中国金融认证中心（CFCA）
电子认证业务规则(CPS)

V2.1

2008 年 03 月 20 日

目　　录

1 概括性描述

1.1 概述

中金金融认证中心有限公司，即中国金融认证中心（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的 CA 之一。

电子认证业务规则（CPS，Certification Practice Statement）是关于认证机构（CA,Certification Authority）在全部数字证书（以下简称证书）服务生命周期中的业务实践（如签发、吊销、更新）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)、十届全国人大常委会表决通过的并于 2005 年 4 月 1 日正式实施的《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》、中华人民共和国行业主管部门编写并审议通过的《电子认证服务管理办法》、《电子认证业务规则规范》(试行)及 CA 的一般运作规范。

CFCA 的证书认证系统分为 Operation CA(OCA)与 Operation CA2(OCA2)两套系统。本文档中，标注了“ * ”号的条款对两套系统的不同之处进行了区分，

其余条款对两套系统均适用。

1.2 文档名称与标识

此文档的名称为《CFCA 电子认证业务规则》，但目前没有注册对象标识符。

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

CA 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。

CFCA 的证书认证系统设在 CFCA 本部，不直接面对订户。它是一个树状结构，由根 CA、政策 CA、运营 CA 三部分组成。根 CA 是政策 CA、运营 CA 的根结点，它负责向国内外顶级电子认证领域扩展信用范围，政策 CA 负责向不同行业、领域拓展信用范围，而运营 CA 则负责根据本 CPS 的要求，向最终订户发放证书。

CFCA 的运营 CA 包括 OCA 与 OCA2 两套系统，OCA2 系统中不再存在政策 CA。

按照证书的功能及申请证书的订户不同，CFCA 提供以下证书类型：

个人普通证书——面向个人订户，在网上信息传递过程中提供身份验证、信息加密和数字签名等功能。个人普通证书只使用一套密钥对，即签名/验签密钥对。

企业普通证书——面向机构订户，在网上信息传递过程中提供身份验证、

信息加密和数字签名等功能。企业普通证书只使用一套密钥对，即签名/验签密钥对。

个人高级证书——面向个人订户，用于实现个人在网上信息传递过程中安全级别较高的身份验证、信息加密和数字签名等功能。个人高级证书使用两套密钥对，一对为加/解密密钥对，另一对为签名/验签密钥对。

企业高级证书——面向机构订户，用于实现机构在网上信息传递过程中安全级别较高的身份验证、信息加密和数字签名等功能。企业高级证书使用两套密钥对，一对为加/解密密钥对，另一对为签名/验签密钥对。

Web server 证书——面向机构或个人订户，安装在订户的 Web 服务器中，在 Web 服务器和浏览器之间提供身份验证、信息加密等功能。

代码签名证书——面向机构或个人订户，主要颁发给软件开发商，主要功能是让订户了解软件代码发行方的身份，并且没有被篡改过。

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。

RA 系统一般为两层结构，分为 RA 服务器和 RA 受理点 LRA。LRA 是面向最终订户的注册机构，其主要功能是对订户提交的资料进行审核，以决定是否同意为该订户发放证书以及进行证书管理。LRA 的证书签发和管理请求由 RA 服务器转发给 CA。RA 服务器负责安全地在订户和 CA 服务器之间交换数据。

RA 的建设与运营应遵循《CFCA RA 建设管理办法》、《CFCA 注册机构运营规范》之规定以及与 CFCA 签署的相关协议。

1.3.3 订户

订户指使用 CFCA 证书的所有终端订户，在电子签名应用中，订户即为电子签名人。

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 申请证书以保证信息机密性的实体，“证书主体”是指与证书信息绑定的实体，它可以是个人、机构、基础设施（如防火墙、路由器）、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义务与责任，而证书主体则是证书所要证明的可信赖方。

1.3.4 依赖方

依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是订户。

1.3.5 其它参与者

在电子认证活动中除了电子认证服务机构（CFCA）、注册机构、订户和依赖方以外的参与者称为其它参与者。

1.4 证书应用

1.4.1 适合的证书应用

CFCA 的数字证书适合应用在网上银行、电子商务、电子政务、企业信息化、网上信息传递以及公共服务等各领域，为建设网络信任环境提供基础性信任服

务，详情请咨询 400-880-9888。

1.4.2 限制的证书应用

CFCA 的数字证书不能在如下方面使用：

1、任何与国家或地方法律、法规规定相违背的应用系统；

2、CFCA 不认可的证书应用系统。

1.5 策略管理

1.5.1 策略文档管理机构

CPS 的制定与修订由业务部负责并牵头组成“CPS 编写组”，办公室、市场部、运行部、技术支持部派人参加。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，请联系：

部门：业务部

电话：010-83526220

传真：010-63555032

邮件：zhaoyu@cfca.com.cn

地址：中国北京宣武区右安门内新安南里甲 1 号

1.5.3 决定 CPS 符合策略的机构

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。

1.5.4 CPS 批准程序

“CPS 编写组”负责起草或修订 CPS 形成讨论稿（或 CPS 修订内容），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 送审稿提交公司法律顾问审阅。在取得法律顾问的意见书后，“CPS 编写组”将经法律顾问审阅过的 CPS 送审稿连同法律顾问的意见书提交业务部，由业务部确定 CPS 文本格式和版本号，形成定稿。

CPS 定稿经业务部分管领导审阅后，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，包括但不限于网站公布和向客户或合作对象书面提交。发布工作由业务部协调相关部门完成，并将 CPS 电子版和法律顾问的意见书交办公室存档。

CPS 的网上发布遵照《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。业务部负责自发布之日起 20 天内向行业主管部门报备。

1.6 定义和缩写

见附录 B《定义和缩写》

2 信息发布与信息管理

2.1 信息库

CFCA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。CFCA 信息库包括但不限于以下内容：证书、CRL，CPS，技术支持手册、CFCA 网站信息以及 CFCA 不定期发布的信息。CFCA 信息库不会对从 CFCA 发出的任何证书和证书吊销信息进行修改，而只会准确地描述上述内容。

2.2 *认证信息的发布

对于 OCA 系统，CFCA 根据 X.509 标准在 OCA 系统的信息库上公布订户证书的相关信息，并发布证书和 CRL。

对于 OCA2 系统，CFCA 根据 X.509 标准在 OCA2 系统的信息库上公布证书的相关信息，并发布证书和 CRL，也可以通过 OCSP 协议对其证书状态进行实时查询，OCSP 提供实时证书状态查询功能。

CPS 以及相关业务规则在 CFCA 网站上发布。

2.3 发布的时间或频率

CPS 以及相关业务规则在修改完成后 15 个工作日内发布到 CFCA 网站上；订户的证书信息实时发布到信息库上；CFCA 将在证书吊销后一小时内在信息库上更新 CRL，根据需要，也可以人工方式实时发布最新 CRL。

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。CPS 经由“CPS 编写组”编写定稿，并经总经理审核通过后，颁布在 CFCA 网站上（http://www.cfca.com.cn）供访问者自由浏览。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

