销。依赖方可通过以下两种方式获取证书状态信息:

（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

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 机构提供在线证书状态查询（OCSP）服务，服务 7*24 小时可用。

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

CA 机构的 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）。CFCA仅对个别RA机构开放证书冻结权限。当有下列情形发生时，可发起对证书冻结申请:

（1）当订户怀疑自己的证书受到威胁且希望暂停使用证书时，订户可发起证书冻结申请;

（2）当订户违反了本CPS相关规定，且具备该权限的RA机构或CA机构有必要暂停订户证书使用时，该机构可发起证书冻结申请。

证书冻结处理程序如下:

（1）订户提起申请，与订户相关的RA机构对订户进行身份核验，核验通过后，向CA机构发起证书冻结申请;

（2）CA 机构收到该申请后，核验 RA 机构权限及申请数据格式规范性，将所申请证书置于撤销状态，并按照规则发布 CRL;

（3）RA 机构告知订户处理结果。

自 CA 机构收到证书冻结请求至实际发布 CRL 期间，订户应停止使用该证书，并立即通知相关依赖方停止使用该证书。

证书解冻处理程序如下:

（1）当暂停使用证书的威胁解除后，若订户希望继续使用该证书且证书依然在有效期范围内，订户可向 RA 机构发起证书解冻申请;

（2）RA 机构对订户进行身份核验，核验通过后向 CA 机构发出证书解冻申请;

（3）CA 机构收到该申请后，核验 RA 机构权限及申请数据格式的规范性，核验通过后将该证书从 CRL 清单中去除，并将证书状态置于有效状态且可使用。

证书处于冻结状态的最长时限为证书的有效期。

4.10 证书状态服务

4.10.1 操作特征

证书状态服务按照本 CPS 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，在证书过期后将其从 CRL 中移除。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。但证书过期后，已撤销的证书将不在 CRL 中发布。

证书撤销后，可通过 OCSP 服务查询其状态。

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过期证书的当前状态。

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

4.12.1 密钥托管与恢复的策略与行为

CA 机构自身密钥不托管给第三方。CA 机构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托管与恢复服务。

密钥恢复是指加密密钥的恢复，CA 机构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 CA 机构申请密钥恢复，经 CA 机构审核后，可恢复密钥并存储于特定载体中。

4.12.2 会话密钥的封装与恢复的策略与行为

不作规范。

4.13 证书归档

本 CPS 中除 CFCA ACS OCA32 签发的证书，在证书过期后，将对过期的证书进行归档，证书及证书归档记录自证书到期日起保留五年。

对于 CFCA ACS OCA32 签发的证书，将在证书签发后三个月内进行归档，归档记录保存至少五年。

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。

5.1.1 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，禁止未经授权的人员访问，确保业务的可靠性。

5.1.2 物理访问

外来人员进出楼内时，需经过中国银联自有物业、CFCA 的两道审核，进出 CFCA 办公区域时，须通过两道门禁系统，且需要有 CFCA 工作人员陪同进出。

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。

授权人员进出 CFCA 综合机房，须经过指纹认证加门禁授权卡身份认证，并有 7*24 小时视频监控设备进行监控。

授权人员进出安全区机房，须经过三道门禁系统，其中两道通过双人指纹加门禁卡认证，另一道通过双人门禁卡认证，且所有门禁的访问控制信息均保存记录。

5.1.3 电力与空调

CFCA 机房符合 GB/T 28447、GB/T 25056 等相关标准建设，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。

5.1.4 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降低漏水对认证系统的影响。

5.1.5 火灾防护

CFCA 机房采用防火材料建设，配备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。

5.1.6 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。

5.1.7 废弃物处理

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《CFCA 生产系统加密机管理办法》销毁；本项下的所有废弃物处理均留存处理记录。

5.1.8 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，并利用专线复制到灾备中心。

5.2 程序控制

5.2.1 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及影响 CA 密钥安全的管理人员视为可信角色，至少包括:

（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;

（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。

CA 机构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。

5.2.3 每个角色的识别与鉴别

CA 机构在雇佣一个可信角色之前将按照本 CPS 第 5.3.2 章节的规定对其进行背景审查。

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

CA 机构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。

5.2.4 需要职责分割的角色

要求职责分割的角色包括（但不限于）以下几种:

