中国金融认证中心

电子认证业务规则（CPS）

V3.3

2017 年 10 月

版 本 控 制 表

版本	修改状态	修改说明	修改人	审核人/批准人	生效期
3.0	修改	声明了 J-01 系统下线策略； 增加了 CS 体系的说明；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	孙圣男、赵改侠、张翼	CFCA 安委会	2015年8月
3.1	修改	补充了 ACS CA 系统的说明	赵改侠	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	赵改侠、闫雪娟	CFCA 安委会	2016年6月
3.3	修改	对该体系涉及到的新建子CA系统进行了补充，对GT系统下的OCA21CPS变更调整进行了说明	陶丽雯	CFCA 安委会	2017年10月
3.3	修改	参考WebTrust相关准则，补发及换发可以在证书有效期内不再重新校验身份，只需提交申请表，并在申请表内注明DN即可。已经过期的证书需按照新申请处理，不能按照更新（补发及换发）处理。	孙圣男	CFCA 安委会	2017年10月

目　　录

1 概括性描述

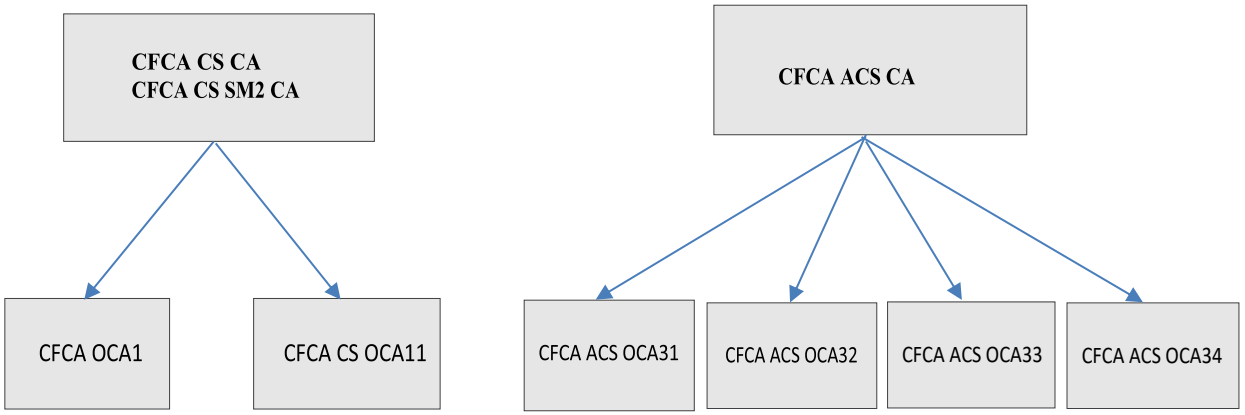
1.1 概述

中国金融认证中心，即中金金融认证中心有限公司（China Financial Certification Authority，英文简称CFCA），于 2000 年 6 月 29 日正式挂牌成立，是经中国人民银行和国家信息安全管理机构批准成立的国家级权威的安全认证机构，是重要的国家金融信息安全基础设施之一，也是《中华人民共和国电子签名法》颁布后，国内首批获得电子认证服务许可资质的电子认证服务机构之一。

电子认证业务规则（CPS，Certification Practice Statement）是关于认证机构（CA，Certificate Authority）在全部数字证书（以下简称证书）服务生命周期（如签发、吊销、更新）中的业务实践所遵循规范的详细描述和声明， 是对相关业务、技术和法律责任方面细节的描述。

本 CPS 是在原电子认证业务规则 V3.2 的基础进行完善修订。2010 年国家密码管理局发布了电子认证服务系统升级改造的通知，CFCA 按照通知要求，由国家密码管理局批准，将电子认证服务系统由 V1.0 升级为 V2.0。原电子认证服务系统（CFCA J-01 系统）V1.0 上的客户将逐步迁移至新系统上，原系统将于 2018 年 11 月停止证书申请服务，2018 年 11 月至 2019 年 11 月 21 日将只提供证书吊销及 CRL 发布服务，2019 年 11 月 21 日彻底停止服务。

CFCA 电子认证服务系统V2.0 主要包含了 CFCA 如下 CA 系统，结构如下图所示。



CFCA 的所有 CA，包含子 CA 均由CFCA 所有，由 CFCA 完全直接控制。该CPS下所包含的CA系统会根据业务发展需要进行调整，每次调整均需对CPS进行更新。因CFCA GT系统不再适用webtrust标准，CFCA GT下的OCA21适用于该CPS。

本文档的编写遵从 IETF RFC 3647(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 公钥基础设施证书策略和证书运行框架)、《中华人民共和国电子签名法》、国家密码管理局颁布的《证书认证系统密码及相关安全技术规范》、《电子认证服务密码管理办法》，中华人民共和国工业和信息化部颁布的《电子认证服务管理办法》、《电子认证业务规则规范(试行)》运作规范。

CFCA 获取了主管单位中华人民共和国工业和信息化部颁发的电子认证服务许可及国家密码管理局颁发的电子认证服务使用密码许可证等资质，并处于资质有效期内。

1.2 文档名称与相关标识

此文档的名称为《CFCA 电子认证业务规则(CFCA CPS)》。

CFCA 向国家OID 注册管理中心注册了相应的对象标识符（OID），本文档的OID 为：2.16.156.112554.1。

1.3 电子认证活动参与者

本文中所包含的电子认证活动参与者有：电子认证服务机构、注册机构、订户、依赖方以及其它参与者，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 CA（Certificate Authority）承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或CRL）发布、政策制定等工作。

1.3.2 注册机构

注册机构RA(Registration Authority)负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

CFCA 与合作机构签署“数字证书合作协议”，合作机构可成为 CFCA 的注册机构，承担本 CPS 中注册机构的义务。注册机构应遵循 CFCA 的《注册机构运营管理办法》中的相关要求。

CFCA 本身也承担RA 职责，订户可直接向 CFCA 提出证书申请。

1.3.3 订户

订户是指向CFCA申请证书的实体。

需要明确的是，证书订户与证书主体是两个不同的概念。“证书订户”是指向 CFCA 申请证书的实体，通常为个人或机构，即为“最终用户”；“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。

1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.3.5 其它参与者

除电子认证服务机构（CFCA）、订户和依赖方以外的参与者称为其它参与者。

1.3.6 受益者及责任

CFCA CA 证书相关联的参与者均为受益者。

1.受益方

CFCA CA 下的证书可以为下述机构提供信赖保证：

（1）所有提交证书协议的订户

（2）获取证书的申请者

（3）获取证书的软件供应商

（4）证书在生效期间的信赖方

2.CFCA CA 下的证书可提供的保证：

（1）证书拥有者的合法存在性

（2）证书拥有者的身份经过有效识别

（3）证书中关于证书拥有者信息的准确性

（4）证书状态 7*24 小时可查询

（5）CA 根据CPS 规则，废止不符合生效条件的证书

1.4 证书应用

1.4.1 证书类型及适合的证书应用

CFCA CS CA、CFCA ACS CA 为离线CA 系统，仅签发中级 CA 证书以及必要的OCSP 签名证书，不签发最终用户证书。

CFCA OCA1 支持签发SM2-256、RSA-1024、RSA-2048 密钥类型的企业证书、个人证书、SSL 服务器证书、VPN 证书、代码签名证书、邮件证书和设备证书等。系统的签名算法采用 SM2/SM3 RSA-2048/SHA1。

CFCA CS OCA11 主要作为CFCA 原电子认证系统J-01 系统（该系统将于 2019 年 11 月到期）的证书迁移目标系统，支持签发SM2-256、RSA-1024、RSA-2048 密钥类型的证书。系统的签名算法采用 SM2/SM3 或者RSA-2048/SHA1。

CFCA OCA21为原全球信任体系CFCA GT下的子CA系统，该系统已不再适用于webtrust标准，不再接受新客户接入。该系统下的客户可根据SHA-256密码算法升级进度，迁移至其他系统。当前该系统支持签发SM2-256、RSA-2048 密钥类型的企业证书、个人证书。系统的签名算法采用SM2/SM3 或者RSA-2048/SHA1。

CFCA ACS OCA31 主要用于满足金融领域客户RSA-2048/SHA256 密码算法的需求，可以签发 RSA-2048、SM2 密钥类型的证书。系统的签名算法采用 SM2/SM3 或者RSA-2048/SHA256。

CFCA ACS OCA32 主要用于签发 CFCA 场景证书，签发RSA-1024、RSA-2048、SM2 密钥类型的证书。系统的签名算法采用SM2/SM3 或者RSA-2048/SHA256。

CFCA ACS OCA33 主要用于满足不同领域客户RSA-2048/SHA256 密码算法的需求，可以签发RSA 2048/SHA256 及 SM2/SM3密钥类型的个人证书、企业证书、设备证书等。系统的签名算法采用 SM2/SM3 或者RSA-2048/SHA256。

CFCA ACS OCA34 主要用于满足特定行业客户RSA-2048/SHA256 密码算法的需求，可以签发RSA 2048/SHA256 及 SM2/SM3密钥类型的个人证书、企业证书等。系统的签名算法采用 SM2/SM3 或者RSA-

2048/SHA256。

本CPS 下的所有SM2 证书可以和国家根形成完整的证书链。

1.4.1.1 个人证书

个人证书用于区分、标识、鉴别个人身份的应用场合。个人证书分个人普通证书、个人高级证书和个人复合证书。个人普通证书用于个人身份识别及签名。个人高级证书可用于个人身份识别以及在应用过程中进行加密、签名等活动，以实现信息保密性、完整性和不可抵赖性。个人复合证书由一张 RSA 签名证书和一张 SM2 签名证书和一张 SM2 加密证书组成，应用于银行密码算法过渡期使用。CFCA 个人证书由 CFCA OCA1、CFCA CS OCA11 、CFCA OCA21、CFCA ACS OCA31、CFCA ACS OCA33签发。

1.4.1.2 企业证书

企业证书用于区分、标识、鉴别企业身份的应用场合。企业证书分企业普通证书、企业高级证书和企业复合证书。企业普通证书用于标识企业身份以及各种签名；企业高级证书可用于标识企业身份，在应用中进行数据加解密、合同、订单等的签名验签，以实现信息保密性、完整性和不可抵赖性。企业复合证书由一张 RSA 签名证书和一张 SM2 签名证书和一张 SM2 加密证书组成，应用于银行密码算法过渡期使用。CFCA 企业证书由 CFCA OCA1、CFCA CS OCA11 、CFCA OCA21、CFCA ACS OCA31、CFCA ACS OCA33签发。

