中国金融认证中心

IdentityCA 体系电子认证业务规则

（Certification Practice Statement Of CFCA Identity CA System）

V1.2

2016 年 06 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		孙圣男	CFCA 安委会	2015 年 07 月
1.1	修订	修改 4 类模板相关内容	张翼	CFCA 安委会	2016 年 06 月

目　　录

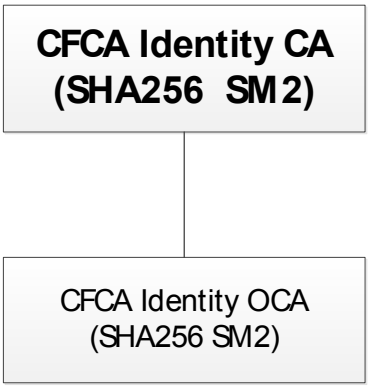
1 概括性描述

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,Certification 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 CFCA Identity CA 体系下的业务规则。CFCA 的 IdentityCA 体系下包括一个根 CA 和一个子 CA 系统，体系结构如下图所示。



CFCA 的所有 CA，包含子 CA 均由 CFCA 所有，由 CFCA 完全直接控制。

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》、《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)》，以及最新的《WebTrust 电子认证资格原则及规范》及 CA 的一般运作规范。

CFCA 遵循 WebTrust 相关要求，并通过外部审计师审计；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 Identity CA 体系电子认证业务规则(CFCA Identity CA System 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：2.16.156.112554.5

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。

CFCAIdentityCA 体系下的文档签名 CA 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

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。

1.3.6受益者及责任

CFCA Identity CA 签发的证书相关联的参与者均为受益者。

1.受益方

CFCA Identity CA 下的证书可以为下述机构提供信赖保证：

（1）所有提交订户协议的订户

（2）获取证书的申请者

（3）证书在生效期间的信赖方

2. CFCA Identity CA 体系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）证书中所有区域均经过验证。

（4）证书中关于证书拥有者信息的准确性

（5）证书状态 7*24 小时可查询

（6）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 Identity CA 仅用于签发下级 CA 证书，不签发最终订户证书。

1.4.1.1 CFCA 文档签名证书

该类证书适合对各类文档(包括但不限于 Adobe PDF 文档、Adobe Photoshop PSD 图形文件）等内容进行签名，用于验证文档签名者或发布者的身份信息，防止对文档内容进行无效修改。CFCA 文档签名证书由 CFCA Identity OCA 签发，密钥长度为 RSA-2048 或者 SM2-256。

1.4.2 受限的证书应用

CFCA Identity CA 下的文档签名证书根据其类型在功能上有所限制，只能用于对文档内容的签名者或发布者进行身份识别及对签发文件的防篡改。

该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。

1.4.3 禁止的证书应用

CFCA Identity CA 体系下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 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 业务部联系：

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。

1.5.4CPS 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。发布工作由业务部协调相关部门完成。

CPS 的网上发布遵照《CFCA 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，CFCA Identity OCA 的证书不公开发布，仅在数据库中发布；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；CFCA Identity OCA 签发的 CRL 信息将在 24 小时内更新；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。

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 Identity CA 体系下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。

对于文档签名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组织机构名称，作为标识订户的关键信息被认证。

CFCA 将对个人或企业提供的有效证件进行鉴别。

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 签发的文档签名证书所包含任何商标或者可能的其他机构信息，均是经过该机构正式授权使用，CFCA 承诺不使用任何未授权或者可能构成侵权的信息。

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。

由于文档签名证书的重要性，高级版本文档签名证书必须使用安全硬件存储（满足 FIPS140-2 标准）并且其文档签名证书的私钥应在硬件中产生，CFCA 可提供智能密码钥匙供订户选择。

3.2.2订户身份的鉴别

订户在申请 CFCA Identity CA 体系签发的证书前应指定并书面授权证书的申请代表（个人订户需为本人申请，不允许他人代理），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，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 CFCA Identity CA 体系证书时，应向 CFCA 提供真实有效的个人身份证明文件。对于机构中的个人申请者，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 CFCA Identity CA 体系证书前应授权本机构工作人员向 CFCA 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）应提供以下证明材料：