（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

CFCA 按照以下要求进行人员管理及控制。

5.3.1 资格、经历和无过失要求

CA 机构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备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

CA 机构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

CA 机构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 5.3.1 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

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 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

CA 机构每年向电子认证服务相关人员（含 RA 机构人员）至少提供一次业务培训，以不断提高职业技能，保持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，也将安排对相关人员（含 RA 机构人员）进行相应的培训。

5.3.5 未授权行为的处罚

一旦发现员工执行了未经授权的操作，该员工将被立即暂停工作，并根据 CA 机构的相关管理制度接受相应的纪律处分。

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须的文档，文档配备满足 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 10.6 章节的要求。

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。

CA 机构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，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）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。

5.4.2 处理审计日志的周期

CA 机构对上条中，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。

CA 机构按照内部管理措施，定期核查记录的完整性，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 CPS 第 5.4.1 章节中的事件类型（1），审计日志保存至关联 CA 密钥失效后五年；事件类型（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。

5.4.5 审计日志备份程序

CA 机构将按照《生产系统日志管理办法》及《生产系统备份管理办法》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。审计日志收集应保证所收集数据的完整性和可用性。日志收集系统涉及 RA、CA、KM 系统、数据库、堡垒机、备份系统等。

5.4.7 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，CA 机构不进行通告。

5.4.8 脆弱性评估

CA 机构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。

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 CP、CPS 及历史版本;

（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记录归档并至少保留至证书失效后五年。

其他归档记录永久保存，直到归档存储不足时，负责归档人员可向信息安全委员会提出消除归档申请，策略管理委员会审议通过后可销毁归档。如果法律法规有其他要求时，CA 机构将调整记录归档保存期限。

5.5.3 归档文件的保护

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

5.5.4 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。

应用日志备份：每日自动进行一次备份，保存到集中备份服务器。

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

CA 机构有自动的电子归档信息的存放系统，满足本 CPS 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

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，CA 机构将启动密钥更新流程，替换即将过期的 CA 密钥对。密钥变更按如下方式进行:

（1）上级 CA 应在其私钥到期时间小于下级 CA 的最长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、产生新的密钥对和新的子 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。

5.7 损坏与灾难恢复

5.7.1 事故和损害处理程序

当 CA 机构遭到攻击、发生通讯网络故障、计算机设备不能正常提供服务、软件遭破坏、数据库被篡改等情况时，CA 机构将根据其制定的业务连续计划等相关规章制度采取合理措施。

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

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。

CA 机构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，CA 机构信息安全委员会负责人召集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，CA 机构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，CA 机构将在 24 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。

CA 机构具有专门的问题报告和响应机制：CA 机构向订户、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 CA 机构报告证书的投诉、私钥泄漏、证书使用不当、其他形式的欺诈、泄漏、使用不当或行为不当等。

CA 机构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。

CA 机构确保全天候（7*24 小时）对高优先级的问题报告首先在 CA 机构内部进行响应，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。

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，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。

5.7.3 实体私钥损害处理程序

CA 机构制定了《签名私钥泄露紧急预案》，其中明确规定 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 CA 机构证实 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，会立即通过官方网站等方式通知订户及依赖方，对所有受影响的证书进行撤销，并不再签发新的证书。

5.7.4 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，CA 机构将在 24 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。CA 机构每年按照业务连续性计划进行演练。

5.8 电子认证服务机构或注册机构的终止

CA 机构授权的 RA 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 RA 机构承接事务。

CA 机构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九十日前，就业务承接及其他有关事项通知有关各方，做好通知订户、移交与认证相关的数据等善后工作。

CA 机构将在暂停或终止电子认证服务六十日前向行业主管部门报告，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。拟终止电子认证服务的，应申请办理《电子认证服务许可证》注销手续。