1.4.1.3 SSL 服务器证书

SSL 服务器证书：该类证书包含通配符证书、多域名证书类型。该类证书适合应用在网上银行、电子商务、电子政务、企业信息化以及公共服务等各领域，用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露；

订户或依赖方可以通过服务器证书验证公司网站所访问的网站是否真实可靠，实现网站身份的真实性确认，为建设网络信任环境提供基础性信任服务。SSL 服务器证书由 CFCA OCA1 或者 CFCA ACS OCA31 签发，密钥长度为RSA-2048 或者 SM2-256。

1.4.1.4 VPN 网关证书

用于标识 VPN 网关，实现客户端与 VPN 网关之间的认证及交互数据的安全传输。VPN 网关证书由 CFCA OCA1 或者CFCA ACS OCA31 签发。

1.4.1.5 代码签名证书

代码签名证书：对代码拥有者的身份进行标识，用于代码发行中的签名， 以保护代码的完整性和安全性；也可应用于普通公文中的电子印章等，表明签发者的真实意图，并保障所签发内容的完整性和不可抵赖性。CFCA 代码签名证书由CFCA OCA1 或者 CFCA ACS OCA31 签发。

1.4.1.6 安全邮件证书

将邮件地址与证书申请者信息进行绑定，以实现邮件地址拥有者的身份认证，以及邮件传输中信息的加解密、签名等操作。CFCA 安全邮件证书由 CFCAOCA1 或者CFCA ACS OCA31 签发。

1.4.1.7 设备证书

用于标识各种设备，实现设备标识以及交互数据的加解密功能，保证传输数据的完整性、安全性等。CFCA 设备证书由 CFCA OCA1、CFCA ACS OCA31或者CFCA ACS OCA33签发。

1.4.1.8 CFCA 预植证书

CFCA 预植证书是 CFCA 的一项扩展业务。CFCA 与注册机构签订合作协议，注册机构根据其业务需要，委托 CFCA 为其用户在安全的环境下生成证书，再由注册机构对订户身份的真实性进行审核，然后将事先

生成的证书与注册机构的用户信息进行绑定，该证书方可用于注册机构的相关应用。CFCA 预植证书可由CFCA OCA1 、CFCA CS OCA11、CFCA OCA21或者CFCA ACS OCA31 签发。

个人证书、企业证书可以是 CFCA 预植证书。此处的预植证书是指由 CFCA 按照本 CPS7.1.4 的规则定义证书 DN （Distinct Name）后，预先在安全的存储介质（如 USBKey） 中生成并植入的数字证书；订户申领该证书时，注册机构须对订户的身份进行审核，将证书的 DN 信息与订户的身份信息绑定，并与应用系统进行关联。当预植证书与订户身份信息的绑定信息经注册机构和CFCA 数字签名确认后，该预植证书方可激活使用。

此处的绑定是指注册机构通过安全的通道将预植证书的 DN 信息与订户的身份信息（包括但不限于姓名、证件类型、证件号码）签名后传送给 CFCA，CFCA 在其预植服务器的数据库中建立订户与证书的对应关系，以确定预植证书对应的实体。

此外的关联是指将预植证书的信息与应用系统的信息（包括但不限于发证机构名称、应用系统类型等）在应用数据库中建立对应的关系，以便使该证书用于特定的应用当中。

CFCA 预植证书可以通过在不同的注册机构的应用中进行绑定，以便在多种应用中使用。

1.4.1.9 CFCA 场景证书

CFCA 场景证书是CFCA 的一项扩展业务。

CFCA 场景证书是一种适用于对即时业务或者特定场景业务进行签名认证的数字证书。在业务结束时自动申请，将业务场景中所有信息整合形成数字证书的扩展域信息。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。

场景证书使用时不限制签名次数，也不限定特定文档，可用于对即时业务或者场景业务中的所有证据分别签名。脱离该场景后，证书即不能使用。CFCA 场景证书由CFCA ACS OCA32 签发，签名算法为 RSA-2048/SHA256 或者 SM2/SM3。

1.4.1.10 云证通证书

CFCA 云证通证书是 CFCA 的一项扩展业务。

CFCA 云证通证书是用户通过云证通 APP 申请的用于移动应用的数字证书，主要应用于手机银行、P2P 以及电子政务等领域数字证书应用。

CFCA 云证通证书由 OCA31 进行签发，密钥类型为 RSA-2048 或者 SM2，签名算法为 RSA-2048/SHA256 或者 SM2/SM3。

1.4.2 受限的证书应用

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书扩展项限制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。

任何未经CFCA认可的证书应用都将不受CFCA的保护。

1.4.3 禁止的证书应用

CFCA 签发的证书不能在如下领域使用：任何与国家或地方法律、法规规定相违背的应用系统，以及任何未经过安全检测的环境及应用。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的策略文档管理机构为 CFCA 风险管理与合规部。当需要编写或修订本 CPS 时， 由风险管理与合规部牵头组织相关人员成“CPS 编写组”，总经理也可以根据需要临时设立。

“CPS 编写组”，并指定编写组负责人。

1.5.2 联系方式

如对本 CPS 有任何疑问，请与CFCA 风险管理与合规部联系：

电话： 010-50955020

传真： 010-63555032

邮件：cps@cfca.com.cn

地址：中国北京西城区菜市口南大街平原里 20-3

1.5.3 决定 CPS 符合策略的机构

“CPS 编写组”拟定初稿或修订稿后，交由公司“安全管理委员会”审议，“安委会”将负责评估 CPS 是否符合相关要求，如果符合，将报总经理审批。总经理审批同意后，本 CPS 方可对外发布，并自发布之日起 20 天内向行业主管部门报备。

1.5.4 CPS 批准程序

“CPS 编写组”负责起草 CPS 形成讨论稿，并征求公司领导和各部门负责人意见，经讨论、修改达成一致意见后形成送审稿。

“CPS 编写组”负责将 CPS 送审稿提交公司“安委会”审阅。在取得“安委会”评审意见后，“CPS 编写组”据此进行修改并提交风险管理与合规部，由风险管理与合规部确定CPS 文本格式和版本号，形成定稿。

CPS 定稿经公司各部门负责人及分管领导审阅后，报总经理审批。总经理审批同意后，方可对外发布 CPS。发布形式应符合行业主管部门等相关主管部门要求，包括但不限于公司网站(http://www.cfca.com.cn)公布和向客户或合作对象书面提交。发布工作由风险管理与合规部协调相关部门完成。

CPS 的网上发布遵照《中金金融认证中心有限公司网站管理办法》执行。自 CPS 发布之日起，所有以各种形式对外提供的 CPS 必须与网站公布的 CPS 保持一致。风险管理与合规部负责自发布之日起 20 天内向行业主管部门报备。

风险管理与合规部定期对 CPS 的内容进行审查（通常为一年一次），以确定是否需要进行修订。各部门也可根据业务发展变化需要及时向风险管理与合规部提出修订申请。本 CPS 也可以根据所遵循标准的要求，提出修订申请。

当修订内容具有重大变更时，CFCA 将按照与初次编写相同的流程进行；当修订内容变动较小时，由风险管理与合规部修订完成后报各部门负责人及公司领导审阅， 并经总经理审批同意后立即在公司网站上发布。每次修订完成后均需由风险管理与合规部自发布之日起 20 日内向行业主管部门报备。

1.6 定义和缩写

见附录《定义和缩写》。

2 信息发布与信息管理

2.1 信息库

CFCA 信息库面向订户及证书应用依赖方提供信息服务。CFCA 信息库包括但不限于以下内容：证书、CRL、CPS、CP、证书服务协议、技术支持手册、CFCA 网站信息以及CFCA 不定期发布的信息。

2.2 认证信息的发布

CFCA 的 CPS、CP 以及相关的技术支持信息等在 CFCA 网站上发布。用户证书可通过CFCA 证书下载平台获取；已被吊销了的证书的信息可从

CRL 站点查获， 证书的状态（有效、吊销、挂起）可通过 OCSP 服务获得。

2.3 发布的时间或频率

CPS、CP 以及相关业务规则在完成 1.5.4 所述的批准流程后的 15 个工作日内发布到CFCA 网站上，并可确保 7*24 小时可访问。

2.4 信息库访问控制

CFCA 的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

CFCA 签发的证书根据证书类别的不同，签发的证书主体名字可能是域名、代码标记名称、证书订户的真实名称、设备名称等，命名符合 X.500 定义的甄别名规范。DN 的详细说明见本CPS 的 7.1.4。

3.1.2 对名称意义化的要求

DN（Distinguished Name）：唯一甄别名，在数字证书的主体名称域中，用于唯一标识证书主体的 X.500 名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

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。

企业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。

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

外网IP，结合该订户的其他信息一起被鉴别和认证。

VPN 网关证书、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或者设备的IP 地址，结合该订户的其他信息一起被鉴别和认证。

安全邮件证书的甄别名称的通用名必须是真实名称，邮件地址必须是有效的地址。

代码签名证书的甄别名称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 将对有效证件进行鉴别。

对于预植证书，其证书甄别名称中包含标识审核订户身份的注册机构相关应用系统信息标识，订户信息将与该注册机构应用系统中的订户标识一起被鉴别和认证。

场景证书的甄别名称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。

云证通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

DN 的命名规则由CFCA 定义，详见本CPS 7.1.4 的说明。

3.1.5 名称的唯一性

CFCA 保证其签发的证书，其主题甄别名，在 CFCA 的信任域内是唯一的。

3.1.6 商标的识别、鉴别和角色

CFCA 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证明订户拥有私钥的方法是通过 pkcs#10 所包含的的数字签名来完成的。

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，以此来判断订户拥有私钥。

3.2.2 订户身份的鉴别

订户在申请证书前应指定并书面授权证书的申请代表，提供有效身份证明文件、证书申请文件，并接受证书申请的有关条款，同意承担相应的责任。

CFCA 接受订户的证书申请后，应对订户的身份真实性进行审核，并按照相关法律法规的要求妥善保存订户申请材料。

CFCA 对订户身份的鉴别过程如下：

CFCA 客户经理收集订户的申请材料，风险管理与合规部审核员对订户材料及身份进行审核，RA 系统操作员录入订户申请信息、RA 系统审核员审核操作员录入信息并协助订户下载证书。

3.2.2.1 个人订户身份的鉴别

个人订户申请证书时，应向 CFCA 或者 CFCA 的注册机构提供真实有效的个人身份证明文件。对于机构中的个人证书申请者，其申请材料中需要加盖公章或者授权等证明材料。CFCA 将对该组织机构进行鉴别。