CFCA 签发的证书采用 X.500 定义的甄别名称（DN）标准来唯一标识一张证书使用者的身份信息。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，用来唯一标识订户的 X.500 名称。此域需要填写反映订户真实身份的、具有实际意义的、与法律不冲突的内容。

3.1.3 订户的匿名或伪名

使用匿名的订户提交的证书申请材料由于不符合要求，将无法通过 RA 的审核，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 保证订户的 DN 是唯一的。同一个订户申请多张证书时，各证书通过顺序号加以区别。

3.1.6 商标的识别、鉴别和角色

订户应向CFCA保证（承诺）并向RA及证书依赖方声明，申请证书时所提供的信息未以任何方式侵犯或违反第三者的注册商标权、服务商标权、商用名称权、公司名称权或任何其它知识产权。

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 的数字签名来完成的。订户签名私钥（private key）由订户在订户端生成，订户发出的数据包中包含用签名私钥进行的数字签名，其他各方用对应的验证公钥可以验证这个签名。因此，订户被视作其签名私钥的唯一持有者。在订户委托 CA 机构或其他可信服务商代替订户生成密钥对的情况下，也可以认为订户是其签名私钥的唯一持有者。CFCA 要求订户妥善保管自己的签名私钥。

3.2.2 组织机构身份的鉴别

组织机构订户在证书申请前应指定并授权证书的申请代表，并接受证书申请的有关条款，承担相应的责任。鉴别组织机构的身份时，指定证书申请者须向 RA 审核人员提供有效证明文件，在填写申请表时加盖企业公章以证明该申请的有效性。如该机构申请 Webserver 证书，还需向注册机构提交相关域名或 IP 地址及拥有该域名或 IP 地址的证明。

CFCA 授权的注册机构将复核并验证申请文件的真实性，并进行批准申请或拒绝申请的操作。

3.2.3 个人身份的鉴别

个人订户持个人有效身份证件，包括：身份证、军官证、士兵证、护照、武装警察身份证、户口本、港澳居民往来内地通行证、台湾居民往来内地通行证等（以上可任择其一），提出证书申请，并接受证书申请的有关条款(见证书申请表)，承担相应的责任。

CFCA 授权的注册机构将复核并验证申请文件的真实性，并进行批准申请或拒绝申请的操作。

3.2.4 没有验证的订户信息

无。

3.2.5 授权确认

当申请者代表个人或组织机构申请证书时，需要出示足够的证明信息以证

明个人或组织机构是否真实存在，申请者是否已获得个人或组织机构的授权。CFCA 或注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.6 互操作准则

无。

3.3 密钥更新请求的标识与鉴别

在订户证书到期后，订户需要对原有证书进行更新。CFCA 要求普通证书的订户产生一个新的密钥对代替过期的密钥对，称作“ 密钥更新 ”。在密钥更新时，订户证书的 DN 没有改变。对于高级证书，证书到期时系统会自动对其进行更新。

若订户为一个现存的密钥对申请一个新证书，则称为 “ 证书更新 ”。

3.3.1 常规密钥更新的标识与鉴别

CFCA 需要订户提供书面申请进行密钥更新操作，密钥更新的同时证书也进行更新，订户更新密钥的流程详见本 CPS 的 4.7。

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，订户证书吊销后的密钥更新处理流程见本 CPS 的 4.2。

3.4 吊销请求的标识与鉴别

满足 4.9.1 节 “ 证书吊销条件 ” 的情况时，注册机构应当审核吊销申请者

的书面申请材料和证书 DN 信息，在审核通过的情况下由注册机构进行吊销操作。证书吊销请求的标识与鉴别流程见本 CPS 的 4.9.3。

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

任何自然人、具有独立法人资格的企事业单位、社会团体等各类组织机构需要在应用中进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，可向 CFCA 或其授权的注册机构提出证书申请。

个人证书由证书使用者本人提出申请；企业证书由企业、组织机构授权的人员申请；Web server 证书由域名拥有机构或个人、或被授权使用该域名的机构中的被授权人申请；代码签名证书由软件开发者本人或软件开发商授权的人员提出申请。

4.1.2 注册过程与责任

4.1.2.1 最终订户

最终订户须明确表示其愿意接受订户协议中所规定的相关责任与义务（如本 CPS9.6.3 所述），并需要完成以下注册过程：

- 填写证书申请表，并提供真实、准确的申请信息；
- 生成或委托生成密钥对；

- 将其公钥通过注册机构或直接传送至 CA；
- 证明其拥有与传送至 CA 的公钥相对应的私钥。

4.1.2.2 注册机构

注册机构须与 CFCA 签订相关协议并同意遵守《CFCA 注册机构运营规范》，并需提供相关的身份证明材料及联系信息。在签订协议的过程中，或在产生 RA 密钥对之前，注册机构须与 CFCA 共同商定合适的 DN 名称及证书内容。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

证书申请者向注册机构提交证书申请后，注册机构对以下申请材料进行检查:

机构订户：参照 3.2.2 节的规定。

个人订户：参照 3.2.3 节的规定。

注册机构需要审查订户的证书申请表格是否按照要求填写、申请材料是否齐全、资质证明材料是否符合要求（如机构订户是否在申请表上加盖公章）。详细要求请参见《CFCA 注册机构运营规范》。

4.2.2 证书申请批准和拒绝

注册机构对证书申请者提交的申请信息及身份信息进行鉴别，鉴别其是否完整、真实、有效。经鉴别符合要求后，将批准申请。如果申请者未能通过审核，注册机构将拒绝申请者的申请，并通知申请者；对于未通过审核的原因，注册机构可以不予解释。

4.2.3 处理证书申请的时间

CFCA 及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符合要求的情况下，处理证书申请的时间不超过 5 个工作日。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

注册机构将客户信息录入系统，通过基于 SPKM 协议的安全通道发送至 CFCA。CFCA 将生成订户下载证书用的凭证，同时将证书下载凭证返回注册机构。注册机构以安全的形式将证书下载凭证提交证书申请者。

CFCA 负责验证注册机构的身份与权限，根据注册机构提交的申请信息向注册机构返回申请者下载证书用的凭证。

4.3.2 电子认证服务机构和注册机构对订户的通告

无论是拒绝还是批准订户的证书申请，注册机构有义务告知订户申请结果。

订户申请批准后，注册机构将下载证书用的凭证以安全的方式提交订户，同时注册机构有义务告知订户在 CFCA 规定的时间内（即 14 天内）下载证书。

4.4 证书接受

4.4.1 *构成接受证书的行为

OCA 系统的申请者收到证书下载凭证后，应在 14 天内登录相关网站或通过 direct 软件下载数字证书。 OCA2 系统的申请者收到证书下载凭证后，应在 14

天内登录相关网站下载数字证书。证书下载完成后视为已经接受证书。如果订户在 14 天内没有进行证书下载操作，证书下载凭证将失效；如果订户在下载证书时发生错误，没有得到证书，而系统记录显示订户下载成功，也同样视为客户已经接受证书（CFCA 技术支持人员有义务协助客户正确地获取证书）。