若 CA 机构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。

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

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

5.9 预植证书生产管理规程

对于预植证书使用的智能密码钥匙（USBKey），CA 机构检查存储介质的相关资质，确保预植证书使用的存储介质通过商用密码检测认证。

CA 机构制定了安全生产相关管理办法，规定了出入库、盘点等操作规范。CA 机构在预植证书生产前对存储介质进行检查，只有空白的介质才能进行生产。CA 机构按照制定好的规则，对智能密码钥匙的唯一标识、RA 机构、订户信息进行管理。CA 机构将严格按照相关管理制度对报废或不合格的存储介质进行处理，对已经下载过证书的存储介质需要报废或者返厂维修时，进行初始化处理，并根据相关流程撤销已经下载的证书，确保未经授权的证书不会被使用。

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

1.CA 密钥对的生成

CA 密钥对包含根 CA 密钥对、OCA 密钥对。对于 CA 密钥对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:

（1）制定根密钥生成计划描述详细的根密钥生成流程和步骤;

（2）根密钥生成和密钥安全保护流程符合 CP 和 CPS 的要求;

（3）根密钥生成过程中执行了计划要求的所有流程和步骤;

（4）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.RA 系统密钥对的生成

RA 系统使用的证书密钥对由符合 GB/T 37092-2018《密码模块安全要求》中的要求的密码模块产生。

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，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 CA 机构的密钥管理系统生成，并通过安全的方式传输给订户。CA 机构的密钥管理系统通过国家密码管理局安全审查，负责为订户提供产生、备份、恢复加密证书密钥等服务。

场景证书的密钥对由负责场景的业务方通过业务系统在可信密码模块中运算生成，并由业务方负责保护场景证书私钥的安全。

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在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、订户知晓的信息（例如订户设置的 PIN）、随机数等运算生成。

CA 机构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，CA 机构拒绝弱密钥申请数字证书。

6.1.2 私钥传送给订户

订户的签名私钥若由订户自己生成时不会进行传送；若由 CA 机构生成时通过安全的离线或在线方式传送给订户。订户委托其他主体产生私钥时，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。

6.1.3 公钥传送给证书签发机构

订户可通过 CA 机构提供的下载服务所建立的安全通道，将公钥发送给 CA 机构，也可通过 RA 系统发送给 CA 系统。

6.1.4 CA 机构公钥传送给依赖方

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

6.1.5 密钥的长度

密钥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 CPS 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

公钥参数由通过密码认证的密码设备生成。CA 机构在采购这类密码设备时，要求密码设备具备相应等级的密码认证证书。CA 机构对生成的公钥参数进行质量检查时，认可使用设备内置的协议和算法已达到标称的安全等级要求。

6.1.7 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），具体配置如下：用于数字签名（包括身份验证）的证书密钥用法设置为数字签名及/或防抵赖；用于密钥或数据加密的证书密钥用法设置为密钥加密及/或数据加密；用于密钥协商的证书密钥用法设置为密钥协商。

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）。

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

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 37092-2018《信息安全技术 密码模块安全要求》二级及以上。

CA 机构制定有专门的《加密机管理办法》，从采购、验收、进出机房、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。

6.2.2 私钥多人控制

CFCA CA 密钥由加密机产生并存放，产生过程有标准的操作脚本，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 位安全管理员中的 3 位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。

6.2.3 私钥托管

CFCA CA 私钥均未在其他地方托管，CA 机构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 CA 机构密钥管理系

统产生保管，密钥管理系统符合商用密码管理规定。

6.2.4 私钥备份

CA 的私钥由 5 位安全管理员中的 3 位人员同时在场操作备份，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。

6.2.5 私钥归档

当 CA 机构的 CA 密钥对到期后，将至少保存五年。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。CA 机构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，CA 机构将按照本 CPS 第 6.2.10 章节所述的方法进行安全销毁。

CA 机构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五年。

6.2.6 私钥导入、导出密码模块

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

6.2.7 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。

6.2.8 激活私钥的方法

CA 机构采用硬件设备（加密机）产生、保存 CA 私钥。CA 私钥激活应由 5 位安全管理员中的 3 位人员同时在场使用其 IC 卡或者智能密码钥匙操作。一旦 CA 私钥被激活，激活状态将保持到 CA 离线。