个人应提交如下材料：

1、证书申请表

2、身份证复印件

3、机构授权证明材料（仅机构中的个人证书申请）

审核员检查订户提交材料的完整性、真实性。并通过可信数据源验证订户身份信息、地址信息、国家信息等进行鉴别。

3.2.2.2 企业订户（机构订户）身份的鉴别

机构订户在申请证书前应授权本机构工作人员向 CFCA 或者 CFCA 的注册机构提出证书申请，并向 CFCA 提供真实有效的机构身份证明文件。

企业（机构）应提供如下材料：

1、证书申请表

2、至少一种机构身份证件

3、申请人的个人身份证件

4、机构授予申请人的授权证明

以上材料需加盖公章。

CFCA 对于机构订户身份的鉴别流程为：

首先，CFCA 指定证书申请材料接收人员接收申请材料，进行初步的完整性检查，确保材料符合身份鉴别要求。

其次，CFCA 指定专门的证书鉴证人员对订户的申请材料进行鉴证，其鉴证的方式为：

（1）对于机构提供的身份证明文件、地址信息、国家信息等，可通过可靠数据源鉴别真实性。（2）确认该机构是否授权申请证书。可通过电话、公函等进行确认。

3.2.2.3 SSL 服务器证书订户身份的鉴别

订户如需要申请普通 SSL 服务器证书，只能向 CFCA 提交申请，CFCA 可以受理机构订户、个人订户的申请。普通 SSL 服务器证书可以包含多域名、通配符证书。订户申请SSL 服务器证书时，应提交如下材料：

1、证书申请表

2、至少一种机构身份证件（个人订户不适用）

3、申请人的个人身份证件

4、机构授予申请人的授权证明（个人订户不适用）

5、拥有公网IP 的证明（域名型的不需要）

6、证书申请CSR 文件

CFCA 除对申请者的身份、地址信息、国家信息等进行鉴别外，还要对域名或者外网IP 及CSR 合规性进行鉴别。其鉴别流程方法如下。

通过域名注册信息查询(whois)功能，得到所申请域名证书的域名注册者资料，查看域名注册者是否和域名证书申请者一致，初步审核确定域名证书申请者确实拥有此域名。如域名申请者与在（whois）查询到的结果不一致，则订户可提供授权证明或者 CFCA 采取邮件方式询问是否授权给证书申请者使用。

对于公网 IP 的鉴别，订户可提供 ISP 商分配 IP 的纸质盖章证明材料或者ISP 的邮件证明材料。

如果申请通配符域名证书，CFCA 将鉴别其拥有的二级域名。对于多域名证书，CFCA 将对所有列举的域名进行鉴别。对于 CSR 文件的鉴别主要包含，CSR 中的信息是否与申请表中的申请信息一致，是否符合相关规范，比如 DN 的顺序等，并验证其是否拥有私钥。

3.2.2.4 代码签名证书申请的身份鉴别

订户如需要申请代码签名证书，只能向 CFCA 提交申请，CFCA 受理个人用户和机构订户申请该类证书。代码签名证书应提交如下材料：

1、证书申请表

2、至少一种机构身份证件（申请企业/组织证书）（个人不需要）

3、申请人的个人身份证件

4、机构授予申请人的授权证明（申请企业/组织证书）

CFCA 对申请者的身份、地址信息、国家信息等进行鉴别，其鉴别方法如下： 如果验证对象为企业，需验证用户企业的合法性、企业的实体存在和商业行为的存在（此企业有正常的商业行为），还要认证申请人是否有资格代表企业， 不对其代码进行鉴别。

3.2.2.5 其他证书类型的身份鉴别

针对设备证书、VPN 证书等，需要鉴别申请者的身份、地址、国家，不对其设备进行验证。

针对安全邮件证书，CFCA 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， 同时鉴别申请人的身份信息、地址、国家等信息。

针对预植证书、场景证书以及云证通证书的鉴别参照个人身份、企业身份方法进行鉴别，也可以采取适当的自动鉴别方式。

3.2.2.6 允许的证件类型

个人证件类型	机构证件类型
居民身份证	税务登记证
护照	组织机构代码证
社会保障卡	企业营业执照
港澳居民往来内地通行证	统一社会信用代码证
台湾居民来往大陆通行证	事业单位法人证书
户口簿	社会团体登记证书
临时居民身份证	民办非企业登记证书
外国人永久居留证	外国（地区）企业常驻代表机构登记证
	政府批文

3.2.3 没有验证的订户信息

CFCA 签发的证书信息没有未经过验证的信息。

3.2.4 授权确认

当申请者代表组织机构订户申请证书时，需要出示足够的证明信息以证明申请者是否已获得组织机构的授权。CFCA 有责任确认该授权信息，并将授权信息妥善保存。

3.2.5 互操作准则

对于申请该CPS 下的证书订户，CFCA 可委托其注册机构承担对订户身份的鉴别职能，CFCA 将不再进行其他鉴别。

3.3 密钥更新请求的标识与鉴别

证书密钥更新有两种情况：补发和换发。

1、证书补发

补发是指在证书有效期内，订户更新证书的操作。

以下情况订户需要申请证书补发：

（1）订户证书丢失或损坏，例如存放证书的介质损坏；

（2）订户认为原有证书和密钥不安全（例如订户怀疑证书被盗用或密钥受到了攻击）；

（3）其它经CFCA认可的原因。

当订户需要补发证书时，应主动向 CFCA 的注册机构提出证书补发申请。在证书的有效期内需进行补发的，订户无需提交身份验证材料，仅需提交证书申请表，注明原证书的DN。CFCA 仅通过订户初次申请时的信息进行身份验证即可。订户仅需要向 CFCA 重新提交CSR，CFCA 校验后发放新的证书。超过有效期后，则需对订户身份进行重新验证。验证流程及要求与初次申请相同。

证书补发时新证书有效期从补发操作起到原证书失效日止。

2、证书换发

换发是指在证书将要过期的三个月内或证书过期后，订户申请更新原证书DN有效期的操作。

证书换发时需要对订户身份进行重新验证。重新验证订户身份的验证流程及要求与初次申请相同。

证书换发新证书有效期将从证书换发之日起至原证书到期为止再另加一个证书有效周期（已经过期的证书换证，其有效期仅为证书有效周期）。

为保障用户在执行证书更新期间服务不受到影响，在 SSL 服务器证书更新 30 天后吊销原有证书。而其他证书会在证书更新时立即吊销原有证书，并发布

CRL 信息。

3.3.1 常规密钥更新的标识与鉴别

同 3.3。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新等同于订户重新申请证书，其要求与 3.2.2 相同。

3.4 证书变更

证书变更是指订户在不改变现有公钥的情况下重新申请一张证书。CFCA 不提供证书变更服务，即订户对证书进行更新时其密钥对必须重新生成。

3.5 吊销请求的标识与鉴别

证书吊销请求的标识与鉴别流程见本CPS 的 4.7。

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

任何实体需要使用CFCA 的证书时，均可向CFCA 的注册机构提出证书申请。

4.1.2 注册过程与责任

1、最终订户

最终订户即申请证书的实体，最终订户须明确表示其愿意接受本 CPS 及相关的 CP 中所规定的相关责任与义务（本 CPS 及相关 CP 公布在 CFCA 网站上），并需要按照 3.2.2 的要求提供真实、准确的申请信息； 根据《中华人民共和国电子签名法》的规定，申请者未向 CFCA 的注册机构提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、CFCA 或者 CFCA 的注册机构造成损失的，订户应承担相应的法律及赔偿责任。订户有责任保护其拥有的证书私钥安全。

2、认证及注册机构

CFCA 既是一个 CA，同时也承担注册机构的职能，如订户可以直接向 CFCA 申请证书，由 CFCA 审核订户信息并处理订户的请求。CFCA 的注册机构对订户提供的身份信息参照 3.2.2 的要求进行鉴别，并记录订户申请时的相关信息，通过 RA 系统向 CA 系统发送请求，CFCA 的 CA 系统校验 RA 请求的格式及权限， 并对通过鉴别后的订户签发证书。CFCA 及其注册机构，应妥善保管证书订户申请信息。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

1. CFCA 处理证书申请至少需要设置 3 个可信角色：信息收集、信息验证、签发证书。

其中信息收集、信息验证可以由同一人完成；但签发证书人员需要与信息收集、信息验证职责分离。

2. 对于证书申请处理，签发证书人员需对申请机构信息做最终审核：

1）对所有用以验证申请机构证书申请的信息和文件进行复核，查找冲突的信息或需要进一步验证的信息；

2）如复核人提出的问题确实需要得到进一步验证，CFCA 必须从申请机构、协议签署人、申请审批人或其他合格的独立信息来源取得进一步验证的资料或证据；

3）CFCA 必须保证已收集的与证书申请相关的信息和资料，足以确保签发的证书不包含 CFCA 已知或应发现的错误信息，否则 CFCA 将会拒绝证书的申请并通知申请机构；

4）如果部分或所有的身份验证资料内容使用语言不是 CFCA 的官方语言，那么CFCA 将会使用经过适当的培训、具备足够的经验和判断能力的人员完成最终

的交叉审核和尽职调查。CFCA 通过以下方法执行交叉审核与尽职调查：

1）依赖翻译的材料内容；

2）依赖拥有此语言能力的第三方机构完成此步骤，CFCA 复核第三方机构的检查结果，并且符合证书标准中的 CFCA 自我审核要求。

CFCA 注册机构执行识别与鉴别功能时，可结合自身鉴别特点，参照 CFCA 执行鉴别方法。

4.2.2 证书申请批准和拒绝

CFCA 按照 3.2.2 的要求对订户提交的申请材料及其身份信息进行鉴别，经鉴别符合要求后，将批准申请。若鉴别未通过，CFCA 及注册机构将拒绝其申请，及时通知申请者并告知拒绝原因。

4.2.3 处理证书申请的时间

CFCA 及其注册机构将在合理的时间内完成证书申请处理。在申请者提交的资料齐全且审核通过的情况下，1个工作日处理完成。

针对场景证书和云证通证书等扩展业务的申请，即时处理。

4.2.4 证书签发行为

在订户申请通过鉴别后，CFCA RA 系统操作员录入订户申请信息，并提交 RA 系统审核员审核；CFCA RA 系统审核员审核通过后，向 CA 系统提交申请；CA 系统向 RA 系统返回证书下载凭证码或证书，CFCA RA 系统审核员将下载的证书发放给订户。