4.4.2 *电子认证服务机构对证书的发布

OCA 系统在签发证书的同时会将该证书发布到对外信息库上进行公开。

OCA2 系统在签发证书的同时会将该证书发布到对外信息库上进行公开。

4.4.3 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 和 RA 不对其他实体进行通告，订户和依赖方可以在信息库上自行查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在使用私钥和证书时须遵循以下约定：

1、 订户只能在规定的范围内（在本 CPS1.4.1 节定义）使用私钥和证书，并对使用行为承担责任；

2、 订户在使用证书时必须遵守《CFCA 数字证书服务协议》及本 CPS 的要求；

3、 订户应当妥善保存其私钥，避免他人未经本人授权而使用本人证书情形的发生。在证书到期或被吊销后，订户应当停止使用该证书。

4.5.2 依赖方公钥和证书的使用

在依赖方接受数字签名信息后需要：

1、 获得数字签名对应的证书及信任链；

2、 确认该签名对应的证书是依赖方信任的证书；

3、 证书的用途适用于对应的签名；

4、 使用证书上的公钥验证签名；

5、 确认数字签名对应的证书状态正常，没有进入 CRL 列表。

依赖方需要采用合适的软（硬）件进行数字签名的验证工作，包括验证证书链及链中所有证书的数字签名。

4.6 证书更新

证书更新是指订户在不改变现有公钥或其它证书信息的情况下申请一张新证书。目前只对高级证书提供该项服务。

4.6.1 证书更新的情形

在证书有效期内，高级证书订户的旧加密密钥丢失或损坏的情况下可以申请证书更新。

4.6.2请求证书更新的实体

个人高级证书由证书使用者本人提出申请；企业高级证书由企业、组织机构授权的人员申请。

4.6.3 证书更新请求的处理

订户向注册机构提交证书更新申请后，注册机构对以下申请材料进行检查：

机构订户：参照 3.2.2 节的规定。

个人订户：参照 3.2.3 节的规定。

注册机构需要审查订户的证书申请表格是否按照要求填写、申请材料是否齐全、资质证明材料是否符合要求（如机构订户是否在申请表上加盖公章）。

注册机构对订户提交的申请信息及身份信息进行完整性、准确性、真实性的鉴别(详见《CFCA 注册机构运营规范》，经鉴别符合要求后，将批准申请。如果订户未能通过审核，注册机构将拒绝订户的申请。对于未通过审核的原因，注册机构可以不予解释。

注册机构将证书更新请求通过基于 SPKM 协议的安全通道发送至电子认证服务机构。电子认证服务机构将生成订户下载证书用的凭证，同时将证书下载凭证返回注册机构，注册机构以安全的方式将证书下载凭证提交订户。

电子认证服务机构负责验证注册机构的身份与权限，根据注册机构提交的申请信息向注册机构返回申请者下载证书用的凭证。

4.6.4 颁发新证书时对订户的通告

同本 CPS4.3.2 之规定。

4.6.5 *构成接受更新证书的行为

OCA 系统的申请者收到证书下载凭证后，应在 14 天内登录相关网站或通过 direct 软件下载数字证书。 OCA2 系统的申请者收到证书下载凭证后，应在 14

天内登录相关网站下载数字证书。证书下载完成后视为已经接受证书。如果订户在 14 天内没有进行证书下载操作，证书下载凭证将失效；如果订户在下载证书时发生错误，没有得到证书，而系统记录显示订户下载成功，也同样视为客户已经接受证书（CFCA 技术支持人员有义务协助客户正确地获取证书。）

4.6.6 电子认证服务机构对更新证书的发布

同本 CPS4.4.2 之规定。

4.6.7 电子认证服务机构对其它实体的通告

同本 CPS4.4.3 之规定。

4.7 证书密钥更新

证书密钥更新是指订户需要生成新密钥并申请为新公钥签发新证书。

4.7.1 证书密钥更新的情形

证书密钥更新有两种情况：补发和换发。补发是指在证书有效期内，订户更新证书（密钥）的操作，补发操作成功时，旧证书将被吊销，新证书有效期从补发成功之日起到旧证书失效日止。换发是指在证书将要过期的三个月内或证书过期后，订户申请更换证书（密钥）的操作，换发操作成功时，旧证书将被吊销，新证书有效期将从证书换发之日起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期）。补发和换发时，证书 DN 均不改变。

以下情况订户需要申请证书补发：

1、 订户忘记或泄漏了证书使用口令；

2、 订户证书（文件）丢失或损坏，例如存放证书的介质损坏；

3、 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）。

以下情况订户需要申请证书换发：订户证书到期或已经过期。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体与本 CPS4.1.1 中的证书申请实体相同。

4.7.3 证书密钥更新请求的处理

订户向注册机构提交密钥更新申请后，注册机构对以下申请材料进行检查：

机构订户：参照 3.2.2 节的规定。

个人订户：参照 3.2.3 节的规定。

注册机构需要审查订户的证书申请表格是否按照要求填写、申请材料是否齐全、资质证明材料是否符合要求（如机构订户是否在申请表上加盖公章）。

注册机构对订户提交的申请信息及身份信息进行完整性、准确性、真实性的鉴别(详见《CFCA 注册机构运营规范》)，经鉴别符合要求后，将批准申请。如果订户未能通过审核，注册机构将拒绝订户的申请。对于未通过审核的原因，注册机构可以不予解释。

注册机构将密钥更新请求通过基于 SPKM 协议的安全通道发送至 CFCA。CFCA 将生成订户下载证书用的凭证，同时将证书下载凭证返回注册机构，注册机构以安全的方式将证书下载凭证提交订户。

CFCA 负责验证注册机构的身份与权限，根据注册机构提交的申请信息向注册机构返回申请者下载证书用的凭证。

4.7.4 颁发新证书时对订户的通告

颁发新证书时对订户的通告同本 CPS 第 4.3.2 节的规定。

4.7.5 构成接受密钥更新证书的行为

构成接受密钥更新证书的行为同本 CPS 第 4.4.1 的规定。

4.7.6 *电子认证服务机构对密钥更新证书的发布

OCA 系统中，电子认证服务机构在签发证书的同时会将密钥更新证书发布到对外信息库上进行公开；同时将旧证书序列号发布到 CRL 列表中。

OCA2 系统中，电子认证服务机构在签发密钥更新证书的同时会将证书发布到对外信息库上进行公开；同时将旧证书序列号发布到 CRL 列表中。

4.7.7 电子认证服务机构对其他实体的通告

对于其签发的证书，CFCA 及其 RA 不对其他实体进行通告。

4.8 证书变更

无。

4.9 证书吊销和挂起

4.9.1 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、当注册机构或 CA 发现订户申请证书时，提供的资料不真实；

2、订户没有按照规定缴纳数字证书服务费用；

3、订户未履行证书服务责任书约定的义务；

4、当注册机构或 CA 发现订户主体消亡；

5、根据法律法规或司法部门的要求，对订户证书进行吊销；

6、订户声明不再使用证书并要求注册机构予以吊销；

7、订户相信或怀疑密钥泄漏或遭受攻击，要求吊销数字证书。

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 RA 审核通过后吊销证书的情形；被动吊销是指当 RA 或 CA 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。当出现上述提到的第 1-5 种情况时，适用于被动吊销，6、7 种情况适用于主动吊销。