1、 证书申请表

2、 至少一种机构证明文件

3、 申请人的个人身份证件

4、 机构授予申请人的授权证明

5、 以上材料需要加盖公章

3.2.2.3 允许的证件类型

个人证件类型	机构证件类型
居民身份证	
护照	税务登记证
军人身份证件	组织机构代码证
股东代码证（不建议使用）	企业营业执照
社会保障卡	法人代码证
武装警察身份证件	事业单位法人证书
港澳居民往来内地通行证	社会团体登记证书
台湾居民来往大陆通行证	民办非企业登记证书
户口簿	外国（地区）企业常驻代表机构登记证
临时居民身份证	政府批文
警察（警官）证	其他
外国人永久居留证	

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 CFCA Identity CA 体系下的 Identity OCA 签发的文档签名证书的订户，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。

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）其他经 CFCA 认可的原因。

当订户需要补发证书时，应主动向 CFCA 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的，订户无需提交身份验证材料。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。

文档签名证书补发操作成功时，旧证书立即被吊销。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，需要对订户身份进行重新验证。

文档签名证书换发操作成功时，旧证书立即被吊销。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 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 4.8.3。

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 Identity CA 体系下签发的证书时，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 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。同时其他机构与 CFCA 合作作为 CFCA 注册机构，受理订户证书申请。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，CFCA 及 RA 对通过鉴别后的订户签发证书。CFCA 作为电子认证机构，应妥善保管证书订户申请信息。CFCA 的注册机构应在适当时间将证书订户的信息归档在 CFCA，同时应履行本 CPS 中所规定的相关责任与义务。

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

并通知申请机构或个人；

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。

3.如果 CFCA 委托其他机构担任 RA 角色，对于 RA 验证后的申请，CFCA 负责最终验证。

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 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 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，1-3 个工作日处理完成。

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 CFCA 下载证书后将证书发放给订户。

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 CPS 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（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。

4.5.2依赖方对公钥和证书的使用

依赖方信赖 CFCA Identity CA 体系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 证书变更

CFCA 不提供证书变更服务。

4.8 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；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；

6）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；

7）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；

8）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；

9)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；

10)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；

11）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；

12）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；

13）证书的重要参数被国际国内主流标准认为有重大风险时；

14）法律、行政法规规定的其他情形。

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*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*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。

4.8.4 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 将在 24 小时内更新 CFCA Identity CA 的 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。

4.8.8CRL 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 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。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

对于 CFCA Identity CA 体系下颁发的证书，CFCA 目前暂不提供此业务。

4.9 证书状态服务

4.9.1操作特征

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 7*24 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。

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。

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》、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

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

目前 CFCA 已对核心数据建立同城数据备份机制。

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 及其注册机构应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）以及相关证书标准；

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。

5.3.6 独立和约人的要求

CFCA 在雇用独立和约人时，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。

5.3.7 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七年。

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、内容审查评估文档。

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七年。

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。

CRL 的备份：文件每天通过自动 FTP 传输到备份服务器，并由人工检查备份是否成功。

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 Identity CA 体系下的证书，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 7X24 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或执行证书的吊销。

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 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的，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注册机构、订户、依赖方等有关各方，并依据与注册机构签署的合作协议向注册机构进行赔偿，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，作出妥善安排。

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的，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。

除订户以外的其他机构不应当存档订户私钥。

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得公钥证书。

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

订户的私钥是由订户自己生成时不会进行传送。

6.1.3 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。

6.1.4 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：

CFCAIdentityCA 体系下的 CA 签名密钥长度及算法如下：

CFCA Identity CA---RSA-4096/SHA-256、SM2-256/SM3

CFCA IdentityOCA—RSA-2048/SHA-1、SM2-256/SM3

订户密钥的长度为 RSA-2048 或者 SM2-256。

6.1.5 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。

6.1.6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。订户证书密钥的使用策略如下：

证书类型	算法	密钥长度	证书最长有效期（年）	密钥用法	增强密钥用法	策略 OID
个人高级文档签名证书	RSA-2048/SHA256 SM2/SM3	RSA-2048、 SM2-256	3	数字签名 不可否认	Email 保护 文档签名 Adobe 文档签名	2.16.156.112554.5.1
企业高级文档签名证书	RSA-2048/SHA256 SM2/SM3	RSA-2048、 SM2-256	3	数字签名 不可否认	Email 保护 文档签名 Adobe 文档签名	2.16.156.112554.5.1
个人普通文档签名证书	RSA-2048/SHA256 SM2/SM3	RSA-2048、 SM2-256	3	数字签名 不可否认	Email 保护 文档签名	2.16.156.112554.5.1
企业普通文档签名证书	RSA-2048/SHA256 SM2/SM3	RSA-2048、 SM2-256	3	数字签名 不可否认	Email 保护 文档签名	2.16.156.112554.5.1