来自 CFCA 注册机构的申请操作可参照 CFCA 的执行。注册机构也可结合自身业务特点，在安全可控的情况下，直接录入订户申请信息校验无误后向 CA 系统提交申请，获得证书下载凭证或者直接下载证书。注册机构应通过安全的方式将证书下载凭证或者存放证书的智能密码钥匙交付给订户。订户如收到证书下载凭证，应在下载凭证有效期 14 天内下载证书，并将证书下载在安全的介

质内。CFCA 官方网站提供证书下载服务，用户也可直接访问 https://cs.cfca.com.cn 下载证书，证书下载成功后，即表示签发完成。

针对预植证书的签发，将由 CFCA 在安全可控的环境下按照一定的规则预先将证书签发并下载在智能密码钥匙中。

4.2.5 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，CFCA 及其注册机构有义务告知订户申请结果。可通过电话、电子邮件或其他方式对订户进行通告。

4.3 证书接受

4.3.1 构成接受证书的行为

订户填写证书申请表，申请表同意本 CPS 中的约定即可视为双方签订了购买数字证书的协议。订户向 CFCA 提供真实、准确的申请信息，经 CFCA 审核通过后，CFCA 向订户签发证书；订户应对收到的证书与其申请信息进行核对，确认无误后方可使用。自用户收到证书后 1 个工作日内无意见的即视为订户已经接受此证书。如订户在自行下载证书的过程中因各种原因未获得证书，但 CA 系统显示证书已经签发，如 CA 系统显示已签发时间超过 1 个工作日，则视同为订户已接收了证书。订户可联系 CFCA 客服人员协助解决证书下载问题。

4.3.2 电子认证服务机构对证书的发布

对于最终订户证书，CFCA 将根据用户的意愿采取适当形式发布，订户没有要求发布的，CFCA 将不发布最终订户证书。

4.3.3 电子认证服务机构对其他实体的通告

对于 CFCA 签发的证书，CFCA 不对其他实体进行通告，依赖方可以在信息库上自行查询。

4.4 密钥对和证书的使用

4.4.1 订户私钥和证书的使用

订户的私钥和证书应用于规定的、批准的用途（在本 CPS1.4.1 节定义），订户在使用证书时必须遵守本 CPS 的要求，妥善保存其私钥，避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。

1、 证书持有者的私钥和证书使用

证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者只有在接受了相关证书后才能使用对应的私钥，并且在证书到期或被吊销后，须停止使用该证书及对应的私钥。

2、 依赖方的公钥和证书使用

当依赖方接受到签名的信息后，应该：

- ✧ 获得对应的证书及信任链；
- ✧ 验证证书的有效性；
- ✧ 确认该签名对应的证书是依赖方信任的证书；
- ✧ 证书的用途适用于对应的签名；
- ✧ 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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

4.4.2 依赖方对公钥和证书的使用

依赖方信赖CFCA 签发的证书所证明的信任关系时需要：

1、获取并安装该证书对应的证书链；

2、在信赖证书所证明的信任关系前确认该证书为有效证书，包括：检查CFCA 公布的最新 CRL，确认该证书未被吊销；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；

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。

4.5 证书密钥更新

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书。

4.5.1 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、其它可能导致密钥更新的情形。

4.5.2 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。

4.5.3 证书密钥更新请求的处理

同 3.3。

4.5.4 颁发更新证书时对订户的通告

同 4.2.5。

4.5.5 构成接受密钥更新证书的行为

同 4.3.1。

4.5.6 电子认证服务机构对密钥更新证书的发布

同 4.3.2。

4.5.7 电子认证服务机构对其他实体的通告

同 4.3.3。

4.6 证书变更

CFCA 不提供证书变更服务。

4.7 证书吊销和挂起

4.7.1 证书吊销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被吊销：

1)订户书面申请吊销数字证书；

2)订户通知 CA 最初的证书申请未经有效授权；

3)订户相信或怀疑密钥泄漏或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者 CA 有证据表明订户证书私钥泄露的情形；

4）当 CA 有证据表明订户将证书使用于法律、行政法规定义为非法事项上，如代码签名者签发了可疑、恶意代码，或者 CA 发现订户证书未恰当使用；

5）当 CA 有证据表明订户未履行本 CPS 或订户协议中约定的义务；或者订户证书不符合本 CPS 的相关要求，如发现存在签名的恶意代码，或者密钥泄露，必须第一时间通知 CA；

6）当 CA 有证据表明订户已丧失证书中域名的使用权，或订户未能更新其域名使用权；

7）CA 获知通配符证书被用于验证具有欺诈误导性质的域名；

8）CFCA 取得了合理证据表明或意识到订户证书中的重要信息内容已经变更；

9）CA 正式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；

10）CA 认定证书中所显示的信息为不准确或具有误导性；或者订户申请证书时，提供的资料不真实；

11）CFCA 因某些原因停止业务，并且没有安排其他的 CA 提供证书吊销服务；

12）当 CFCA 从事电子认证业务的资格被吊销后，CFCA 除继续维持CRL/OCSP信息库的情况外，将吊销或终结所有已签发的证书；

13）CFCA 用于签发证书的 CA 证书私钥可能被泄露时，将根据应急预案吊销所有已签发的证书；

14）CFCA 取得了合理证据表明或意识到订户已经被列在相关的黑名单中，或其经营地区被CFCA 所在国家的监管机构禁止；

15）证书的重要参数被国际国内主流标准认为有重大风险时；

16）法律、行政法规规定的其他情形。

4.7.2 请求证书吊销的实体

已申请CFCA 证书的订户可请求证书吊销。

同时， CFCA 也可在 4.7.1 所述的情形下主动吊销订户的证书。

4.7.3 请求吊销的流程

吊销分为主动吊销和被动吊销。主动吊销是指由订户提出吊销申请，由CFCA 或CFCA 注册机构审核通过后吊销证书的情形；被动吊销是指当 CFCA 确认订户违反证书应用规定、约定或订户主体已经消亡等情况发生时，采取吊销证书的手段以停止对该证书的证明。在代码签名证书中，如果一个证书对应一个软件，那么吊销证书只影响这一个软件，如果一个证书对应多个软件，那么一旦证书被吊销所有软件都会受影响。

1 主动吊销

订户申请吊销证书前应指定并书面授权证书吊销申请代表，提供有效身份证明文件及证书吊销申请文件，并接受证书吊销申请的有关条款，同意承担相应的责任。

CFCA 7*24 小时接受订户证书吊销申请，并处理订户证书吊销请求。订户可通过CFCA 7*24 热线、CFCA 在线服务等方式提出申请。

CFCA 收到订户的吊销申请材料后，将查询订户需吊销的证书是否为 CFCA 所发放，证书是否在有效期内，吊销理由是否属实，若均通过则对证书进行吊销。

2 被动吊销

当出现被动吊销的情形时，CFCA 将以适当形式通知订户，告知拟吊销的证书内容、吊销原因、吊销操作时限等事项，在确认订户收到吊销通知且无异议后予以吊销。

4.7.4 吊销请求宽限期

在主动吊销的情形下，订户一旦发现需要吊销证书，应及时向 CFCA 提出吊销请求。

在被动吊销的情形下，订户在收到吊销通知后的 3 个工作日内可向 CFCA 提出申辩理由，CFCA 将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在 3 个工作日内未回复或回复无异议则 CFCA 将予以吊销。

4.7.5 CFCA 处理吊销请求的时限

在主动吊销的情形下，CFCA 收到吊销请求并审核完成后，24 小时内吊销证书。

在被动吊销的情形下，订户在收到吊销通知后的 3 个工作日内可向 CFCA 提出申辩理由，CFCA 将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在 3 个工作日内未回复或回复无异议，则 CFCA 将于 24 小时内予以吊销，并在证书过期后至少保留 1 年吊销信息。

4.7.6 依赖方检查证书吊销的要求

依赖方在信任此证书前应检查证书的有效性，确认证书未被吊销。

4.7.7 CRL 发布频率

CFCA 本CPS 所含系统发布的CRL 信息，将在 3 小时内更新 CRL 列表；订户有特殊要求的，将根据订户的需求，适当更新 CRL 发布的频率。CFCA 签发的CRL 信息，根据需要，也可以人工方式实时发布。

4.7.8 CRL 发布的最大滞后时间

CRL 发布的最大延迟时间不超过 24 小时。

4.7.9 在线证书状态查询的可用性

CFCA 提供OCSP 查询服务，服务 7*24 小时可用。

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 RFC2560 标准。

客户通过http 协议访问CFCA 的 OCSP 服务，CFCA 会对查询请求进行检查，检查的内容包括：

- ◆ 验证是否强制请求签名
- ◆ 用 CA 证书验证签名是否通过
- ◆ 验证证书是否生效或者已经过期
- ◆ 验证证书颁发者是否在信任证书列表内

OCSP 响应包含如下表所述基本域和内容

域	值或者值的限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。
版本	V1
签名算法	签发 OCSP 的算法。sha256RSA、SM3、SM2 算法签名。
颁发者	签发 OCSP 的实体。签发者公钥的数据摘要值和证书甄别名。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书废止信息。
证书标识	包括数据摘要算法、证书甄别名、数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书废止信息	当返回证书状态为废止时包含废止时间和废止原因。

OCSP 的扩展信息与RFC2560 一致。

CFCA 的 OCSP 信息的更新频率不超过 24 小时，OCSP 服务响应最大时间不超过 10 秒，OCSP 服务响应信息最大有效期不超过 7 天。

4.7.10 吊销信息的其他发布形式

证书吊销信息可以通过 CRL 或者OCSP 服务获得。订户可通过证书扩展域中的 CRL 地址获得CRL 信息。

4.7.11 对密钥遭受安全威胁的特别处理要求

当订户发现、或有充足的理由发现其密钥遭受安全威胁时，应及时提出证书吊销请求。

4.7.12 证书挂起

CFCA 目前暂不提供此业务。

4.8 证书状态服务

4.8.1操作特征

证书状态可以通过CFCA 提供的 OCSP 服务获得。

4.8.2服务可用性

CFCA 提供 7*24 小时不间断证书状态查询服务。

4.9 订购结束

以下两种情形将被视为订购结束：

1、 证书到期后即视为订购结束。

2、 证书吊销视为订购结束。

4.10 密钥生成、备份与恢复

为保证订户密钥的安全性，订户应在安全的环境下独立生成密钥对，并将产生的密钥通过加密等手段存储在安全的介质中，订户应及时备份密钥，并确保备份密钥的安全性，以防密钥丢失。在生成密钥对之后与安装服务器证书之前的时期内不应更改服务器的任何配置，以防密钥丢失。在密钥丢失或可能泄漏后，需及时申请密钥更新。