4.9.2 请求证书吊销的实体

在符合本 CPS4.9.1 所述的情形下，请求证书吊销的实体与本 CPS4.1.1 证书申请实体相同。

另外，注册机构或 CFCA 也可以在本 CPS4.9.1 所述的情形下主动吊销订户的证书。

4.9.3 请求吊销的流程

1、 当最终订户吊销证书时可按以下流程进行：

1) 订户（或其授权委托人）填写书面申请表并签名或盖章，同时提交合法的证明材料，向 CFCA 或注册机构提出吊销证书请求。该流程类似于证书注册的流程，不同之处在于订户需要填写的申请表格为吊销申请表。

2) CFCA 或接到吊销申请的注册机构，验证申请者身份及吊销理由的正当性，并对审核资料书面归档。

3) CFCA 或证书注册机构在验证吊销申请后吊销证书。

4) CFCA 及时将证书吊销信息发布到 CFCA 信息库和目录服务。

2、当 RA 提出吊销 RA 证书时，需要正式向 CFCA 提出吊销请求，由 CA 完成吊销操作。CFCA 也可以根据情况主动发起吊销 RA 证书操作。该 RA 应将由其保管的订户信息在五个工作日内完整地移交给 CFCA。

4.9.4 吊销请求宽限期

订户一旦发现需要吊销证书，应向发放该证书的注册机构及时提出吊销请求。全部工作应当在 4 小时内完成。

4.9.5 电子认证服务机构处理吊销请求的时限

CFCA 或其授权的证书注册机构从收到吊销请求到审核完成，做出吊销决定并将吊销证书发布到目录服务，全部工作应当在 4 小时内完成。从订户正式提出证书吊销申请到证书正式吊销前 4 小时内因使用该证书造成的损失，CFCA 不予承担。

说明：订户在正式提出证书吊销申请后不得在交易中继续使用此证书，否则由此产生的后果，由订户自行承担。订户在正式提出证书吊销申请后必须立即将此情况通知与此证书相关的依赖方，以便在交易中停止使用该张证书，否则由此产生的后果，由订户自行承担。

4.9.6 依赖方检查证书吊销的要求

依赖方应当检查他们所信任的证书是否被吊销。检查方式是通过查询 CFCA 发布的 CRL 完成。

4.9.7 CRL 发布频率

CRL 发布频率为 1 小时一次，在发布的同时对原有内容进行更新。

4.9.8 CRL 发布的最大滞后时间

CFCA 在生成 CRL 的 1 小时后会更新信息库。

4.9.9 在线的吊销/状态查询的可用性

CFCA 向订户和依赖方提供 CRL 服务，该服务 7X24 小时可用。

4.9.10 在线的吊销查询要求

依赖方在信赖一张证书前必须对此证书进行证书状态查询，查询方式为检查 CRL，CFCA 没有设置任何读取权限。

4.9.11 吊销信息的其他发布形式

CFCA 目前尚未提供。

4.9.12 对密钥遭攻击的特别处理要求

当 CFCA 发现、或有充足的理由相信根密钥泄漏时，CFCA 将会采取合理、安全、及时的措施通知证书的潜在依赖方。

4.9.13 证书挂起

CFCA目前无此业务。

4.10 证书状态服务

4.10.1 *操作特征

OCA 系统中，证书状态可以通过 LDAP 目录查询服务获得。

OCA2 系统中，证书状态可以通过 LDAP 目录查询和 OCSP 查询服务获得。

4.10.2 服务可用性

CFCA 提供 7X24 小时不间断证书状态查询服务。

4.11 订购结束

以下三种情形将被视为订购结束：

1、订户在证书到期后两周内没有提出对证书密钥进行更新，将被视为订购结束。

2、在证书有效期内，订户主动提出对证书进行吊销视为订购结束，CFCA 将按照“证书吊销流程”处理订户申请。

3、被动吊销视为订购结束。

4.12 *密钥生成、备份与恢复

对于普通证书：

为保证订户密钥的安全性和唯一性，CFCA 建议订户自己生成密钥对并进行备份，在私钥丢失或被怀疑泄漏后，需及时申请密钥更新。在订户委托 CFCA 或其它可信服务商代替生成密钥对的情况下，CFCA 会从技术和制度上保证被委托方不会留存私钥的备份。

对于高级证书：

OCA 系统中，高级证书订户的加/解密密钥对由 CFCA 产生，签名/验签密钥对由订户自己产生。

OCA2 系统中，高级证书订户的加/解密密钥对由国家设立的专门密钥管理机构（KMC，密钥管理中心）生成、备份和恢复。目前 KMC 托管在 CFCA，系统每天对数据进行备份。签名/验签密钥对由订户自己产生。

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中国金融电子化公司（国家金融重点保护单位）配楼内，其备份机房位于中国银联上海信息中心机房大楼，进入机房须经过三道审核，机房电磁屏蔽指标达到国家 BMB3 B 级标准。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

外来人员进入机房大楼，需经过中国金融电子化公司、CFCA 两道的门卫检查。进入 CFCA 办公区域需要有 CFCA 工作人员陪同。

操作人员进入安全区机房，须经过双人双指纹认证、门禁授权卡身份认证，并有 24 小时视频监控设备进行监控。

操作人员进入最安全区机房，须经过两次双人双指纹认证，并且对所有操作过程进行记录。

5.1.3 电力与空调

CFCA 采用独立的双线路方式供电，同时采用双 UPS 方式，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，

CFCA 还自备柴油发电机，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》、GB50174-93 《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

CFCA CA 系统使用的存储介质被放置在防磁、防静电干扰的环境中，并处于 24 小时录像监控下，可以防止由于环境变化和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；加密设备在抛弃前要根据生产商的指导做归零处理。

5.1.8 异地备份

为保证数据的完整性与可恢复性，预防系统因不稳定因素导致无法正常运行的情况发生，CFCA 在上海建立了异地备份中心，存储系统的备份数据。异地备份的内容包括：CA 数据（包含所有日志信息）、目录数据。

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。

5.3 人员控制

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。

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 独立和约人的要求

CFCA 目前没有独立和约人。

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培训和相关的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

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，包括企业（个人）姓名、证件号码、地址、邮箱、联系人等信息。

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

对于 CA 密钥和订户证书生命周期内的管理事件日志，CFCA 每半年进行一次内部检查、审计。

对于系统安全事件和系统操作事件日志，CFCA 每周进行一次检查、处理。

对于物理设施的访问日志，CFCA 每月进行一次检查、处理。

5.4.3 审计日志的保存期限

密钥和证书信息档案至少保存到证书失效后 5 年，审计文档至少保存 1 年。

5.4.4 审计日志的保护

CFCA 建立完善的管理制度，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，并且有异地备份，严禁未经授权的任何操作。

5.4.5 审计日志备份程序

CFCA 每天进行一次数据备份操作。

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 归档记录的类型见本 CPS 的第 5.4.1 节。除此之外，对订户证书、CA 证书也进行归档。

