中国金融认证中心

证书策略

（Certificate Policy

Of CFCA）

V3.0

2015 年 08 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
1.0	形成版本并审核通过			CFCA 安委会	2011 年 06 月
2.0	修订	根据 2013 年 4 月 7 日安委会评审结论修改相关内容	赵改侠	CFCA 安委会	2013 年 4 月
2.1	修订	依据 BR 的补充相关条款	赵改侠	CFCA 安委会	2014 年 3 月
3.0	修订	根据最新 CPS 以及政策变更修改，本 CP 适应于 CFCA 所有 CPS。	赵改侠 张翼	CFCA 安委会	2015 年 8 月

目　　录

1 概括性描述

1.1 概述

证书策略（CP，Certificate Policy）是认证机构（CA,Certification Authority）制订的一组策略，表明 CFCA PKI 体系中的各个参与者的划分与其义务，并包含 CFCA 证书基本策略。

本证书策略的适用范围为 CFCA 发放的证书。

1.2 文档名称与标识

此文档的名称为《CFCA 证书策略(CFCA CP)》。

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（Certification 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 与合作机构签署协议，合作机构可成为 CFCA 的注册机构，并遵照 CFCA 的《注册机构运营管理办法》开展数字证书业务。

CFCA 进行 webtrust 审计的 CA 系统所需要要的注册机构设在 CFCA 内部，由 CFCA 本身承担 RA 职责，不委托其它机构行使此职责。

1.3.3 订户及证书类型

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；“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。

1.4 证书应用

1.4.1 适合的证书应用

CFCA 证书支持相应的合法应用，具体应用场景和配套软件（如浏览器）在相应 CPS 1.4 节中说明。

1.4.2 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。

1.5 策略管理

1.5.1 策略文档管理机构

本 CP 的策略文档管理机构为 CFCA 业务部。当需要编写或修订本 CP 时，由业务部牵头组织相关人员成“CP 编写组”，总经理也可以根据需要临时设立“CP 编写组”，并指定编写组负责人。

1.5.2 联系方式

如对本 CP 有任何疑问，请与 CFCA 业务部联系：

电话：010-83526220

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 CP 符合策略的机构

“CP 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”将负责评估本 CP 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 CP 方可对外发布。

1.5.4 CP 批准程序

“CP 编写组”负责起草 CP 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。

“CP 编写组”负责将 CP 送审稿提交公司“安委会”审阅。在取得“安委会”评审意见后，“CP 编写组”据此进行修改并提交业务部，由业务部确定 CP 文本格式和版本号，形成定稿。

CP 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 CP。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。发布工作由业务部协调相关部门完成。

CP 的网上发布遵照《CFCA 网站管理办法》执行。自 CP 发布之日起，所有以各种形式对外提供的 CP 必须与网站公布的 CP 保持一致。

业务部定期对 CP 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业务部提出修订申请。本 CP 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，由业务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。

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 7X24 小时可访问；订户有特殊要求的，将根据订户的需求，适当提高 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。

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 身份标识与鉴别

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个人名称、组织机构名称、部门名称、组织机构信息与个人信息组合体，域名、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 CP 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。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。

具体甄别名规则见《CFCA DN 规则》、《CFCA 预植证书 DN 规则》文档。

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 CP 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 证书订户信息鉴别

订户在申请 CFCA 签发的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 或者 CFCA 的注册机构接受订户的证书申请后，应对订户的身份真实

性进行审核，并按照双方的约定妥善保存订户申请材料。具体鉴别内容参见CPS3.2.2 章节。

3.2.3 互操作准则

对于向CFCA 申请数字证书的订户,如申请的证书签发系统为进行WebTrust 审计的 CA 系统签发时，CFCA 承担对订户身份的鉴别职能，暂不委托其他机构行使此职责。如委托其他证书发放机构审核订户身份信息，对已经审核过的证书订户身份信息，CFCA 将会重新进行验证；其他情况不在此规定。