在订户委托其他可信服务商代替订户生成密钥对的情况下，应要求服务商承担相应的保密责任。

4.11 证书归档

本 CPS中除CFCA ACS OCA32 签发的证书，在证书过期5年后将对过期的证书进行归档。归档记录保存至证书失效后10年。

对于CFCA ACS OCA32 签发的证书，将在证书签发后3个月内进行归档，归档

记录保存至少5年。

5 认证机构设施、管理和操作控制

5.1 物理控制

系统的物理安全和环境安全是整个CFCA 系统安全的基础，它包括基础设施的管理、周边环境的监控、区域访问控制、设备安全及灾难预防等各方面。为保证 CFCA 系统物理环境的安全可靠，CFCA 系统被放置于安全稳固的建筑物内并具备独立的软硬件操作环境，充分考虑了水患、火灾、地震、电磁干扰与辐射、犯罪活动以及工业事故等的威胁。

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楼内）内，进入机房须经过三道审核，机房电磁屏蔽效能满足 GJBz20219－94 标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

5.1.2 物理访问

外来人员进入楼内，需经过中国银联北京信息中心、CFCA 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。

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

操作人员进入安全区机房，须经过三道门禁系统，其中两道是双人指纹加门禁卡认证，一道是双人门禁卡认证，并且所有门禁的进出信息都会在监控室的安保系统中记录。

5.1.3 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，任何一台 UPS 出

现故障，均能保证系统供电持续运行 30 分钟以上。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UPS 实施供电。

CFCA 机房采用多台中央空调和新风设备，保证机房内温度和湿度达到国家标准（GBJ19-87《采暖通风与空气调节设计规范》、GB 50174-2008、GB 50174-93《电子计算机机房设计规范》）。

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减小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，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。

5.1.6 介质存储

对于存放重要数据的存储介质，CFCA 制订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 废物处理

敏感的文件资料（包括纸介质、光盘或软盘废物等）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。

5.1.8 数据备份

根据《GB/T20988-2007 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同城灾备中心。

5.2 程序控制

5.2.1 可信角色

CFCA 的可信角色包括：

客户服务人员

安全管理人员

密钥与密码设备管理人员

加密设备操作人员

系统管理人员

人力资源管理人员

5.2.2 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。

其它操作，例如发放证书，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。

5.2.3 每个角色的识别与鉴别

CFCA 在雇佣一个可信角色之前将会按照本 CPS 第5.3.2 节的规定对其进行背景审查。

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

CFCA 使用数字认证和订户名/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：

安全管理员、系统管理员、网络管理员、操作员、订户信息收集人员、订户身份及信息审核人员、RA 录入人员、RA 审核制证人员。

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

成为CFCA 可信角色的人员必须提供相关的背景、资历证明，并具有足以胜任其工作的相关经验，且没有相关的不良记录。

5.3.2 背景审查程序

CFCA 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的真实性进行鉴定。

(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必须符合第 5.3.1 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

CFCA 对录用人员按照其岗位和角色安排培训。培训内容有：PKI 的相关知识、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、ISO9000 质量控制体系、CPS 等。

CFCA 处理证书业务相关的员工必须接受下列培训：

1)向所有负责信息身份验证的职员（“验证专家”）提供技能培训。培训内容包括基础PKI 知识、审核与验证制度和流程、对验证过程的主要威胁因素（如，网络钓鱼及其他社会工程学策略）以及证书标准；

2)保留人员培训记录，并且确保“验证专家”能够胜任身份信息验证工作的技术要求；

3)验证专家必须按其不同的技术水平等级被授予不同的签发证书权限，技术水平分级标准应与培训内容以及业绩考核标准一致；

4)确保为验证专家分配签发证书权限前，不同技术水平等级的验证专家都具有足够的胜任能力；

5)要求所有的验证专家通过关于证书标准中身份验证要求的 CA 内部考试。

5.3.4 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 CA 系统更新升级时也会对其员工进行相应的培训。

5.3.5 工作岗位轮换周期和顺序

CFCA 根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

5.3.6 未授权行为的处罚

员工一旦被发现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罚，其处理办法根据 CFCA 相关的管理规范执行。

5.3.7 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。

5.3.8 提供给员工的文档

CFCA 向其员工提供完成其工作所必须的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

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 系统记录的证书订户身份信息。

3、证书生命周期中的各项操作，包括证书申请、证书密钥更新、证书吊销等事件；

4、系统、网络安全记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理工单、系统变更工单等；

5、人员访问控制记录；

6、系统巡检记录。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

5.4.2 处理日志的周期

CFCA 对上条中 1 类日志由密钥管理员收集并管理；2、3 类日志由数据库保存，并每天进行一次增量备份，每周进行一次全备份；4 类日志每天自动保存在备份设备上；5 类日志每季度进行一次审计；6类日志每天进行一次检查。

5.4.3 审计日志的保存期限

与证书相关的审计日志至少保存到证书失效后十年。

5.4.4 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。

5.4.5 审计日志备份程序

对于系统日志、数据库日志和相关业务日志，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。

5.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

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，CFCA 不进行通告。

5.4.8 脆弱性评估

根据审计记录，CFCA 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

CFCA 归档记录的类型除了本CPS 的第 5.4.1 节内容外，还包括以下信息：

1、 证书申请资料、身份验证资料、与证书订户的协议、订户证书、CRL 等；

2、 电子认证业务规则、证书策略、管理制度等；

3、 员工资料，包括员工信息、背景调查、培训、录用离职等资料；

4、 各类外部、内部审查评估文档。

5.5.2 归档记录的保存期限

CFCA 针对归档记录将保存至证书失效后 10 年。

如果法律需要，CFCA 将延长记录保存期限。CRL 或OCSP 中的证书吊销记录在此证书的有效期内不会被删除。

5.5.3 归档文件的保护

CFCA 对归档文件有相应的保存制度。

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、删除或其它操作。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，并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、操作系统的备份、CRL 文件的备份、及日志的备份。

数据库备份：采用本地备份和异地备份、增量备份与全部备份相结合的方式进行备份。

操作系统的备份：系统初次上线后进行一次备份，在系统有调整时进行备份。

5.5.5 记录的时间戳要求

归档的记录都需要标注时间；系统产生的记录按照要求添加时间标识。

5.5.6 归档收集系统

CFCA 有自动的电子归档信息的存放系统。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员才能获得归档信息。当归档信息被恢复后会对其进行完整性检验。

5.6 电子认证服务机构密钥更替

当 CA 密钥对的累计寿命超过第 6.3.2 中规定的最大有效期时，CFCA 将启

动密钥更新流程，替换已经过期的 CA 密钥对。CFCA 密钥变更按如下方式进行：

一个上级CA 应不迟于其私钥到期之前 60 天停止签发新的下级 CA 证书（“停止签发日期”）；

产生新的密钥对，签发新的上级 CA 证书；

在“停止签发证书的日期”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；

上级 CA 将继续利用原来的 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持续计划等相关规章制度采取合理措施。

业务持续计划由“CFCA 运营安全管理委员会”（以下简称安委会）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。安委会的成员包括公司领导与各部门负责人，负责人为总经理。

业务中断事件分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。

当发生紧急事件后，安委会负责人召集安委会成员举行会议，对事件进行评估。运行部按照确定的处理机制进行处理，市场部、技术支持部根据实际情

况，针对受影响客户进行妥善处理。在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 5.7.4 的规定进行。

对于一般故障，CFCA 将在 2 小时内解决；对于紧急事件，CFCA 在 24 小时内解决；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数据备份中心恢复电子认证服务。

对于 CFCA 签发的证书，CFCA 还具有专门的问题报告和响应能力：

1)CFCA 向订户、依赖方、软件开发商和其他的第三方提供了清晰指引，说明如何向CFCA 报告证书的投诉、私钥泄漏、证书使用不当、或其他形式的欺诈、泄漏、使用不当或行为不当。CFCA 设置了 7*24 服务热线（400-880-9888），有能力提供 7*24 小时接受和认可此类报告的服务。

2)CFCA 将在问题报告的 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吊销或其它相应手段：

问题的性质；

收到的对特定证书或网站问题报告数量；

投诉人的身份；

相关的法规。

3) CFCA 可确保全天候（7*24 小时）对高优先级的问题报告首先在 CA 内部进行响应。然后，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吊销。

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 5.7.1 中的规定区分是紧急事件还是灾难事件，按照不同的事件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

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

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

CFCA 一旦证实根私钥泄露时，会立即通知订户及依赖方，对所有证书进行吊销，并不再签发新的证书。

5.7.4 灾难后的业务连续性能力

CFCA 建有数据备份中心，有相应的业务持续计划，可确保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数据备份中心恢复电子认证服务。

5.8 电子认证服务机构或注册机构的终止

CFCA 拟终止电子认证服务时，将在终止服务六十日前向行业主管部门报告，并办理电子认证服务资质的注销手续。

CFCA 拟暂停或者终止电子认证服务时，将在暂停或者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订户、依赖方等有关各方，并依据对订户和依赖方的数字证书服务协议向订户和依赖方进行赔偿；向电子认证业务承接方提供认证相关信息，包括但不限于：证书办理资料、证书信息库、最新的证书状态资料等。

CFCA 将在暂停或者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。

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。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

1、CA签名密钥的生成

CA 的签名密钥在加密机内部产生，加密机具有国家密码主管部门的相应资质。加密机采用密钥分割或秘密共享机制进行备份。在生成 CA 密钥对时，CFCA 按照加密机密钥管理办法，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，密钥管理员凭借口令和智能 IC 卡对密钥进行控制。在第三方审计人员的监督下，由 5 名中的 3 名具有密钥管理及操作权限的人员同时到达 CFCA 最安全区同时进行操作，产生 CA 密钥。CA 密钥的生成、保存和密码模块符合国家密码主管部门的要求，并具有国家密码主管部门的相应资质。

2、RA密钥的生成

RA 的签名私钥在安全控制下产生，RA 证书由CFCA 签发。

3、订户密钥的生成

订户的签名密钥的生成由订户负责，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。订户的加密密钥由 CFCA 的密钥管理系统生成，并通过安全的方式传输给订户。CFCA 的密钥管理系统是由国家密码管理批准运营的专业密钥管理系统，负责为电子认证服务订户产生、备份、恢复加密秘钥等服务。

除订户以外的其他机构不应存档订户私钥。

预植证书的密钥生成方式参见《CFCA 预植证书证书策略》。

场景证书的密钥生成由负责场景业务的业务提供方生产，并负责保护场景证书私钥的安全。

如果 CFCA 或其注册机构 RA 获知订户私钥交予了未授权人员或不与订户关联的组织，CFCA 将按照相关标准要求撤销该私钥所对应的公钥证书。

CFCA 有义务指导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，并可在订户需要时提供相应的技术支持人员帮助订户生成正确的密钥。