5.5.2 归档记录的保存期限

自证书期满或撤销之日起，记录将会保存至少 5 年以上。如果法律需要，CFCA 将延长记录保存期限。

5.5.3 归档文件的保护

CFCA 根据本 CPS 的存档要求保护存档记录，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。

5.5.4 归档文件的备份程序

系统每天对证书信息全部进行备份，该备份数据采用物理隔离方式，与外界不发生信息交互。

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完整性进行检验。

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下或因不可抗力造成 CFCA 主中心机房无法正常提供服务时，CFCA 将依据《CFCA 业务持续计划》（保密）实施修复。

CFCA 承诺：异地灾难备份中心与 CFCA 生产系统之间的距离不少于 1000 公里，保证在发生灾难 24 小时之内恢复 CA 的目录查询服务，一月之内恢复证书签发和证书管理服务。在数据恢复中，最多允许丢失发生灾难后 48 小时内的数据。

5.7.2 计算资源、软件和/或数据的损坏

当计算资源、软件和/或数据受到破坏后，将依据《CFCA 系统故障报告与处理流程》（保密）进行处理，必要时启动备份系统。

5.7.3 实体私钥损害处理程序

当实体私钥发生泄漏时，CFCA 将依据《CFCA CA 签名私钥泄漏紧急预案》、

《CFCA CA 签名私钥泄漏的紧急处理流程》（以上为保密文档）进行处理。

5.7.4 灾难后的业务连续性能力

灾难发生后 CFCA 将依据《CFCA 业务持续计划》（保密）的有关规定，立即启用异地灾难备份中心为订户继续提供服务，保证业务的持续进行。

5.8 电子认证服务机构或注册机构的终止

当 CFCA 及其 RA 需要停止其业务时，将会严格按照《电子认证服务管理办法》第四章（第二十三条至第二十七条）之规定执行。

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，加密机通过国家密码主管部门的批准和许可。在生成CA密钥对时，三名安全管理员必须同时到达CFCA最安全区，任何人无法独立完成操作。私钥不能以明文方式离开加密机。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，并通过了国家密码主管部门的鉴定。

2、RA密钥的生成

RA的签名私钥由自己产生，CFCA推荐使用加密机等硬件加密设备产生密钥，亦可使用软件产生密钥。RA的加密密钥由CA用软件产生。

3、订户密钥的生成

对于普通证书，签名密钥对在订户端产生，订户可以通过硬件或者软件产生签名私钥。订户可以自主选择国家密码主管部门批准的硬件设备生成签名密钥对，例如加密机、USB Key、智能卡等。订户在选择这些设备时应事先向CFCA咨询有关系统兼容性事宜(可以在CFCA网站查询)。CFCA并不是硬件设备提供商，不对由硬件设备造成的任何损失负责。

订户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。

对于高级证书：

OCA 系统中，高级证书订户的加/解密密钥对由 CA 产生，签名/验签密钥对由订户自己产生。

OCA2 系统中，高级证书订户的加/解密密钥对由国家设立的专门密钥管理机构（KMC，密钥管理中心）生成、备份和恢复。签名/验签密钥对由订户自己产生。

6.1.2 *私钥传送给订户

CFCA 一般不提供代订户生成签名私钥的服务。在订户委托 CFCA 或其它可信服务商代替生成密钥对的情况下，CFCA 会从技术和制度上保证被委托方不会留存私钥的备份。私钥会通过离线或在线的安全方式传送给订户。

OCA 系统中，高级证书订户的加/解密密钥对由 CA 生成，其中的私钥会通过离线或在线的安全方式传送给订户。

OCA2 系统中，高级证书订户的加/解密密钥对由国家设立的专门密钥管理机构（KMC，密钥管理中心）生成，其中的私钥会通过离线或在线的安全方式传

送给订户。

6.1.3 公钥传送给证书签发机构

订户通过与 CFCA 建立基于 SPKM 协议的安全通道把公钥发送给 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）可从 CFCA 的信息库获得。

6.1.5 密钥的长度

CFCA 完全遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前：

CFCA 用于签名的 RSA 密钥长度为 1024 位；

注册机构用于签名和加密的 RSA 密钥长度为 1024 位；

订户产生的签名密钥长度为 1024 位；

订户产生的加密密钥长度为 1024 位；

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理机构许可的加密设备生成，这些设备遵从国家密码管理机构的有关规范和标准，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。

6.1.7 密钥使用目的

CA 私钥用于签发自身证书、下级 CA 证书、订户证书和 CRL，CA 的公钥用于验证私钥签名。

订户的签名密钥对可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性，加密密钥对可以用于信息加密和解密。

订户的签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

密码模块（加密机）安置在 CFCA 核心区域，使用通过国家密码管理机构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、ECC、Diffe Hellman 等公钥算法，RSA 模长可选 512、768、1024、2048 比特；支持 SDBI、DES、TRIPLE-DES、IDEA、RC2、RC4、RC5 等对称算法，支持 128 比特高强度加密；支持 MD2、MD5、SHA1、SDHI 等 HASH 算法。

6.2.2 私钥多人控制（m 选 n）

CFCA 从技术及制度上保证了敏感的加密操作需要在多个可信角色的共同参与下才能完成。在操作现场，必须有超过 2 位并具备权限的密钥管理人员和操作人员，同时对加密机中的密钥进行操作，任何人无法独立完成操作。

6.2.3 私钥托管

对于 CA 私钥,CFCA 无托管业务；对于订户加密私钥的托管，CFCA 将根据国家相关部门之规定执行。

6.2.4 私钥备份

1、CA 的私钥保存在防高温、防潮湿及防磁场影响的环境中，对私钥的备份操作须 3 人以上(包括 3 人)才可完成。

2、CFCA 每天对 CA 的全部私钥（包括订户高级证书的加密私钥）进行备份。

3、RA 的私钥由 RA 产生，由 RA 自行备份。

4、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 5 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 不对 RA 和订户的私钥进行归档。

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，在本（异）地同时部署了备份加密设

备，CA 密钥对在备份传递时以离线加密方式进行。

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

6.2.8.1 个人和企业证书

个人和企业证书订户的私钥可以存放在订户计算机软件密码模块中，也可以存放在硬件密码模块中。当私钥存放在计算机软件密码模块中时，订户需要采取合理的措施防止其他人在非授权情况下使用该机器。当密码模块完成对私钥保护口令的验证后，意味着私钥被激活，可以使用。

6.2.8.2 Web server 证书

对于 Web server 证书，如果没有使用硬件密码模块产生、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。

6.2.8.3 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 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

对于个人和企业证书，当软（硬）件密码模块被下载、订户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。对于 Web server 证书，当服务程序被下载、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、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。

订户根据实际情况自行保存并销毁私钥。(在加密私钥到期后一定期限内建议订户继续保存该私钥，以便解开前期加密的信息。)