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。

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。在证书初次发放后的三个月内需进行补发时，CFCA 仅通过订户初次申请时的信息进行身份验证即可。超过三个月后，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。

服务器类证书补发操作成功时，新证书下载成功一个月后吊销老证书，其他类型的证书补发时立即吊销老证书。新证书有效期从补发成功之日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，订户申请更新证书的操作。以下情况订户需要申请证书换发：订户证书即将到期或已经过期。

在订户证书到期前的三个月内，CFCA 将通过适当的方式通知用户对证书进行换发操作。订户证书换发时，如证书还未过期，个人（普通、高级）证书、企业（普通、高级）证书，可通过证书登陆应用系统在线更新，应用系统通过原证书对订户信息进行鉴别。如订户证书已经过期，需要对订户身份进行重新验证。

服务器类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。

服务器类证书换发操作成功时，新证书下载成功一个月后吊销旧证书，其他类型的证书换发时立即吊销老证书。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）。

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，其要求与初次申请鉴别相同。

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 CP 的 4.8.3。

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

任何实体需要使用 CFCA 签发的证书时，均可向 CFCA 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 CFCA CPS 及相关的 CP 中所规定的相关责任与义务（CPS 及相关 CP 公布在 CFCA 网站上），并需要按照 CPS3.2.2 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 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，并将证书应用于合法的场景。

2、注册机构

CFCA 既是一个 CA，同时也承担了部分注册机构的职能，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。同时银行或者其他机构与 CFCA 合作成为 CFCA 注册机构，受理订户证书申请。注册机构对订户提供的证书申请信息参照 CPS3.2.2 的要求进行鉴别，CFCA 及 RA 对通过鉴别后的订户签发证书。CFCA 的注册机构应遵照 CFCA 制定的《注册机构运营管理办法》履行相关义务，同时应履行本 CP 中所规定的相关责任与义务。

4.2 证书申请处理

4.2.1 证书订户提交申请

订户需要申请 CFCA 证书时，可以通过 CFCA 官网下载证书申请表，或者向 CFCA 证书受理人员索取。通过 CFCA 注册机构申请 CFCA 数字证书时，可以在注册机构的网点或网站获得申请表。订户按照申请表的要求填写相关内容。机构申请证书时，提交的证书申请表需要加盖公章，证书申请人将申请请表连同相关证明材料通过传真、邮件或者快递的方式递交给 CFCA 受理人员。

4.2.2 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。CA 通过以下方法执行交叉审核与尽职调查：

4.1）依赖翻译的材料内容；

4.2）依赖拥有此语言能力的 RA 完成此步骤，CFCA 复核 RA 的检查结果，并且符合证书标准中的 CFCA 自我审核要求。

4.2.3 证书申请批准和拒绝

CFCA 按照 CPS3.2.2 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 将拒绝其申请，及时通知申请者并告知拒绝原因。

4.2.4 处理证书申请的时间

CFCA 将在合理的时间内完成证书申请处理。具体时间在证书相应 CPS 中规定。

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

在订户申请通过鉴别后，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；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，由 CA 或注册机构以安全的形式将证书或证书下载凭证码反馈给订户。

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，CFCA 有义务告知订户申请结果。CFCA 会以电话、电子邮件或其他方式对订户进行通告。

4.4 证书接受

4.4.1 构成接受证书的行为

订户填写证书申请表，同意本 CP 中的约定，提供真实、准确的身份信息经 CFCA 审核通过后，收到 CFCA 签发的证书后，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。

4.4.2 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的发布；订户没有要求发布的，CFCA 将不发布最终订户证书。

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 不对其他实体进行通告，依赖方可以在信息库上自行查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户的私钥和证书应用于规定的、批准的用途，订户在使用证书时必须遵守本 CP 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。预植证书及对应的私钥只有在该证书被绑定激活后才能使用。