6.1.2 私钥传送给订户

订户的私钥由订户自己生成时将不会进行传送。由 CFCA 生成时将离线或者在线安全方式传递。订户委托 CFCA 或者其他人产生私钥时，CFCA 或者受托方需确保私钥在交给客户前未被使用，并不能保留签名私钥的备份。

6.1.3 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， 或者通过电子邮件的形式发送给 CFCA。

6.1.4 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。

6.1.5 密钥的长度

CFCA 遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前 CFCA 电子认证系统支持签发 SM2-256、RSA-1024、RSA-2048 密钥的证书，将根据用户的需求为订户提供相应密钥类型的证书。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成，CFCA 在采购这些设备时要求其必须具有国家密码主管部门的相应资质，并遵从国家密码主管部门发布的《证书认证系统密码及相关安全技术规范》以及其他相关规范和标准要求，如对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求等。

6.1.7 密钥使用目的

根 CA 私钥用于签发自身证书、下级CA 证书、和CA 的吊销列表，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。各类证书密钥的使用策略如下：

证书类型	证书最长期限（年）	密钥用法	增强密钥用法
CA 证书	30	数字签名、CRL 签名	无
个人普通证书	5	数字签名，不可否认	客户端认证、安全 Email 验证
个人高级证书	5	签名证书：数字签名，不可否认 加密证书：密钥加密，数据加密、密钥协商	客户端认证、安全 Email 验证
企业普通证书	5	数字签名，不可否认	客户端认证、安全 Email 验证
企业高级证书	5	签名证书：数字签名，不可否认 加密证书：密钥加密，数据加密、密钥协商	客户端认证、安全 Email 验证
SSL 服务器证书	5	数字签名、密钥协商、密钥加密	服务器身份验证，客户端身份
VPN 证书	5	签名证书：数字签名，不可否认 加密证书：密钥加密，数据加密、密钥协商	服务器身份验证，客户端身份验证
代码签名证书	5	数字签名、密钥协商、密钥加密	代码签名
邮件证书	5	数字签名、密钥协商、密钥加密	安全Email 验证

证书类型	证书最长期限（年）	密钥用法	增强密钥用法
设备证书	5	签名证书：数字签名，不可否认 加密证书：密钥加密，数据加密、密钥协商	服务器认证,客户端认证
场景证书	1 天	数字签名、不可否认	无
云证通证书	2	数字签名、不可否认	客户端认证、安全 Email 验证

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，使用通过国家密码主管部门鉴定并批准使用的具有完全自主知识产权的高速主机设备，支持 RSA、DSA、SM2、Diffe Hellman 等公钥算法，RSA 模长可选 2048、4096 比特；支持 SDBI、TRIPLE-DES、IDEA、SM1、SM4 等对称算法，支持 128 比特高强度加密；支持SHA1、SDHI、SHA256、SM3 等HASH 算法。

CFCA 使用的加密机其公钥算法为 RSA-1024、RSA-2048、SM2-256，HASH 算法为SHA1、SHA-256、SM3，具有国家密码主管部门颁发的产品资质证书。

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。加密机仅仅与对应系统直连，并存放在屏蔽机房内。

6.2.2 私钥多人控制

CFCA CA 密钥存放在加密机中，加密机的管理密钥被分割保存在 5 张 IC 卡中，IC 可分别由 5 位经过授权的安全管理员掌握，并保存在屏蔽机房中的最安全区内的保险箱中。当激活 CA 私钥时，必须由 5 个管理员中的 3 个管理员同时在

场才能完成，从技术及制度上保证了敏感的加密操作的安全性。

6.2.3 私钥托管

对于 CA 私钥,CFCA 无托管业务。

6.2.4 私钥备份

CA 的私钥由加密机产生，加密机有双机备份，并保存在防高温、防潮湿及防磁场影响的环境中，对加密机的备份操作须 3 人以上(包括 3 人)才可完成。订户的私钥由订户产生，建议订户自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄漏。

6.2.5 私钥归档

当 CFCA 的 CA 密钥对到期后，这些密钥对将被归档保存至少 10 年。归档的 CA 密钥对保存在本CPS6.2.1 所述的硬件密码模块中，并且 CFCA 的密钥管理策略和流程都确保了归档后的 CA 密钥对不会再被用于生产系统中。当归档 CA 密钥对达到归档保存期限之后，CFCA 将按照本 CPS6.2.10 所述的方法进行安全地销毁。

CFCA 基于 PKI 理论为订户产生的加密私钥的归档参照 CA 的密钥归档方法进行归档。

6.2.6 私钥导入、导出密码模块

CFCA 通过硬件模块生成 CA 密钥对，部署了备份加密设备，CA 密钥对在备份传递时以离线加密方式进行。

通过硬件产生的订户私钥不能导出密码模块。其他方法产生的订户私钥在导出时应采取加密的方式进行。

6.2.7 私钥在密码模块的存储

私钥以密文的方式分段加密存放在硬件加密模块中。

6.2.8 激活私钥的方法

1、激活订户私钥

订户若使用软件产生、保存私钥,则私钥是保存在服务程序的软件密码模块中，这时订户使用口令保护私钥。当服务程序启动，软件加密模块被加载，密码模块验证口令完成后，私钥被激活。

当订户使用硬件密码模块产生、保存私钥时，订户使用硬件密码模块口令（或 pin 码）保护私钥，硬件加密模块被加载，密码模块验证口令完成后，私钥被激活。

2、激活CA 私钥

CFCA 采用硬件设备（加密机）产生、保存 CA 私钥，其激活数据按照本CPS6.2.2 要求进行分割。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

对于订户私钥，当服务程序被停止、系统注销或系统断电后私钥进入非激活状态。

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。

6.2.10 销毁私钥的方法

当 CA 的生命周期结束后，CFCA 将根据本 CPS 6.2.5 之相关规定将CA 私钥进行归档，其它的 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地销毁。

订户私钥的销毁须经授权后安全地销毁。密钥生命周期最后，销毁所有订户密钥的副本和碎片。

6.2.11 密码模块的评估

CFCA 使用国家密码主管部门鉴定并批准使用的具有自主知识产权的高速主机加密设备，接受其颁布的各类标准、规范、评估结果等各类要求。

6.3 密钥对管理的其它方面

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CPS5.5 的相关规定。

6.3.2 证书操作期和密钥对使用期限

CA 证书的有效期不超过 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。特殊情况下，对于签名类证书，为了验证在证书有效期内签名的信息，与之对应的公钥可以在证书的有效期限以外使用， 直到私钥受到损害或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

1、 CFCA 的 CA 私钥产生遵循本 CPS6.2.2 中的要求。

2、 对于订户，激活数据是保护私钥的密码。CFCA 推荐订户使用强口令来保证私钥的安全性，该口令需要：

- 长度至少为 8 位
- 建议订户不要使用生日、简单重复的数字等容易被人猜中或破解的信息做为口令

6.4.2 激活数据的保护

1、 CFCA 的密钥管理者须保护他们所维护的密钥，并且须签署协议来承诺所

承担的责任。

2、 订户必须以加密的形式保存私钥，建议使用双因素认证（如硬件设备加强口令）来保护其私钥。

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 IC 卡，通常被保存在 CFCA 最安全区机房， 不能携带离开CFCA。如在某种特殊情况下需要进行传输时（如建设灾备系统时），其传送过程需要在CFCA 安全管理人员和密钥管理人员共同监督的情况下进行。

对于证书订户，通过网络传输用于激活私钥的口令时，需要采取加密等保护措施，以防丢失。

6.4.3.2 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。订户私钥的激活数据在不需要时由订户自行销毁，订户应确保他人无法通过残余信息、存储介质直接或间接地恢复激活数据。

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、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、维护信息库和吊销证书的密钥、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。

6.5.2 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、技术或其他因素是否足够。

6.5.3 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；安全控制措施程度必须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

根据系统安全管理的相关规定，CFCA 要求 CA 与 RA 系统采用可信安全操作系统对外提供服务。企业客户也必须使用可信任操作系统。

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、多层防火墙设置、人员职责分割、内部操作控制、业务持续计划等各方面。

6.6.2 计算机安全评估

CFCA 信任证书认证系统已通过国家密码管理局等有关部门的安全性审查。

6.7 生命周期技术控制

6.7.1 根密钥控制

对于证书根密钥生成需要有证书审核从业者的现场参加，从业者通过现场查看 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 CPS 和CP 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，作为今后的审核依据。

其他 CA 的密钥控制参照上述要求进行。

6.7.2 系统开发控制

CFCA 的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求。

6.7.3 安全管理控制

CFCA 认证服务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，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。同时，按照ISO9000 质量管理体系标准建立了严格的管理制度。对于核心数据，采用远程数据复制技术，并利用专线实时复制到同城灾备中心。

6.7.4 生命期的安全控制

CFCA 的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求，其产品源代码在国家密码主管部门处留有备份，以保证系统的延续性。

6.8 网络的安全控制

CFCA 认证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、由路由器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权限控制进行数据保护；

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。

6.9 时间信息

证书、CRL、OCSP、电子认证服务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、证书吊销列表和在线证书状态协议

7.1 证书

CFCA 签发的证书格式符合 GM/T 0015-2012 数字证书格式规范，包含如下证书域。

7.1.1 版本号

CFCA 签发的证书格式符合 X.509 V3 标准，这一版本信息包含在证书版本属性内。

7.1.2 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 签发的证书将包含私有扩展项，私有扩展项将被设置为非关键性扩展。对于 CA 证书的证书扩展项，除 4 个扩展项：基本限制(BasicConstraints)，密钥用法(KeyUsage)， 证书策略（CertificatePolicies）， 扩展密钥用法

（ExtendedKeyUsage），其他扩展项遵循 RFC 5280 标准。

7.1.2.1 颁发机构密钥标识符

CFCA 订户证书及 CA 证书中包含颁发机构密钥标识符扩展项，此扩展项用于识别与证书签名私钥相对应的公钥，可辨别同一 CA 使用的不同密钥。该扩展项为非关键项。

7.1.2.2 主题密钥标识符

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

7.1.2.3 密钥用法

密钥用法指明已认证的公开密钥用于何种用途。

对于 CA 证书的密钥用法，该项为关键扩展。密钥用法包含证书签名、CRL 签发，其他密钥用法不能出现。对于订户证书，该项为非关键扩展，SM2 类证书为关键扩展，其密钥用法参见 6.1.7。