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、DES、TRIPLE-DES、IDEA、RC2、RC4、RC5、SM1、SM4 等对称算法，支持 128 比特高强度加密；支持 MD2、MD5、SHA1、SDHI、SHA256、SM3 等 HASH 算法。

CFCA Identity CA 体系使用的加密机其公钥算法为 RSA-2048、RSA-4096、SM2-256，HASH 算法为 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

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、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，CFCA 的 Identity OCA 签发的证书有效期为 1-3 年。

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。对于加密类证书，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

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：

- 至少为 8 位数字
- 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。

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 全球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。

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、由防火墙对来自外部的访问信息进行过滤控制；

2、将功能独立的服务器放置在不同的网段；

3、多级防火墙划分不同网段，并采用了完善的访问控制技术；

4、通过验证和存取访问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/T0015-2012 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

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，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 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。

针对文档签名证书，此项为客户端身份验证、代码签名、安全电子邮件、

时间戳中的一种或者多种。

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。

7.1.3 算法对象标识符

CFCA Identity CA 体系签发的证书符合 RFC 3280 标准，采用 RSA-2048/SHA-256、RSA-4096/SHA-256 算法签名或者 SM2/SM3 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》。

Identity OCA 签发的证书 DN 可以包含以下部分：

1、 CN 部分：订户的法定真实名称。

2、 OU 部分：订户部门名称，OU 部分出现任何实体名称或者简称的，CFCA 将对该实体进行鉴别。

3、 O 部分：用于表示申请者的法定真实名称。

4、 C 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 3166-2013Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes）。

对于文档签名证书，必须包含以上各项，且 CN 部分必须是订户的真实名称，CFCA 建议订户在申请证书前，按照此要求生成证书签名请求文件（CSR，Certificate Signature Request），经 CFCA 审核通过后由 CFCA 据此签发证书，文档签名证书格式参见附录 B。

7.1.5 名称限制

CFCA Identity CA 体系下签发的证书，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，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；

订户证书策略对象标识符如下：

7.1.7 文档签名证书策略对象标识符：2.16.156.112554.5.1。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

CFCA 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、 接受外部审计机构的定期评估。

3、 接受第三方审计公司的 Webtrust 审计。

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；

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；

3、 定期评估：按照国际及国内相关标准要求接受外部审计机构的定期评估。

4、 CFCA 将每年进行 Webtrust 评估审计，且审计报告发布日期不得晚于审计期间结束后三个月。

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。

对于外部审计师的要求如下：

从业者必须是具有提供与信息科技、信息安全、PKI 和系统审计有关的第三方认证服务资质的独立会计师事务所；

从业者在提供服务时，其 Webtrust 审核服务资质必须是有效的；

从业者必须是 AICPA 或其他具有明确成员资质标准的协会成员。

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

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 接受外部审计机构的审计后，CFCA 会在公司网站上公布外部审计结果。

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 等均为 CFCA 的财产，CFCA 对其拥有知识产权。

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. 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。

3. 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。
4. 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。
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. 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。

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。

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。

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，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、 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

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。

9.9 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 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、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。

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 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，并将修订版本在官方网站上公布。

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，在采取任何解决途径之前，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。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 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。

9.17 其它条款

CFCA 承诺遵循《WebTrust 电子认证资格原则及规范》最新标准，若 CPS 与该指导准则不符，以准则为准。

10 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。

11 附录 B 证书格式

个人高级文档签名证书		
证书域	**域值**	
版本	V3	
序列号	包含20位的随机数	
签名算法	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
颁发者	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
有效期起止日		证书有效期时间
有效期终止日		证书有效期终止时间
主题	CN = 张三	必须有
	OU = 业务部	部门名称（非必须） 企业内个人需填写 非企业内个人应无此区域。
	O = 中金金融认证中心有限公司	企业内个人需填写，非企业内个人，本区域填写个人姓名
	L = 北京	个人身份ID上的 市，省，国家，身份证号码
	S = 北京	
	C = CN	
	SN = 123456789012345678	
公钥	RSA（2048）	1.2.840.10045.2.1（SM2算法标识符）
颁发机构访问信息	[1]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://gtc.cfca.com.cn/identityoca/indentityoca.cer	
颁发机构密钥标识符		
基本限制	Subject Type=End Entity	