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。

4.5.2 依赖方公钥和证书的使用

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。

4.6 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。

4.6.1 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。

4.6.2 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。

4.6.3 证书密钥更新请求的处理

同 3.3。

4.6.4 颁发更新证书时对订户的通告

同 4.3.2。

4.6.5 构成接受密钥更新证书的行为

同 4.4.1。

4.6.6 电子认证服务机构对密钥更新证书的发布

同 4.4.2。

4.6.7 电子认证服务机构对其他实体的通告

同 4.4.3。

4.7 证书更新

4.8 CFCA 不提供证书变更服务。证书吊销和挂起

4.8.1 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，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 CFCA CPS 或订户协议中约定的义务；或者订户证书不符合 CFCA CPS 的相关要求；

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。

在此基础上，代码签名证书额外情形如下：

1） 发现代码签名的内容中包含了有嫌疑的代码，包括但不限于病毒，木马，监听控件，恶意软件，以及其他任何不符合当地法律的代码。

4.8.2 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 4.8.1 所述的情形下主动吊销订户的证书。

4.8.3 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 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。

4.8.3.1 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 X 24 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 X 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。

4.8.3.2 被动吊销

当出现被动吊销的情形时，CFCA 将以书面形式通知订户，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。

4.8.4 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。

4.8.5 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。

4.8.6 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。

4.8.7 CRL 发布频率

CFCA 针对不同系统签发的证书区别更新 CRL 信息，具体时间要求见相关 CPS；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。

4.8.8 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。

4.8.9 在线证书状态查询的可用性

CFCA 提供 OCSP 查询服务，服务 7X24 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	**值或者值得限制**
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。sha1RSA、sha256RSA、sm3SM2 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。

4.8.10 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。

4.8.11 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。

4.8.12 证书挂起

CFCA目前暂不提供此业务。

4.9 证书状态服务

4.9.1 证书在线查询

证书状态可以通过 CFCA 提供的 OCSP 服务获得。

4.9.2 服务可用性

CFCA 提供 7X24 小时不间断证书状态查询服务。

4.10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。

4.11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，并将生产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。

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。

CFCA 灾难备份中心位于北京市亦庄经济开发区科创十四街 20 号院 2 号楼一层，灾备机房建设标准与主机房相同。

CFCA 预植证书生产中心位于北京市亦庄经济开发区科创十四街 20 号院 2 号楼二层。

5.1.2 物理访问

外来人员进入 CFCA 主运营楼内，需经过中国银联北京信息中心、CFCA 两道的审核，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。

灾备中心的访问控制与主运营中心的一样。

证书预植操作被放置在二层生产中心独立的区域中，具有物理三层保护。所有预制操作均有录像监控，CFCA 制定了严格的授权操作规范，确保预制生产过程中的安全。对于预植生产中心的物理访问控制，CFCA 通过门禁磁卡识别鉴别不同人员，并确定相应的权限。

5.2 证书生产管理规定

对于预植证书使用的智能密码钥匙（USBKey），CFCA 将检查存储介质的相关资质，确保预植证书使用的存储介质符合国家密码管理局的安全规定，并要求存储介质生产厂家声明符合国际标准 ISO 15782-1/FIPS 140-2/ANSI x9.66。

预植证书生产前 CFCA 将对存储介质进行检查，只有空白的介质才能进行生产。CFCA 按照制定好的规则，对智能密码钥匙的唯一标识、注册机构、订户信息进行管理。CFCA 将严格按照相关制度处理报废或不合格的存储介质，对已经下载过证书的存储介质需要报废或者返厂维修时，必须进行初始化处理，并根据相关流程吊销已经下载的证书，确保未经授权的证书使用。

CFCA 制订了安全生产管理办法，库房管理员凭借《送货清单》办理入库手续，并按照规定进行质量检查；成品出库时，库管员填写成品出库单，成品出库时加帖封条，以确保运输过程中的安全；库管员应每月对库房盘点一次，填写盘点记录，交生产主管和中心总经理。