6.2.9 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。其他情况下进入的非激活状态，需要 5 位安全管理员中的 3 位人员同时在场操作解除私钥激活状态。

6.2.10 销毁私钥的方法

当 CA 的生命周期结束后，CA 机构将根据本 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 位以上可信人员参与下进行安全销毁，并保持安全销毁记录。

6.2.11 密码模块的评估

CA 机构使用通过商用密码产品检测认证的加密机设备，其密码模块至少需要满足密码模块安全要求二级以上要求，并定期对密码模块的安全性进行评估。

6.3 密钥对管理的其他方面

6.3.1 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 4.13 章节的相关规定。

6.3.2 证书操作期和密钥对使用期限

CA 用于签发订户证书的密钥有效期不超过三十年，订户证书有效期最长不超过五年三个月，场景证书最长有效期一天。

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。

6.4 激活数据

6.4.1 激活数据的产生和安装

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

6.4.2 激活数据的保护

CA 机构的 CA 密钥激活数据，由 5 位安全管理员分持，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。安全管理员需要使用 CA 密钥激活数据时，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。

6.4.3 激活数据的其他方面

6.4.3.1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，应保存在 CA 机构最安全区机房。当在某种特殊情况下（如建设灾备系统时）需要进行传输时，其传输传送过程需要在 CA 机构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。

6.4.3.2激活数据的销毁

CA 机构通过对设备进行初始化的方式来销毁 CA 私钥的激活数据。

6.5 数据安全控制

6.5.1 制定安全方案确保数据安全目标

（1）CA 机构采取授权访问的策略和加密签名的手段，确保对 C

A 的控制及证书申请等相关证书数据和证书流程的机密性、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、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）CA 机构将确保其维护的数据符合相应法律规定的其他安全要求。

6.5.2 安全方案定期风险评估

（1）CA 机构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、销毁的内外部威胁;

（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 机构用于控制这些风险的制度、流程、信息系统、技术或其他因素是否足够。

6.5.3 安全计划

CA 机构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，合理地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安全控制措施，涵盖行政、组织架构、技术和物理环境等。制定安全控制措施时，应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。

6.6 计算机安全控制

6.6.1 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、异构防火墙防护、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。

6.6.2 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，并按照网络安全等级保护三级要求执行测评。

6.7 生命周期技术控制

6.7.1 系统开发控制

CA 机构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。

CA 机构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。

6.7.2 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。CA 机构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，在系统上线前清除缺省配置，关闭不需要的端口等。

CA 机构按照 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。

6.7.3 生命期的安全控制

CA 机构制定了日常的审计制度、网络安全等级保护测评、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。

6.8 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）部署边界防火墙设备，对来自外部网络的访问请求进行精细化过滤与访问控制;

（2）依据业务功能划分服务器区域，将不同功能模块的服务器部署在独立的网段，实现逻辑隔离;

（3）采用多级防火墙架构划分安全域，在各安全域间部署严格的访问控制策略与技术手段;

（4）实施基于身份认证的访问控制机制，通过权限分级管理实现数据分级保护;

（5）在网络关键节点部署入侵检测系统，构建实时监测、告警响应、事件处置的全流程安全防护体系;

（6）全网终端统一部署企业级防病毒软件，建立定期自动更新机制，确保病毒库保持最新状态;

（7）关键网络设备和系统采用冗余架构设计，包括硬件冗余、链路冗余等，保障系统高可用性。

6.9 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。

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。证书格式除使用标准域和必需的扩展项外，特定证书将使用私有扩展项，比如场景证书等。

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

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 签名算法

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	
RSA	1.2.840.113549.1.1.1	
sha1WithRSA	1.2.840.113549.1.1.5	
sha256WithRSA	1.2.840.113549.1.1.11	

7.1.5 颁发者

颁发者是签发证书的实体，通过一个非空的甄别名来表示 CFCA 的 CA 名称。颁发者 DN 如下表所示:

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

7.1.6 有效期

证书有效期是一个时间段，在这个时间段内，CFCA 将对证书的状态信息进行维护。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