7.1.2.4 基本限制

基本限制项用来标识证书的主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长，该项定义遵照 RFC5280 之规定。SM2 类订户证书该项为关键扩展。

7.1.2.5 增强型密钥用法

本项指明已验证的公钥可用于一种或多种用途，可作为对密钥用法扩展项中指明的基本用途的补充或替代。该扩展项为非关键项。增强密钥用法参见 6.1.7。

7.1.2.6 CRL 分布点

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。该扩展项为非关键项。

7.1.2.7 主题备用名称

主题备用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RFC5280 的规定。

SSL 服务器证书必须包括该扩展域，且只能存在域名或者外网 IP 地址。代码签名证书主体备用名必须存在，必须使用“permanentldentifier”，必须不能存在域名和 IP 地址。在主题备用名中永久识别名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。

7.1.3 算法对象标识符

CFCA 签发的证书符合 RFC5280 标准，采用 RSA-2048/SHA1 算法签名或者 RSA-2048/SHA256、SM2/SM3 密码算法签名。

SM2 算法其 OID 为：1.2.840.10045.2.1 附加参数为 1.2.156.10197.1.301

7.1.4 主题名称

本项用于描述与主题公钥项中的公钥对应的实体的情况。CFCA 签发证书的甄别名符合X.500 关于甄别名的规定，CFCA 保证签发的证书每个主题实体的甄别名称是唯一的。为了确保甄别名称的唯一性，CFCA 制定了《CFCA 数字证书 DN 规则》、《预植证书 DN 规则》。

DN 可以包含以下 7 部分：

1、 CN 部分：如果是个人证书，则该部分只能是系统标识、订户名称、RA 自定义内容和数字，其中系统标识填写注册机构的英文简称，同时可以根据需要填写表示其他有意义的内容，订户名称填写个人姓名，RA 自定义内容填写客户号等，数字部分是如果前三段都相同时， 填写区分不同证书的顺序号；如果是企业证书，则该部门仍然按照系统标识、订户名称、RA 自定义内容和数字填写，其中系统标识填写系统标识填写注册机构的英文简

称，同时可以根据需要填写表示其他有意义的内容，订户名称填写企业名称，RA 自定义内容填写如客户号+企业中使用该张证书的具体人员姓名或部门等，建议使用可体现唯一标识的内容。

2、 OU【2】部分：如果是个人普通证书和企业普通证书，则该部分是证书类型，其他证书该部分为可选部分，用于表示证书类型，如下表信息：

证书类型	OU
个人普通证书	Individual-1
企业普通证书	Organizational-1

如 OU 表示实体的部门名称，则CFCA 必须对该部分进行验证。

3、 OU【1】部分：该部分为可选部分，可以表示实体的部门名称或者用于表示CFCA 本地 RA 的名称。

如 CFCA 本地RA： OU=Local RA。

如 OU 表示实体的部门名称，则CFCA 必须对该部分进行验证。

4、 O 部分：该部分为必选部分，表示实体的真实名称或者签发 CA 的 CA 系统名称。使用英文时应与实体有效证件上的真实名称意义一致， 并且不能产生歧义。

5、 L 部分：个人证书、企业证书、预植证书、场景证书没有该部分，其他类型的证书该部分为必选部分。用于表示营业地址所在地。

6、 S 部分：个人证书、企业证书、预植证书、场景证书没有该部分，其他类型的证书该部分为必选部分。用于表示营业地址所在省。

7、 C 部分：该部分为必选部分，用于表示证书申请者所在国家或地区的英文简称，全部大写，如中国订户标识为：C=CN

DN 中包含的国家、省市级名称必须使用权威部门颁发的标准名称（例如：

ISO country code)。

7.1.5 名称限制

CFCA CS CA 下签发的证书，其实体名称不允许为无意义的匿名或者伪名，必须是有明确含义的识别名称，使用英文名称时应能正确表达实体名称。

7.1.6 证书策略及对象标识符

CA 证书的证书策略扩展项中，certificatePolicies:policyIdentifier 设置为anyPolicy。

7.1.7 策略限制扩展项的用法

未使用本扩展域。

7.1.8 策略限定符的语法和语义

未使用本扩展域。

7.1.9 关键证书策略扩展项的处理规则

未使用本扩展域。

7.2 CRL

7.2.1 版本号

CFCA 目前使用的是X.509 V2 版本的CRL。

7.2.2 CRL 和CRL 条目扩展项

CRL 数据定义如下：

1、版本（Version）

显示CRL 的版本号。

2、CRL 的签发者（Issuer）

指明签发CRL 的CA 的甄别名。

3、CRL 发布时间（thisUpdate）

4、预计下一个CRL 更新时间(next update)

5、签名算法

6、列出吊销的证书，包括吊销证书的序列号和吊销日期。

7.3 在线证书状态协议

CFCA CS CA 系统提供在线证书状态查询服务。其他系统根据业务需要提供该项服务。

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 认证机构审计和其它评估

8.1 评估的频率或情形

CFCA 在如下情形中进行评估：

1、 根据《中华人民共和国电子签名法》、《电子认证服务管理办法》《电子认证服务密码管理办法》规定，接受主管部门的评估和检查。

2、 CFCA 电子认证系统每年进行信息系统三级等级保护测评。

3、 CFCA 根据业务发展情况，对注册机构进行评估。

评估的频率为：

1、年度评估：接受主管部门对 CFCA 进行的年度检查；聘请外部测评机构进行等级保护测评。

2、运营前评估：在新系统向公众提供服务之前由行业主管部门对新系统进行评估，评估合格后方可正式运营；

8.2 评估者的资质

若需邀请外部审计机构对 CFCA 进行评估，CFCA 将选择熟悉 IT 运营管理、

具有多年审计经验的审计机构对 CFCA 的运营管理进行一致性审计。在进行审计前，审计机构必须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

评估者与CFCA 应无任何业务、财务往来或其它足以影响评估客观性的利害关系。

8.4 评估内容

评估的内容包括但不限于以下方面：

1、CA 物理环境和控制

2、密钥管理操作

3、基础 CA 控制

4、证书生命周期管理

5、CA 业务规则

8.5 对问题与不足采取的措施

CFCA 管理层将对评估报告进行评估，对在审计中发现的重大意外或不作为采取行动。从完成审计到采取行动纠正问题的时间不超过 20 天。

8.6 评估结果的传达与发布

当 CFCA 接受行业主管部门的检查或评估后，行业主管部门会向公众发布对 CFCA 的检查或评估结果。

当 CFCA 进行内部审计后，审计结果将只在公司内部进行传达。

8.7 其他评估

CFCA 将进行持续的自我审核，至少每季度进行一次自我审核，以对自身的服务质量进行控制。自我审核通过对上次审核期间末至本次审核期间初这段期间内的电子认证活动是否符合相关约定。CFCA 对自身的电子认证活动进行抽样审查，样本量不得少于此期间内签发证书总数的百分之三。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

根据市场和管理部门的规定，CFCA 将收取合理的费用，并在订户向 CFCA 订购证书时，提前告知证书的签发与更新费用。

9.1.2 证书查询费用

CFCA 暂不收取此项收费，但保留对此项服务收费的权利。

9.1.3 证书吊销或状态信息的查询费用

CFCA 暂不收取此项收费，但保留对此项服务收费的权利。

9.1.4 其它服务费用

CFCA 保留收取其他服务费的权利。

9.1.5 退款策略

除非 CFCA 违背了本 CPS 所规定的责任与义务，订户可以要求退款。否则，CFCA 对订户收取的费用均不退还。

订户应当提供符合 CFCA 要求的完整、真实、准确的证书申请信息，否则 CFCA 对此造成的损失和后果不承担任何责任。

9.2 财务责任

9.2.1 保险范围

CFCA 根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。

9.2.2 其它资产

CFCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

此要求对证书订户同样适用。

9.2.3 对最终实体的保险或担保范围

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。

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 与订户之间的协议、资料中未公开的内容等属于保密信息。除非法律明文规定或政府、执法机关等的要求，CFCA 承诺不对外公布或透露订户证书信息以外的任何其它隐私信息。

2、 订户私钥属于机密信息，订户应当根据本 CPS 的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

9.3.2 不属于保密的信息

不属于保密的信息包括：

1、CA 系统签发的证书信息和CRL 中的信息。

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，非由于接受方的

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 保护机密信息的责任

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

9.4 个人信息私密性

9.4.1 隐私保密方案

CFCA 尊重所有订户和他们的隐私，个人隐私信息保密方案遵守现行法律和政策规定。任何订户选择使用 CFCA 的证书服务，就表明已经同意接受 CFCA 的隐私保护制度。

9.4.2 作为隐私处理的信息

CFCA 在管理和使用订户提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该订户的基本信息将被视为隐私处理，这些信息将只能由 CFCA 使用，非经订户同意或有关法律法规、公共权力部门根据合法的程序要求，CFCA 不会任意公开。

9.4.3 不被视作隐私的信息

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

9.4.4 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 可以向特定的对象公布隐私信息，CFCA 无需承担由此造成的任何责任。

9.4.5 使用隐私信息的告知与同意

1、 订户同意，CFCA 在业务范围内并按照本 CPS 规定的隐私保护政策使用所获得的任何订户信息，无论是否涉及到隐私，CFCA 均可以不用告知订户。

2、 订户同意，在任何法律法规或公共权力部门要求下，CFCA 向特定对象披露隐私信息时，CFCA 均可以不用告知订户。

9.4.6 依法律或行政程序的信息披露

除非符合下列条件，CFCA 不会将订户的保密信息提供给其他个人或第三方机构：

1、 司法、行政部门或其他法律法规授权的部门依据政府法律法规、规章、决定、命令等的规定通过合法授权提出的申请。

2、 订户采用书面形式的信息披露授权。

3、 本 CPS 规定的其他可以披露的情形。

9.4.7 其它信息披露情形

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，承担相应的保护隐私责任。在法律法规或公共权力部门通过合法程序或订户书面申请授权要求下，CFCA 可以向特定的对象公布隐私信息，CFCA 无需承担由此造成的任何责任。

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属于 CFCA。

9.6 陈述与担保

9.6.1 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》等法律规定，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 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 有责任审计其注册机构电子认证业务是否符合本CPS 约定。CFCA 对注册机构的审计至少一年一次。CFCA 具有保存和使用证书持有人信息的权限和责任。