6.2.11 密码模块的评估

CFCA使用国家密码管理机构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。密钥操作性能如下：

指标		加密机
1024 位 RSA 算法（128 字节报文）	生 成 密 钥	48 秒/次
	公 钥 运 算	272 次/秒
	私 钥 运 算	63 次/秒

2048 位 RSA 算法（256 字节报文）	生 成 密 钥	58 秒/次
	公 钥 运 算	52 次/秒
	私 钥 运 算	1.44 次/秒
SSF33（1024 字节）	加 密	12Mbps
	解 密	12Mbps

6.3 密钥对管理的其它方面

6.3.1 公钥归档

作为 CFCA 备份策略的一部分，CA、注册机构和订户的证书都已经归档保存。

6.3.2 证书操作期和密钥对使用期限

CA 证书的有效期为 15 年，CFCA 能够发放的订户证书有效期为 1-5 年。各注册机构在遵循与 CFCA 合作协议的基础上，可以根据实际情况向订户提供有效期在 5 年以内的证书。

CA 密钥对使用期限和 CA 证书的有效期保持一致，均为 15 年。订户证书的密钥对和订户证书的有效期保持一致。

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、 对于注册机构和订户，激活数据是保护私钥的密码。CFCA 推荐注册机构和订户使用强壮口令来保证私钥的安全性，该口令需要：

- 由订户产生
- 至少为 6 位字符或数字
- 至少包含一个字符和一个数字
- 不能包含很多相同的字符
- 不能和订户名相同
- 不能包含订户信息中较长的字符串

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秘密份额，并且须签署协议来承诺所承担的责任。

2、 注册机构必须将管理员和注册机构的私钥以加密的形式保存，并使用口令保护，在使用浏览器时，使用“ 高安全 ”选项。

3、 订户必须以加密的形式保存私钥，建议使用双因素认证（如硬件设备加强壮口令）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 IC 卡和加密设备，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 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。

6.5.1 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、多层异构的防火墙设置、人员职责分割、内部操作控制、业务持续计划等各方面。

6.5.2 计算机安全评估

根据 ISO/IEC 15408-1/2/3:1999 （Information technology-Security techniques-Evaluation Criteria for IT Security)、GB/T 18336.1-2001 标准，CFCA 证书认证系统通过了国家密码管理局、国家信息安全测评中心等有关部门的评估认证。(相应的资质证书可以在 CFCA 网站上查询)

6.6 生命周期技术控制

6.6.1 系统开发控制

CFCA 的系统由符合国家相关安全标准和具有密码标准资质的可靠开发商开发，其开发过程符合 CFCA 系统管理的各项规定。

6.6.2 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 (CA 数据、目录数据、日志信息)，每天安排专人定时进行备份，每月由专人负责数据恢复，以验证数据的有效性。

6.6.3 生命期的安全控制

CFCA 的系统由具有符合国家相关安全和密码标准资质的可靠开发商开发，其开发过程符合 CFCA 系统管理的各项规定。其产品源代码保存在国家密码管理

局，以保证系统的延续性。

6.7 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、多级异构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 CFCA 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。

6.8 时间戳

证书、CRL、认证服务系统日志均包含时间信息，该信息无需加密保存。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

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

X.509 V3 证书的扩充部分主要包括:

7.1.2.1 颁发机构密钥标识符

CFCA 最终订户证书及中级 CA 证书中包含签发 CA 密钥标识符扩展项，当证书签发者包含主题密钥标识扩展项时,签发 CA 密钥标识符由 160 位的签发证书的 CA 进行 SHA-1 散列运算后的值构成；否则，它将包含签发 CA 的主题和序列号。该扩展项的 criticality 域设置为 FALSE。

7.1.2.2 主题密钥标识符

当证书包含主题密钥标识符扩展项时，该值由证书主题的公钥产生。使用该扩展项时，其扩展域的 criticality 域设为 FALSE。

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,该项定义遵照 RFC3280 之规定

7.1.2.4 Basic constraints: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 RFC3280 之规定。

7.1.2.5 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。该扩展项的 criticality 项设为 FALSE。

7.1.2.6 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 RFC3280 之规定，该扩展项的 criticality 项设为 FALSE。

7.1.3 算法对象标识符

CFCA签发的证书符合RFC 3280标准，采用SHA-1 RSA算法签名。

7.1.4 名称形式

CFCA 签发的证书采用 X.500 定义的甄别名称（DN）标准来唯一标识一张证书使用者的身份信息。DN 必须包括以下五部分：

1、cn 部分（用来表示订户名）：

字节	个人普通证书	个人高级证书	企业普通证书	企业高级证书	Web server 证书	代码签名证书
1,2 字节：主版本号	4	4	4	4	域名或 IP 地址	机构名称或个人姓名的中文或英文
3 字节：次版本号	1	1	1	1		
@	分隔符号					

第 5 字节：证件类型编码	0、1、2、5、A、B、C、D、E、F	0、1、2、5、A、B、C、D、E、F	3、4、7、8、9	3、4、7、8、9		
第 6 字节：证书号码	相应的证件号码	相应的证件号码	相应的证件号码	相应的证件号码		
@	分隔符号					
RA 自定义内容	RA 自定义内容	RA 自定义内容	RA 自定义内容	RA 自定义内容		
@	分隔符号					
八字节数字	证件号码相同的证书持有者的顺序号					
cn 实例	041@011010172 0120326@jack@ 00000001	041@011010172 0120326@tom@0 0000003	041@3110101720120 6@zhongda@0000000 2	041@31101017201 206@zhongda@000 00001	www.sunny.com	温州银行或 WZCB

注：1）Direct Server 证书以 Server 开头，后续内容同企业高级证书。
cn 实例为 Server041@31101017201206@zhongda@00000001。
2）Web server 证书的 cn 内容为域名或 IP 地址。
3）代码签名证书的 cn 内容为机构名称或个人姓名。
4）证件号码部分最长为 20 个字节。
5）RA 自定义内容为可选项，最长为 50 个字节。
6）分隔符（@）为 CFCA 保留字符，证件号码、英文/拼音名、RA 自定义内容中不得使用。

2、ou[2]部分（用来表示证书类型）：

	个人普通证书	个人高级证书	企业普通证书	企业高级证书 (Direct Server 证书)	Web Server 证书	代码签名证书
ou=	Customers	Business Customers	Enterprises	Units	Web Servers	CodeSign

注：代表证书类型中的每个英文单词，第一个字母大写，其余小写。

3、ou[1]部分（用来表示注册机构的英文/拼音名简称）。ou[1]命名先由注册机构提交命名申请，标明 ou[1]的字符全名称（大小写英文字符串），经 CFCA 批准后方可使用。如中国建设银行：OU=CCB

4、o 部分：用来表示 CFCA 提供的证书认证系统的英文简称，目前有两个证书认证系统对外提供服务，分别命名如下：

o=CFCA Operation CA Entrust CA 系统第三层 CA 的英文简称

o=CFCA Operation CA2 国产 CA 系统对外提供服务的 CA 的英文简称

5、c 部分：(用来表示中国的英文简称，全部大写)

c=CN

7.1.5 名称限制

CFCA 签发的证书，其实体名称不允许为匿名或者伪名，必须是有明确含义的识别名称。

7.1.6 证书策略对象标识符

未使用本扩展域。

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（this Update）

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（本条款只适用于 OCA2 系统）

CFCA 认证系统签发的 OCSP 响应符合 RFC2560 标准。OCSP 响应至少包含如下表所述的基本域和内容。

域	值或值的限制
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。使用 sha1WithRSAEncryptio(OID:1.2.840.113549.1.1.5)算法签名。
颁发者	签发 OCSP 的实体。签发者公钥的 SHA1 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、证书状态以及证书吊销信息。
证书标	包括数据摘要算法(SHA1，OID: 1.3.14.3.2.26)、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。
证书吊销信息	当返回证书状态为吊销时包含吊销时间和吊销原因。