本项用于描述与主体公钥项中的公钥对应的实体的情况，以主体唯一甄别名 DN 表示。

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

属性	值	说明
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	CN 的值根据 RA 系统的配置可进行脱敏处理。
机构部门（OU2）	通常情况下用于表示证书类型，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	
机构部门（OU1）	通常用于标识 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	
机构（O）	通常表示签发 CA 系统名称，比如 CFCA ACS OCA31；也可以是订户机构法定证件上的名称	
国家（C）	CN	

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

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 CPS 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（AuthorityInfoAccess）

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。

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

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

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（extKeyUsage）

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。CA 机构签发的证书根据不同的证书类型，该项有不同的配置。

7.1.9.8 CRL 分发点

本扩展项描述 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。

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。

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

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 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。

7.3.1 版本号

IETF RFC 6960 定义的 OCSP V1 版。

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 评估的频率或情形

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，变更前后均应进行风险评估；

（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。

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 责任和其他业务条款

9.1 费用

9.1.1 证书生命周期操作相关服务费用

CFCA 直接向订户提供证书签发、补发、换发等服务时，可收取合理相关服务费用，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。

9.1.2 其他服务费用

CFCA 保留收取其他服务费的权利。

9.1.3 退款策略

仅在 CFCA 违反本 CPS 所规定的义务时，订户可以通过其支付费用的通道申请退回其已支付但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，相应的证书将被同步撤销。若因订户原因，在证书服务期内申请退出证书服务体系，CFCA 将不退还剩余有效期间的服务费用。

9.2 财务责任

9.2.1 保险范围

CFCA 根据业务发展情况，同时考虑国内保险种类，自行决定不

同证书类型的投保策略。

9.2.2 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 的规定承担对订户及对依赖方的责任。

9.2.3 对最终订户的保险或保证范围

CFCA 可根据业务发展情况，决定就其电子认证服务为最终订户制定投保策略。无论是否投保，CFCA 对最终订户的损害赔偿责任以《CFCA 电子认证服务协议》约定范围为限。

9.3 业务信息保密

9.3.1 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、审计等活动的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）其他被 CFCA 标注密级的信息。

9.3.2 不属于保密的信息

不属于保密的信息包括:

（1）证书记载信息、CRL 信息;

（2）在提供方披露数据和信息之前，已被接受方所持有的数据和信息;

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

（4）经公开或通过其他途径成为公众领域的一部分数据和信息;

（5）有权披露的第三方，披露给接受方的数据和信息;

（6）其他可以通过公共、公开渠道获得的信息。

9.3.3 保密信息的保护责任

CFCA 通过各种严格的管理制度、流程和技术手段来保护保密信息，包括但不限于商业机密、订户资料、客户信息等。CFCA 的每个员工都要接受信息保密方面的培训。

当 CFCA 在法律法规、监管部门或执法部门的要求下必须依法提供本 CPS 中具有保密性质的信息时，CFCA 应按照要求向监管部门或执法部门提供相关的保密信息，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。

9.4 个人信息保护

9.4.1 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》，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，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。

9.4.2 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。

9.4.3 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。

9.4.4 保护隐私的责任

CFCA、RA 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、监管部门或执法部门通过合法程序要求下，CFCA 可以向监管部门或执法部门提供隐私信息，CFCA 无需承担由此造成的任何责任。

9.4.5 个人信息的收集

CFCA 作为合法的第三方电子认证服务机构，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。CFCA 证书服务的合作方（包括但不限于 RA 机构），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。

9.4.6 个人信息的使用

在与证书服务及应用无关的情况下，CFCA 不会使用订户个人信息。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。

9.4.7 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方式联系 CFCA，CFCA 将在二十个

工作日内回复更正请求;

（3）个人信息的删除：CFCA 按照法律法规要求对订户个人信息进行删除。

9.4.8 个人信息的共享

CFCA 不会以商业目的或在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 经过订户本人书面授权或同意后提供订户个人信息，并有义务要求接收方采取有效手段保护上述信息。

9.4.9 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五年，法律法规另有规定的除外。

9.5 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 制定并发布的 CP、CPS、技术支持手册、证书和 CRL 等的所有权和知识产权均归 CFCA