所有访问及操作均有日志记录，预制服务器记录 USBKey 证书操作及与订户信息绑定的相关记录，并做到全程可审计。

其余的基础设施及相关管理控制描述参见 CPS 说明。

6 认证系统技术安全控制

本章节参见相关 CPS 内容

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 GM/T 0015-2012 数字证书格式规范，包含如下证书域。

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。对于根 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）。其值从公钥中或者生成唯一值的方法导出。该扩展项为非关键项。

7.1.2.3 密钥用法

本节参见 CPS7.1.2.3

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 RFC3280 之规定。针对 CA 证书，该项为关键扩展，针对订户证书，该扩展项为非关键项。

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。

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 RFC3280 及 RFC2459 之规定。

处于该域中的任何信息必须全部经过审核。

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

CFCA EV 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

理的时间内向用户提供查询结果。

8 认证机构审计和其它评估

此章节与 CPS 内容相同。

9 法律责任和其他业务条款

9.1 费用

此章节与 CPS 内容相同。

9.2 财务责任

此章节与 CPS 内容相同。

9.3 业务信息保密

同 CPS。

9.4 个人信息私密性

同 CPS。

9.5 知识产权

同 CPS。

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 及 CP 的内容，同时会根据业务的调整对 CPS 及 CP 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 CFCA 的 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、担保及义务

1. 同相应 CPS 中此相关部分。

9.6.3 订户的陈述与担保及义务

同相应 CPS 中此相关部分。

9.6.4 依赖方的陈述与担保及义务

同相应 CPS 中此相关部分。

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 CFCA CP 的规定。

9.7 免责条款

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和/或不真实和/或不完整的信息而获得 CFCA 签发的证书，订户在使用该证书时引起的纠纷，CFCA 不予承担任何法律责任。

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和/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 不承担赔偿和/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 不承担赔偿和/或补偿责任。

9.8 有限责任

同 CPS。

9.9 CFCA 承担的赔偿责任的限制

1. 除非有另外的规定或约定,对于非因本 CP 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 CP 的相关条款给予赔偿。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 和本 CP 实施的，则不视为 CFCA 具有任何过错，也不对订户或依赖方承担任何赔偿或补偿责任。
3. 无论本 CP 是否有相反或不同规定，就以下损失或损害，CFCA 不承担任何赔偿和/或补偿责任：
   a) 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、或失去或无法使用任何数据、设备或软件；
   b) 由上述损失相应生成或附带引起的损失或损害；

无论本 CP 是否有相反或不同规定，如果 CFCA 根据本 CP 或任何法律规定须承担赔偿和/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 生效及有效期限

本 CP 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 CP 提前终止。

9.10.2 终止

CFCA 有权终止本 CP（包括其修订版本），本 CP（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 CP 在 CFCA 官方网站公布之日起，上一版本的 CP 效力将自动终止。

9.10.3 效力的终止与保留

CP 中涉及的审计、保密信息、隐私保护、知识产权等方面，以及涉及赔偿的责任限制条款，在本 CP 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 CP 中提及的服务、规范、操作等信息，可以通过电话联系 CFCA，联系电话：010-83526220。

9.12 修订

CFCA 有权修订本 CP，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 CP1.5.4“CP 批准程序”相同。

9.12.2 通知机制和期限

CFCA 有权修订本 CP 中的任何术语、条款，事前无需通知任何一方，但在修订之后会及时公布在 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 CP 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 CP 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 CP 的相关内容。

9.13 争议处理

同 CPS。

9.14 管辖法律

CFCA CP 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 CP 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 CP 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 CP

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 CP 的完整性

本 CP 将替代所有以前的或同时期的、与相同主题相关的书面或口头解释。CPS、CP、订户协议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其他方。

9.16.3 分割性

本CP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

本章节参见相关CPS。

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 Protocal)
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。