	Path Length Constraint=None	
证书策略	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	http://www.cfca.com.cn/us/us-17.htm 为证书策略地址
CRL分发点	[1]CRL Distribution Point Distribution Point Name: Full Name: http://crl.cfca.com.cn/IdentityOCA/RSA/crl4.crl	文档签名证书的CRL分发点
密钥用法	数字签名 不可否认	
主题密钥标识符		
增强密钥用法	Email保护 文档签名 Adobe文档签名	

	企业高级文档签名证书	
证书域	**域值**	
版本	V3	
序列号	包含20位的随机数	
签名算法	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
颁发者	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
有效期起止日		证书有效期时间
有效期终止日		证书有效期终止时间
主题	CN = 法定真实名称	必须有
	OU = E-banking network	部门名称（非必须）
	O = China E-banking network	法定的组织机构名称，如使用非官方名称，应能正确反映其组织机构名称，并且不能引起歧义。如名称超过64字节，应使用缩写,但缩写不应引起对机构名称的歧异。
	L = Beijing	营业地址：包括国家、州或省、城市或乡镇、街道号码、邮编。 国家、州或省、城市或乡镇是必选项 街道号码和邮编是可选项。
	S = Beijing	
	C = CN	
	SN = 123456789012345678	证件号

公钥	RSA（2048）	1.2.840.10045.2.1（SM2算法标识符）
颁发机构访问信息	[1]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://gtc.cfca.com.cn/identityoca/indentityoca.cer	
颁发机构密钥标识符		
基本限制	Subject Type=End Entity Path Length Constraint=None	
证书策略	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	http://www.cfca.com.cn/us/us-12.htm 为EV证书策略地址
CRL分发点	[1]CRL Distribution Point Distribution Point Name: Full Name: http://crl.cfca.com.cn/IdentityOCA/RSA/crl4.crl	文档签名证书的CRL分发点
密钥用法	数字签名 不可否认	
主题密钥标识符		
增强密钥用法	Email保护 文档签名 Adobe文档签名	

个人普通文档签名证书		
证书域	**域值**	
版本	V3	
序列号	包含20位的随机数	
签名算法	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
颁发者	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
有效期起止日		证书有效期时间
有效期终止日		证书有效期终止时间
主题	CN = 张三	必须有
	OU = 业务部	部门名称（非必须） 企业内个人需填写 非企业内个人应无此区域。
	O = 中金金融认证中心有限公司	企业内个人需填写，非企业内个人，本区域填写个人姓名
	L = 北京	个人身份ID上的 市，省，国家，身份证号码
	S = 北京	
	C = CN	
	SN = 123456789012345678	
公钥	RSA（2048）	1.2.840.10045.2.1（SM2算法标识符）
颁发机构访问信息	[1]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://gtc.cfca.com.cn/identityoca/indentityoca.cer	
颁发机构密钥标识符		
基本限制	Subject Type=End Entity Path Length Constraint=None	
证书策略	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:	http://www.cfca.com.cn/us/us-17.htm 为证书策略地址

	http://www.cfca.com.cn/us/us-17.htm	
CRL分发点	[1]CRL Distribution Point Distribution Point Name: Full Name: http://crl.cfca.com.cn/IdentityOCA/RSA/crl4.crl	文档签名证书的CRL分发点
密钥用法	数字签名 不可否认	
主题密钥标识符		
增强密钥用法	Email保护 文档签名	

企业普通文档签名证书		
证书域	**域值**	
版本	V3	
序列号	包含20位的随机数	
签名算法	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
颁发者	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
有效期起止日		证书有效期时间
有效期终止日		证书有效期终止时间
主题	CN = 法定真实名称	必须有
	OU = E-banking network	部门名称（非必须）
	O = China E-banking network	法定的组织机构名称，如使用非官方名称，应能正确反映其组织机构名称，并且不能引起歧义。如名称超过64字节，应使用缩写,但缩写不应引起对机构名称的歧异。
	L = Beijing	营业地址：包括国家、州或省、城市或乡镇、街道号码、邮编。 国家、州或省、城市或乡镇是必选项 街道号码和邮编是可选项。
	S = Beijing	
	C = CN	
	SN = 123456789012345678	证件号
公钥	RSA（2048）	1.2.840.10045.2.1（SM2算法标识符）
颁发机构访问信息	[1]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access	

	Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://gtc.cfca.com.cn/identityoca/indentityoca.cer	
颁发机构密钥标识符		
基本限制	Subject Type=End Entity Path Length Constraint=None	
证书策略	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	http://www.cfca.com.cn/us/us-12.htm 为EV证书策略地址
CRL分发点	[1]CRL Distribution Point Distribution Point Name: Full Name: http://crl.cfca.com.cn/IdentityOCA/RSA/crl4.crl	文档签名证书的CRL分发点
密钥用法	数字签名 不可否认	
主题密钥标识符		
增强密钥用法	Email保护 文档签名	

12 附录 C 可靠数据源

数据源可靠性

CFCA在决定一个数据源为可靠数据源之前，将对以下进行评估：

1、数据提供时间，数据存在时间

2、数据源更新时间、更新周期

3、数据源的提供者和数据采集目的

4、此数据源是否可公开访问的情况

5、伪造或修改此数据源数据的难度

如果数据源提供者为CFCA本身，或者CFCA的所有者，或者CFCA的下级机构，则不能作为各种身份和资质认证的可靠数据源。

Certification Practice Statement
Of
CFCA Identity CA System

V1.2

June 2016

History of Revisions

Version	Action	Description	Modified By	Reviewed/ Approved By	Effective Date
1.0	**Draft, review and approve the first version.**		**Sun Shengnan**	**Security Committee**	**July 2015**
1.1	**Amend**	**Add temple and minor corrections**	**Zhang Yi**	**Security Committee**	**June 2016**

Contents

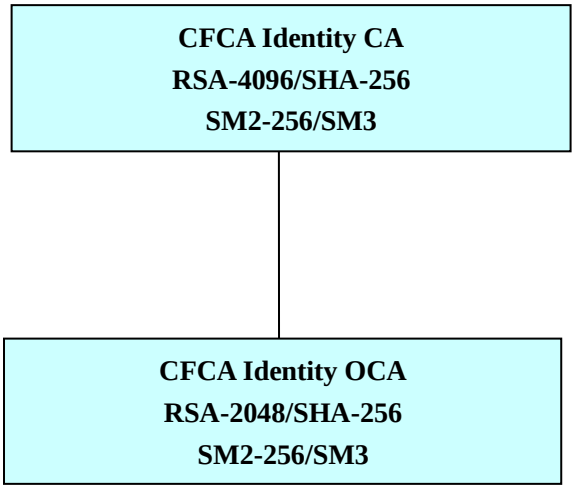
13 Introduction

13.1 Overview

Established on June 29, 2000, China Financial Certification Authority (CFCA) is a national authority of security authentication approved by the People's Bank of China and State Information Security Administration. It's a critical national infrastructure of financial information security and is one of the first certification service suppliers granted a certification service license after the release of the Electronic Signature Law of the People's Republic of China. Certification Practice Statement (CPS) is a detailed description and statement of the practices which a certificate authority (CA) applies in the whole life cycle of digital certificates (certificates for short) (e.g. issuance, revocation, and renew). It also describes the details of the business, technologies and legal responsibilities.

This CPS presents practices under the CFCA Identity CA System. The System constitutes of CFCA Identity Root CA and CFCA Identity OCA. The following figure shows the system structure.

CFCA Identity CA System



All the subordinate CAs of CFCA are owned and controlled by the CFCA directly.

This CPS conforms to IETF RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework); the《Electronic Signature Law of the People's Republic of China》 approved by the Tenth NPC and enforced on April 1, 2005; the 《Specification of Cryptography and Related Security Technology for Certificate Authentication System》and 《The Rule of Electronic Certification Services' Cryptography Administration》 released by the State Cryptography Administration; the 《Methods for the Administration of Electronic Certification Services》, 《Specification of Electronic Certification Practices (Trial Version)》 enacted by the Ministry of Industry and Information Technology of the People's Republic of China (MIIT); WebTrust 2.0 and other common practice norms of CA.

CFCA meets the requirements of WebTrust and has been audited by external auditors. CFCA holds a valid license of electronic certification services issued by MIIT, the competent department to CFCA.