所有。

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。

9.6 陈述与保证

9.6.1 电子认证服务机构的陈述与保证

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地存放和保护，建立和执行的安全机制符合国家政策的规定。针对预植证书，预植操作人员在全方位视频监控环境下执行预植操作，在出厂前进行质量检查，确保出厂的预植证书符合预植规则。

CFCA 的运营遵守 CPS 并随着业务的调整对 CPS 进行修订。

根据《电子认证服务管理办法》要求，CFCA 将不定期对 RA 机构开展业务是否符合本 CPS 约定进行审计。CFCA 具有保存和使用证书持有人信息的权利。

CFCA 不参与订户及依赖方使用数字证书的具体行为，不承担因

订户及依赖方自身过错使用证书所造成的损害赔偿责任。

9.6.2 注册机构的陈述与保证

作为 CFCA 的 RA 机构，应遵守 CFCA 的 CP、CPS、《注册机构运营管理规范》和有关数字证书服务的合作协议等，并承诺以下事项:

（1）RA 机构向订户告知数字证书申请前的相关事项，使订户明确地知晓并书面同意关于使用 CFCA 数字证书的意义、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）RA 机构按照本 CPS 的规定，审核订户申请材料的真实性、完整性、准确性，并注册用户信息；若订户的证书申请材料审查未通过，则不得受理订户的注册申请;

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

（4）RA 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）RA 机构发放预植证书时，应在对订户进行身份核验后，将预植证书信息与确定的实体进行绑定，并将绑定信息签名后通过安全通道传输给 CFCA，收到 CFCA 的确认信息后，该预植证书才能在应用系统中激活使用。RA 机构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;

（6）RA 机构应全流程确保将预植证书交付给订户之前不被使

用;

（7）RA 机构应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 的电子认证业务合规性审计及监管部门的监督检查;

（8）RA 机构有义务通知订户及时阅读 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《CFCA 电子认证服务协议》内容的前提下，为订户办理数字证书。

9.6.3 订户的陈述与保证及义务

订户确认已经阅读和理解本 CPS 及《CFCA 电子认证服务协议》的全部内容，并同意受此 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 机构协商;

（3）订户应在上述信息、资料发生改变时及时通知 CFCA 或原 RA 机构。如因订户故意或过失提供的资料不真实、不完整、不准确或资料改变后未及时通知 CFCA 或原 RA 机构，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 机构或 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 机构或 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 机构或 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 CPS 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 机构或 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 机构或 CFCA 提出争议处理请求并通知有关各方。

9.6.4 依赖方的陈述与保证及义务

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）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，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。

9.6.5 其他参与者的陈述与保证

未列明的其他参与者应遵循本 CPS 的规定。

9.7 免责声明

（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 不向任何一方承担赔偿或补偿责任;

（3）CFCA 对各类证书的适用范围做了规定，若证书被超出范围使用或被用于其他未被 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。

9.8 CFCA 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《CFCA 电子认证服务协议》。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/或依赖方的任何预期损失或间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失;

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、仲裁机构的裁决或法院的判决承担相应的赔偿责任。

9.9 有效期限与终止

9.9.1 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。本 CPS 自 CFCA 在其官方网站公布的版本中标注的生效日期起生效，除非 CFCA 特别声明 CPS 提前终止。

9.9.2 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）终止日期的三十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。

9.9.3 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。

9.10 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，可通过本 CPS 第 1.5.2 章节中联系方式联系 CFCA。

9.11 修订

CFCA 有权修订本 CPS。CFCA 将定期评估本 CPS 的适用性，并将修订后的版本在官方网站上公布。修订后的版本自版本中标注的生效日期起生效。一经发布，更改即时生效，并对当时及之后获发证书的申请人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。

9.11.1 修订程序

修订程序与本 CPS 第 1.5.4 章节“CPS 批准程序”相同。

9.11.2 通知机制和期限

CFCA 有权修订本 CPS 中的任何术语、条款，修订后将及时公布在 CFCA 网站上。如在修订公布后七个工作日内，订户没有申请对其证书进行撤销，将被视为同意该修改。

9.11.3 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 依据的法律法规和相关主管部门规章变更时，CFCA 将依照有关规定修改本 CPS 的相关内容。