9.6.2 注册机构的陈述与担保

作为CFCA 的注册机构，应遵照 CFCA 的CPS&CP 承担电子认证业务中注册机构的职责，其电子认证业务操作受行业及 CFCA 的相关管理规定。

1. 注册机构根据 CFCA 制订的策略和运行管理规范，对订户的证书申请材料进行审核，并注册证书订户的信息。通过安全通道将证书订户的信息传送给CFCA。
2. 如注册机构对订户的证书申请材料审查没有通过，注册机构有向订户进行告知的义务。
3. 注册机构发放预植证书时，应在对订户的身份进行验证后，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，该预植证书才能激活使用。并告知订户应修改智能密码钥匙的初始口令，不在公共场所使用智能密码钥匙。
4. 注册机构应制订合理的业务流程，确保将预植证书发放给订户之前，对预植证书进行妥善保管，并确保在未与订户身份信息进行绑定之前不会被使用。
5. 注册机构应在合理的时间内完成证书申请处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间为 1-3 个工作日。
6. 注册机构须对订户的信息及与认证相关的信息妥善保存，并于适当的时

间转交给CFCA 归档。注册机构应根据相关协议内容配合 CFCA 需要的电子认证业务合规性审计。

7. 注册机构应使订户明确地知道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，尽到对订户安全提示的义务。
8. 注册机构有义务通知订户阅读CFCA 发布的CP、CPS 以及其它相关规定，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。

9.6.3 订户的陈述与担保

订户声明和承诺：

订户确认已经阅读和理解了 CPS 及有关规定的全部内容，并同意受此 CPS 文件规定的约束。

1. 订户应遵循诚实、信用原则，在申请数字证书时，应当提供真实、完整和准确的信息和资料，并在这些信息、资料发生改变时及时通知 CFCA 的注册机构。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 注册机构，造成的损失由订户自己承担。
2. 订户使用CFCA 数字证书时应使用经合法途径获得的相关软件。
3. 订户应通过可靠方式产生密钥对，防止密钥遭受攻击丢失、泄漏和误用；订户应当妥善保管 CFCA 签发的数字证书的私钥和密码，不得泄漏或交付他人。如因故意或过失导致他人知道、盗用、冒用数字证书私钥和密码时，订户应承担由此产生的责任。
4. 订户应采取必要手段来保障申请证书时的密钥对中的私钥的安全存储、使用控制、与保密性（包括用于存储私钥的装置或设备），如订户使用的数字证书私钥和密码泄漏、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注册机构申请废

止该数字证书，相关手续遵循本CPS 的规定。

5. 订户应将证书用于合法目的并符合本CPS。
6. 订户应对使用证书的行为承担责任：
   ① 使用证书的行为应符合全部适用的法律法规。
   ② 使用证书的行为应符合订户真实意愿或者仅为了处理已获得授权的事务。
   ③ 使用证书的行为符合用户协议约定的使用范围和条件。
7. 订户在取得证书后应确认证书信息无误。
8. 订户申请代码签名证书后，一旦发现如下情况，应当立即向 CA 申请吊销：
   ① 有证据表明，此代码签名证书被用于签署可疑代码，包括但不限于病毒，木马，或者其他不恰当的程序。
   ② 证书中内容不再正确或不再准确。
   ③ 此证书私钥信息已被泄露，或者其他相关部分已被错误使用。
9. 订户保证一旦在证书被吊销后，将不能再使用该证书。
10. 订户明确了解如果 CFCA 发现了订户证书的不当使用，或者订户证书被用于违法甚至犯罪行为，CFCA 有权直接吊销订户证书。
11. 订户损害CFCA 利益的，须向 CFCA 赔偿全部损失。这些情况包括但不限于：

① 订户在申请数字证书时没有提供真实、完整、准确的信息，或者在信息变更时未及时通知 CFCA；

② 订户知道或者应当知道自己的私钥和密码已经失密或者可能已经失密，但未及时告知有关各方且未终止使用；

③ 订户有其他过错或未履行双方约定。

12. 订户有按期缴纳数字证书服务费的义务，费用标准请咨询 CFCA 商务人员。

13. 随着技术的进步，CFCA 有权要求订户更换数字证书。订户在收到数字证书更换通知后，应在规定的期限内向 CFCA 提出更换。因订户逾期没有更换数字证书而引起的后果，由订户自行承担。

9.6.4 依赖方的陈述与担保

依赖方声明和承诺：

1、 获取并安装该证书对应的证书链；

2、 在信赖证书所证明的信任关系前确认该证书为有效证书，包括：检查 CFCA 公布的最新CRL，确认该证书未被吊销；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；

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。

9.6.5 其它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。

9.7 担保免责

1、证书申请人或订户故意或过失提供或未按照要求提供不准确或不真实或不完整的信息而获得 CFCA 签发的证书，订户因在使用该证书时而产生的任何纠纷，由证书申请人或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，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（“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、对于明显由于 CFCA 的合作方的越权行为或其他过错行为所引发的违反约定义务而对订户造成的损失，CFCA 不承担赔偿或补偿责任。

9.8 有限责任

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。

9.9 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。但无论如何，如果CFCA能够证明其提供的服务是按照《电子签名法》、《电子认证服务管理办法》、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或补偿责任。

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：

（1）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、以及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；

（2）由上述第（1）项所述的损失相应生成或附带引起的损失或损害；

（3）非CFCA的行为而导致的损失；

（4）因不可抗力而导致的损失，如罢工、战争、灾害、恶意代码病毒等。

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。

9.10 有效期限与终止

9.10.1 有效期限

本CPS自CFCA在其官方网站（http://www.cfca.com.cn）公布之日起生效，除非CFCA 特别声明CPS 提前终止。

9.10.2 终止

CFCA 有权终止本CPS（包括其修订版本），本CPS（包括其修订版本）自 CFCA 在其官方网站公布终止声明的 30 日后终止。

自新版本的CPS 在CFCA 官方网站公布之日起，上一版本的 CPS 效力将自动终止。

9.10.3 终止后的存续条款

CPS 中涉及的审计、保密信息、隐私保护、知识产权等方面，以及涉及赔偿的有限责任条款，在本 CPS 终止后继续有效。

9.11 对参与者的个别通告与沟通

参与者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：010-50955020。

9.12 修订

CFCA 有权修订本 CPS，并将修订版本在官方网站上公布。修订版本自公布之日起生效。

9.12.1 修订程序

修订程序与本 CPS1.5.4“CPS 批准程序”相同。

9.12.2 通知机制和期限

CFCA 有权修订本CPS 中的任何术语、条款，事前无需通知任何一方，但在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吊销，将被视为同意该修改。

9.12.3 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。

9.13 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的泄漏和/或篡改时，应在有效期内向 CFCA 提出争议处理请求并通知有关各方，有效期为 3 个月。

争议处理流程为：

1、 争议解决的通知：

当争议发生时，在采取任何行动措施之前，订户应首先通知 CFCA。

2、 争议解决的方式：

如果争议在最初通知之日起 10 天内未被解决，CFCA 将召集由 3 名安全认证专家组成外部专家小组。外部专家小组以协助解决争议为目的，收集相关事实。

专家小组应在成立之日起 10 天内（除非当事人同意将此段时限延长至特定时段）完成建议并向当事人传达。专家小组的建议对当事人无约束力，但当事人一方若书面签署文件表示同意该建议，则争议的双方即按照建议的内容解决争议。如果订户在书面签署文件同意专家小组建议后后悔，并将争议提交仲裁， 则该建议将视为CFCA 与订户之间就争议解决达成的协议且受法律保护。

3、 正式争议解决：

若专家小组未能在约定时限内提出有效建议，或者所提的建议不能使双方当事人就争议的解决达成一致意见，争议双方仅可以将争议提交北京仲裁委员会仲裁。

4、 索赔时限

任何订户或依赖方欲向 CFCA 提出索赔，应在知道或应当知道损失发生时起的两年内提出。超出两年的，该索赔无效。

9.14 管辖法律

CFCA CPS 和协议中条款的制定遵守《中华人民共和国合同法》和《中华人民共和国电子签名法》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。

9.15 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国家信息安全主管部门要求。若本 CPS 的某一条款被主管部门宣布为非法、不可执行或无效时，CFCA 将对该不符合性条款进行修改，直至该条款合法和可执行为止。本 CPS 某一个条款的不可执行性不会影响其它条款的法律效力。

9.16 一般条款

9.16.1 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、订户协议及依赖方协议及其补充协议构成各参与者之间的完整协议。

9.16.2 转让

CA、RA、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。

9.16.3 分割性

本 CPS 的某一条款被主管部门宣布为非法、不可执行或无效时，CFCA 将对该不符合性条款进行修改，直至该条款合法和可执行为止，但此条款的不可执行性不会影响其它条款的有效性。

9.16.4 强制执行

无。

9.16.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的的客观情况。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、互联网或其它基础设施无法使用等。但各方都有义务建立灾难恢复和业务连续性机制。

附录A 定义和缩写

缩写表

项目	缩写定义
ANSI	美国国家标准协会（The American National Standards Institute）
CA	电子认证服务机构（Certificate Authority）
RA	注册机构(Registration Authority)
CRL	证书吊销列表(Certificate Revocation List)
OCSP	在线证书状态协议(Online Certificate Status Protocol)
CP	证书策略(Certificate Policy）
CPS	电子认证业务规则（Certificate practice Statement）
CSR	证书签名请求（Certificate Signature Request）
IETF	互联网工程任务组(The Internet Engineering Task Force)

定义表

项目	概念定义
电子认证服务机构	受订户信任的，负责创建和签发、管理公钥证书的权威机构，有时也可为订户创建密钥。
注册机构	面向证书订户，负责订户证书的申请、审批和证书管理工作。
数字证书	经CA数字签名包含数字证书使用者身份公开信息和公开密钥的电子文件。

证书吊销列表	一个严格要求进行周期性发布的列表，被CA签名，用于标记一系列不再被证书发布者所信任的证书列表。
在线证书状态协议	IETF颁布的用于检查数字证书状态的协议。
证书策略	一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。例如，一个特定的CP可以指明某类证书适用于鉴别从事企业到企业（B-to-B）交易活动的参与方，针对给定价格范围内的产品和服务。
电子认证业务规则	关于电子认证服务机构在签发、管理、吊销或更新证书（或更新证书中的密钥）过程中所采纳的业务实践的声明。
订户	申请证书的实体。
依赖方	依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构。
私钥	经由数学运算产生的密钥（由持有者保管），用于制作数字签名，亦可依据运算方式，就相对应的公开密钥加密的文件或信息（以确保资料的机密性）予以解密。
公钥	经由数学运算产生的密钥，可公开取得、并可用于验证由其对应的私钥所产生的数字签名。公开密钥亦可依据其运算方式，将信息或档案加密，再以对应的私钥进行解密。
唯一甄别名	在数字证书的主体名称域中，用于唯一标识证书主体的X.500名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。