7.3.1 *版本号（本条款只适用于 OCA2 系统）

OCA2 系统可以提供支持 RFC 2560 1.0 版(X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP)的 OCSP 服务。通过 OCSP server 证书的私钥对正确的查询结果进行签名。

7.3.2 *OCSP 扩展项（本条款只适用于 OCA2 系统）

采用标准扩展，基于 X.509 版本 3 证书所使用的扩展模型，主要有：

1、随机数(Nonce)

2、证书吊销列表参考(CRL References)

3、可接受的回复类型(Acceptable Response Types)

4、证书吊销列表项目扩展(CRL Entry Extensions)

5、服务定位器（Service Locator）

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》规定，接受主管部门的评估和检查。

2、 其它评估。

评估的频率为：

1、年度评估：由 CFCA 邀请第三方的审计机构每年进行评估；

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

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。

8.3 评估者与被评估者的关系

评估者与被评估者应无任何业务、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 管理层将对审计报告进行评估，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

评估结果根据需要在内部进行传达，并根据要求上报给行业主管部门。

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

关于证书费用问题请咨询有关注册机构或 CFCA 市场部。

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，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、准确的个人信息，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

企业订户需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，他们必须合理地承担对订户及对依赖方的责任。

此要求对 CFCA 同样适用。

9.2.3 对最终实体的保险或担保范围

根据《中华人民共和国电子签名法》的规定，订户在此同意：由于 CFCA 的责任给订户造成的直接损失，CFCA 仅赔偿订户一定金额的直接损失，即 CFCA 将根据使用证书的种类，承诺一定额度的赔付，具体情况参见本 CPS 的９．８之规定。

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 与其授权的注册机构、订户、依赖方之间的协议、资料中未公开的内容等属于保密信息。

2、 订户私钥属于机密信息，订户应该根据本 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。

3、 所有对于 CFCA 或其相关机构的审计报告、审计结果等信息视为机密信息。

4、 有关认证系统的运营信息、技术手册等资料属于保密信息。

5、 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个人隐私信息；同时，CFCA 在同所有注册机构签署授权协议时，都将此条作为协议条款。

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，个人私密信息保密方案遵守现行法律和政策。任何人选择使用 CFCA 的任何服务，就表明已经同意接受 CFCA 的有关隐私保护声明,详细内容请参看 CFCA 网站 http://www.cfca.com.cn。

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，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，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、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、专利申请权等知识产权；CFCA 制订并发布的 CPS 以及相关政策、发布的证书和 CRL 均为 CFCA 的财产，CFCA 对其拥有知识产权； 在 CFCA 域内目录中使用的代表单位的甄别名称(DN),以及在同一域内发给最终实体的证书中的甄别名称都会包含一个相关的代表 CFCA 的名称，CFCA 对此拥有知识产权。

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为进行网上业务的各方提供信息安全保障。

CFCA 保证使用 CFCA 数字证书与安全软件的订户的网上交易信息对无关联的第三方是保密的，而且在网上传输中是不可篡改的，利用数字签名机制保证交易的不可抵赖性。

在订户通过 CFCA 数字证书对交易信息进行加密和签名的条件下，保证交易信息的保密性、完整性、抗抵赖性。

CFCA 的运作遵守《中华人民共和国电子签名法》等法律，接受行业主管部门的领导，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。

CFCA 或其授权的任何注册机构并非登记人或证书订户的代理人、受信人、受托人或其它代表。登记人或证书订户代理人无权以合约或其他方式约束 CFCA 或其授权的注册机构承担登记人或订户的代理人、受信人、受托人或其它代表之职责。

CFCA 保证在现有技术条件下签发的数字证书不会被伪造、篡改。在订户通过数字证书对交易信息进行加密和签名的条件下，保证交易信息对无关者是保密的，保证交易信息的完整性、抗抵赖性，CFCA 保证该交易对双方具有抗抵赖性。如果发生纠纷，CFCA 承担下述义务：

1） 提供签发该张订户数字证书的 CA 证书。

2） 提供该张数字证书在交易发生时，在或不在 CFCA 发布的 CRL 内的证明。

3） 对数字证书、数字签名、时间戳的真实性、有效性进行技术确认。

9.6.2 注册机构的陈述与担保

CFCA 通过注册机构向订户发放 CFCA 数字证书， 注册机构通过 LRA 面向证书订户，负责审核申请人的身份并决定接受或拒绝申请人申请、负责录入订户信息，并将证书申请信息安全地传送到 CA。

注册机构声明和承诺：

1、 根据 CFCA 制订的策略和运行管理规则，对订户的证书申请材料进行审核，通过审查确保证书中信息的真实性、完整性和准确性，并有权决定接受或拒绝证书申请；

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，如证书申请被批准，RA 有义务通知订户并且指导订户得到证书；

3、 RA 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不超过 5 个工作日。

4、 RA 须对订户的信息及与认证相关的信息妥善保存，保存期限为数字证书失效后五年。

5、 RA 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。

6、 基于 CFCA 规定的信息传输协议和标准与 CA 交换数据；

7、 证书签发及被吊销时及时通知订户。

8、 在接到具有授权的申请人关于证书管理的有效请求时，进行相应证书

管理操作，并保留全部操作记录和日志；

9、有义务通知订户阅读 CFCA 发布的 CPS 和《CFCA 数字证书服务协议》和其它相关规定，在订户完全知晓并同意 CPS 和《CFCA 数字证书服务协议》内容的前提下，为订户办理数字证书。

10、保留订户的信息及与认证相关的信息，保存期限为数字证书失效后五年。

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。

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 或原注册机构。如因订户故意或过失提供的资料不真实或资料改变后未及时通知 CFCA 或原注册机构，造成的损失由订户自己承担。

在通过注册机构的审核、录入后，订户即可获得数字证书的下载凭证，订户应妥善保管下载凭证，亲自用其中的密码从 CFCA 网站下载数字证书。订户获得的下载凭证密码为一次性使用，有效期为 14 天。如果在 14 天内没有下载数字证书，订户需要到注册机构重新办理。

订户应将证书用于合法目的并符合 CFCA 证书策略和本 CPS；

订户应对使用证书的行为承担责任。

使用可信系统产生密钥对，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。

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时，或者订户主体不存在，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，相关手续遵循注册机构的规定。