9.12 争议解决

任何一方须在知晓争议情形后的三个月内，向相关方提出争议处理请求，同时将此情况通知相关各相关方。若双方未能在约定期

限内通过协商解决争议，则任何一方均有权将争议提交至北京仲裁委员会，按照该会届时有效的仲裁规则进行仲裁。仲裁裁决为终局，对双方均具有约束力。

此外，任何订户或依赖方若欲向 CA 机构提出索赔诉求，必须在其知道或者应当知道自身权利遭受损害之日起的一年内提出。一旦超出一年期限，该项索赔将不具备法律效力，CA 机构有权拒绝受理。

9.13 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。

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 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。

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

9.15.2 转让

CA 机构、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

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。

9.15.4 强制执行

无强制执行规定。

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，但各方都有义务建立灾难恢复和业务连续性机制。

9.16 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: 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 OCA32	
			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 OCA32	
			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。

附录 B: 证书类型

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企业身份，代表企业对电子信息进行电子签名，利用数字签名防止企业交易信息被篡改，利用数字加密技术保证企业业交易信息的保密性。
	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交换、密钥协商、数据加密等。
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交换、密钥协商、数据加密；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。
	场景证书	一种针对特定业务场景签发的证书，标识参与场景的个人或机构主体，可将特定业务场景中的信息固化至证书扩展域特定字段。使用场景证书对即时业务或者场景业务证据签名后，可证明证据在取证结束后无篡改，并保证多个证据之间的关联性和一致性。场景证书为单场景使用，可用于对即时业务或者场景业务中的证据进行签名。
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（RA）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（RA）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。

	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。

附录 C：定义与缩写

下列定义适用于本 CPS。

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]
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]

[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
[6] GB/T 25069-2022 3.389

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]
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

[7] GB/T 25069-2022 3.576
[8] GB/T 25069-2022 3.119
[9] GB/T 25069-2022 3.121
[10] GB/T 25069-2022 3.120

		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，证书主体还可以是盖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	对不属于证书认证机构（CA）内部的工作人员，但从事 CA 有关业务的人员等独立签约人员。
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。
27	通用名（CN）	是 DN（甄别名）的一个属性，通常用于标识证书主体的名称（入域名、机构名称或者个人姓名）。

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）

[11] GB/T 31508-2015 3.6

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）

附录 D: 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	1.2.840.113549.1.1.11/ 1.2.156.10197.1.501	sha256withRSA 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] e=[电子邮箱地址] 仅邮件证书 ou=[证书类型] ou=[RA 简称] o=CFCA OCA 名称 c=CN	如：cn=CITIC@张三@0110108*******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 个人身份证件信息应做脱敏处理
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、防抵赖 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 = CP Qualifier : [CFCA 电子认证服务证书策略 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/Email 保护/ocsp 签名/代码签名	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	1.2.840.113549.1.1.11/ 1.2.156.10197.1.501	sha256withRSA 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] e=[电子邮箱地址] 仅邮件证书 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、防抵赖 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 = CP Qualifier : [CFCA 电子认证服务证书策略 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	1.2.840.113549.1.1.11/ 1.2.156.10197.1.501	sha256withRSA 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、防抵赖 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 = CP Qualifier : [CFCA 电子认证服务证书策略 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

终端用户（场景证书）		
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	1.2.840.113549.1.1.11/ 1.2.156.10197.1.501	sha256withRSA 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 场景证书由 OCA32 签发
有效期	不早于不晚于	不超过 24 小时
主体名称	cn=[场景参与者信息] ou[2]=[Scene] ou[1]=[收集场景的机构简称] o=CFCA ACS OCA32 c=CN	如：CN = 051@刘成海@A452226********3639@36 位随机数 OU [2]= Scene OU [1]= BOD O = CFCA ACS OCA32 C = CN 个人身份证件信息应做脱敏处理
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、防抵赖	
证书策略	Policy Identifier = [证书类型 oid] Policy Qualifier ID = CP Qualifier : [CFCA 电子认证服务证书策略 URL]	
基本限制	主体类型（Subject type）	最终实体
机构信息访问		
专有扩展		
场景集合（SceneBundle）	完整场景信息哈希值	oid:2.16.156.112554.9.1

根 CA 证书		
属性	**值**	**备注**
版本	X.509 V3	
序列号	1aef3cfbe4464544f64f89a97f23917	
签名算法	1.2.840.113549.1.1.11	sha256withRSA
颁发者	CN = CFCA ACS CA O = China Financial Certification Authority C = CN	
有效期不早于	2015年9月23日 11:24:08	
有效期不晚于	2035年9月28日 11:24:08	
主体名称	CN = CFCA ACS CA O = China Financial Certification Authority C = CN	
公钥	30 82 02 0a 02 82 02 01 00 d8 5b c2 74 e5 bb 4c 5d 4c 8d d6 8a 66 6c a4 f8 7f 7c c9 27 a4 94 aa ee 9a 29 34 f6 5d 63 e9 7d e7 d7 98 a2 f8 ad 85	

	23 b4 7d 61 ab 90 c3 7e 38 b0 e1 fd c2 41 3e a3 0f 0e fa 08 f7 2f b4 30 aa b6 45 b4 e4 53 b2 e7 d7 45 9b 6c 5a 5d cf f4 fa 57 15 22 ae d9 12 d2 ec 75 0b 30 d9 3d dd 1d 65 0e e5 54 b9 dc 19 b7 5d 80 51 96 5a d5 6c 60 e3 b6 d7 ab 8d 79 67 a5 ac fc 2b 84 b8 a4 28 76 ca d7 a7 31 a2 aa 93 ea 70 b9 08 47 1e ec 13 ac bd f4 07 f2 55 2e 40 d1 ef fc 2e 90 b9 8d 31 9e a7 66 65 b2 48 19 c5 4e 67 03 fa c4 33 8d ac 50 18 7f 9d 3e 25 14 55 e4 ab bc be 99 0d 49 2d 21 03 45 55 ce cf 15 d0 20 01 08 c6 c9 81 e6 10 0b 31 ee 13 b5 ea cc 1e f3 cc a0 95 0f 62 c4 9b 17 96 6b da 7a 46 64 8d cc 12 89 98 a8 36 db 66 a4 fe 91 b3 9e ad a5 10 fe 5d 48 60 c5 c4 c2 f8 8f 2f 94 41 63 6c 5b 37 26 73 2a 57 a9 b0 2e 5f 1e e9 00 81 fd 4f 25 48 49 fc e1 23 51 5c fe db 2b 0e ca 37 8b 4f 9a 7e 2e 4f ae dd 60 e6 6a fa d0 36 62 da 14 b1 b3 1b 4b 65 f3 a1 55 3f a4 59 fa 4c e3 52 26 40 32 ed c2 c7 41 60 02 6a 9f ef 69 a3 32 4e 15 ed 8b 1f 86 16 64 e3 6c c1 c1 38 8d d7 3a 67 ad 20 5e 53 b6 5f 4f 1b 30 b3 d1 93 22 d6 b9 e4 03 34 b2 a1 eb 08 dd f6 bd 53 a8 13 3c be 85 61 df cc 9e 7c 68 4f 7f da 42 bc 7a 21 29 14 88 48 50 46 2e 53 aa b8 2d 93 86 a8 d3 56 71 c3 2d ac 2f d9 c2 66 e5 c9 4f 3e 66 b1 5a 5c 62 86 cc 1c 47 d4 af a8 ea 22 fd bd 36 1f b0 2e 12 b0 27 ca 6e 23 07 a2 e8 e3 e6 bb b5 7d ca 51 ae 9a 50 51 63 ed f4 db b1 ae 5a 37 3b 05 e9 1f 57 40 19 cf 3f 50 40 ed 04 f0 ff 38 d3 39 ed 25 69 09 e1 d4 24 b6 51 ed 6a 42 3d 41 b6 77 e4 76 02 73 02 03 01 00 01	
公钥参数	05 00	
标准扩展项		
颁发者密钥标识符	11e178d33820faedebd6239630a87db999db5ff7	
主体密钥标识符	11e178d33820faedebd6239630a87db999db5ff7	
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

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	