由于以下情况订户损害 CFCA 利益的，订户须向 CFCA 赔偿全部损失。这些情况是：

1) 订户在申请数字证书时没有提供真实、完整、准确信息，在这些信息变更时未及时通知 CFCA；

2) 订户一旦发现任何可能导致证书订户私钥安全性危机的情况，订户应立刻告知 CFCA 或证书注册机构。订户知道自己的私钥已经失密或者可能已经失密未及时告知有关各方、并终止使用；

3) 订户有其他过错或未履行双方约定。

订户有按期缴纳数字证书服务费的义务，费用标准请咨询注册机构。

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，应在规定的期限内到原数字证书注册机构更换。因订户逾期没有更换数字证书而引起的后果，CFCA 不承担责任。

9.6.4 依赖方的陈述与担保

依赖方声明和承诺：

1、使用适当的软件和/或硬件进行数字签名的验证或其它操作；

2、确信在交易前检查 CRL 获知证书状态和验证签名；

3、只在符合相关策略和本 CPS 规定的证书应用范围内信任该证书；

4、确认证书链的合法性；

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

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提供或未按照要求提供不准确和/或不真实和/或不完整的信息而获得 CFCA 签发的数字证书，订户在使用该证书时引起的责任，CFCA 不予承担。

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 不承担责任。

3、CFCA 对各类证书的适用范围作了规定，若证书被超范围使用或被用于其他不被允许的用途，CFCA 不承担责任。

4、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，但对此不承担法律或政策之外的责任。

5、对于明显由于 CFCA 的合作方或代理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 不承担赔偿责任。

6、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

不承担赔偿责任。

9.8 有限责任

CFCA 承担的赔偿责任是有限的，参见 9.9。

9.9 赔偿

订户或依赖方依据 CFCA 提供的认证服务进行民事活动遭受损失，而 CFCA 能够证明其提供的服务是按照《电子签名法》和向行业主管部门备案的 CPS 实施的，CFCA 将不予赔偿订户的损失。以下损失不在赔偿之列：

1) 任何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、或失去或无法使用任何数据、设备或软件；

2) 由上述损失相应生成或附带引起的损失或损害。

订户或依赖方在发现或怀疑由 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。

2、CFCA 对企业高级数字证书订户的赔偿上限为人民币捌拾万元整，即￥800,000.00 元；CFCA 对企业普通数字证书订户的赔偿上限为人民币伍拾万元整，即￥500,000.00 元。CFCA 对个人数字证书订户的赔偿上限为人民币贰万元整，即￥20,000.00 元。

3、CFCA 对企业数字证书依赖方的赔偿上限为人民币伍拾万元整，即￥500,000.00 元，对个人数字证书依赖方的赔偿上限为人民币贰万元整，即￥20,000.00 元。

9.10 有效期限与终止

本 CPS 自发布之日起生效，当新版本生效时，旧版本将自动失效。

9.10.1 有效期限

除非 CFCA 特别声明 CPS 提前终止，在 CFCA 颁布新版本 CPS 之前，本 CPS 一直有效。

9.10.2 终止

在本 CPS 终止之前，CFCA 将会对外公开声明，并尽量通知相关各方。

9.10.3 效力的终止与保留

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：010-83526220。

9.12 修订

CFCA 有权修订本 CPS，并将修订版本在网站上公布(http://www.cfca.com.cn)。

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。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 争议处理

订户或依赖方在发现或怀疑由 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，在采取任何解决途径之前，订户应首先通知 CFCA 及注册机构。

2、 争议解决的方式：

如果争议在最初通知的 10 天内未被解决，CFCA 将召集由 3 名安全认证专家组成的外部专家小组。外部专家小组以协助解决争议为目的，收集相关事实。专家小组应在成立后 10 天内（除非当事人同意将此段时限延长至一特定时段）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。但当事人一方若签署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。如果订户事后反悔并将争议提交仲裁，那么该建议将视为 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导致其它条款的不可执行性。

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。CP、CPS、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

无。

9.16.3 分割性

无。

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。

9.17 其它条款

无。

附录A、证书格式说明

(1) 个人普通证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Customers] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥(Public key）秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Digital Signature , Key Encipherment(A0)
基本限制 (Basic constraints)		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]

(2) 企业普通证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[enterprises] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Digital Signature , Key Encipherment(A0)
基本限制（Basic constraints）		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]

(3) Web server 证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Web Servers] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Digital Signature , Key Encipherment(A0)
基本限制（Basic constraints）		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]

(4)代码签名证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Codesign] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Digital Signature(80)
基本限制（Basic constraints）		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]

(5) 企业高级证书之加密证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Units] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Key Encipherment , Data Encipherment(30)
基本限制 (Basic constraints)		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]
1.2.156.1.8888		
微缩图算法		Sha1
微缩图		

(6) 企业高级证书之签名证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Units] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Digital Signature(80)
基本限制（Basic constraints）		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]
1.2.156.1.8888		
微缩图算法		Sha1

微缩图		

(7) 个人高级证书之加密证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Business Customers] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Key Encipherment , Data Encipherment(30)
基本限制 (Basic constraints)		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]
1.2.156.1.8888		
微缩图算法		Sha1

微缩图		

(8) 个人高级证书之签名证书

字段名称		字段内容
标准栏(Standard field)		
版本（Version）		X509 V3
序列号（Serial number）		
签名算法（Signature algorithm ID）		sha1RSA
发行者（Issuer）		O=CFCA Operation CA2 C=CN
有效期（Validity period）	有效期起始时间	[由 CFCA 与注册机构共同设定]
	有效期终止时间	[由 CFCA 与注册机构共同设定]
主题(Subject name)		cn=[根据 CFCA DN 规则设置的名称] ou=[Business Customers] ou=[注册机构] o=CFCA Operation CA2 c=CN
公钥（Subject public key info）		算法识别（Algorithm ID）：RSA 公开密码钥（Public key）：秘钥长度 1024-bit
标准延伸字段（Standard extension）		
颁发机构密钥标识符(Authorith key identifier)		F08D EDB3 41BB FBEF 081E 5502 C331 37EF 3C14 4ECD
主题密钥标识符(Subject key identifier)		由 CFCA 设定
密钥用法(key usage)		Digital Signature(80)
基本限制（Basic constraints）		最终实体(End Entity)
CRL 分布点（CRL distribution point）		分布点名称=[证书撤销分布点 Directory Address]
1.2.156.1.8888		
微缩图算法		Sha1

微缩图		

附录B、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)
LRA	本地注册机构（Local Registration Authority）
CRL	证书吊销列表(Certificate Revocation List)
OCSP	在线证书状态协议(Online Certificate Status Protocal)
CP	证书策略(Certificate Policy)
CPS	电子认证业务规则（Certificate practice Statement）
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	被颁发证书的证书主体。
依赖方	证书的接收者，他依赖于该证书和（或）该证书所验证的数字签名。在本标准中，术语“证书使用者”与“依赖方”可互换使用。

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，用来唯一标识订户的名称。此域需要填写反映订户真实身份的、具有实际意义的、与法律不冲突的内容。
OCA2	CFCA对外提供服务的一个运营CA，其全称为O=CFCA Operation CA2,C=CN。
OCA	CFCA对外提供服务的一个运营CA，其全称为O=CFCA Operation CA,C=CN。