13.2 Document Name and Indentification

This document is the Certification Practice Statement of CFCA Identity CA System (CFCA Identity CA System CPS).

CFCA has registered the corresponding Object Identity (OID) of this document in the National Registraion Center for OID. The OID of this document is 2.16.156.112554.5.

13.3 Electronic CertificationParticipants

Electronic certification participants appear in this document include: Certificate Authorities, Registration Authorities, Relying Parties, Subscribers and other participants. The followings are descriptions.

13.3.1 Certification Authorities

A Certificate Authority (CA) is responsible for certificate issuance, renew and revocation, key management, certificate status information service, release of Certificate Revocation List (CRL) and policy formulation, etc.

13.3.2 Registration Authorities

A Registraion Authority (RA) is responsible for the acceptance, approval and

management of subscriber certificates. It deals with the subscribers directly and deliveries certificate management information between the subscribers and the CA.

The RA function of CFCA Identity OCA system under the CFCA Identity CA System is performed by CFCA internally and no other authorities are entrusted to perform this responsibility.

13.3.3 Subscribers

Subscribers are the entities of certificates issued by CFCA.

It should be noted that, "Subscriber" and “Subject" are two different terms used in this CPS to distinguish between two different roles: "Subscriber", is the entity， individual and organization generally， which contracts with CFCA for the issuance of certificates and; “Subject", is the entity which the certificate is bound to. The Subscriber bears ultimate responsibility for the use of the certificate but the Subject is the individual that is authenticated when the certificate is presented.

13.3.4 Relying Parties

A relying party is an individual or organization that acts on reliance of the trust relations proved by the certificates.

13.3.5 Other Participants

Others beside CFCA, subscribers and relying parties are refered to as Other Participants.

13.3.6 Beneficiaries and Responsibilities

Participants related to the CFCA Identity CA System are all beneficiaries. The benefits are listed below.

1. Beneficiaries

Beneficiaries of certificates may be:

(1) The subscriber entering into the Subscriber Agreement for the certificate;

(2) The applicant who obtained the certificate;

(3) All relying parties that actually rely on such certificates during their validity periods.

2. Certificates provide the following warranties:

(1) Legal existence of certificate owner;

(2) Effective recognition to certificate owner's identity;

(3) All areas in certificate are verified;

(4) Accuracy of certificate owner information;

(5) 24 *7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired Certificates.

(6) CFCA will promptly revoke the Certificate upon the occurrence of any revocation event according to CPS.

13.4 Certificate Usage

13.4.1 CFCA Certificate Types and Appropriate Uses

CFCA Identity CA are only used for signing subordinate CA certificates

13.4.1.1 CFCA Document Signing Certificate

CFCA document signing certificate is applied to sign on documents including but not limited to Adobe PDF/ Adobe Photoshop PSD image file. The certificate usage is to verify signer's or publisher's identity information and prevent any invalid modification. CFCA Document Signing Certificate is issured by CFCA Identity OCA. Their key sizes are RSA-2048 or SM2-256.

13.4.2 Restricted Certificate Uses

The document signing certificate under CFCA Identity CA System is functionally restricted, it could only be used to identify signer or publisher and prevent any modification.

The intended key usages are described in the extensions of the subscriber certificates. However the effectiveness of the restriction depends on the applications. Therefore, if the participants fail to follow such restrictions, their interests are not protected by CFCA.

13.4.3 Prohibited Certificate Uses

Certificates under the CFCA Identity CA System cannot be used in applications

that violate any national or local law and regulation.

13.5 Policy Administration

13.5.1 Policy Document Administration Organization

The policy document administration organization of this document is the Risk & Compliance Department of CFCA. It sets up the "CPS Team" to compile or amend this CPS when needed. The General Manager can also set up a temporary CPS team and appoint a person to take charge of the drafting revision.

13.5.2 Contact

Any question on this CPS, please contact the Risk & Compliance Depatment:

Phone: +86 010-50955020

Fax: +86 010-63555032

Email: cps@cfca.com.cn

Address: NO.20-3, Pingyuanli, Caishikou South Street, Xicheng District, Beijing, China

13.5.3 Department Determining CPS Suitability for the Policy

The CPS team is responsible for compiling the draft or revision of the CPS, and submitting it to the Security Committee to review. The Security Committee reviews the CPS and determinies whether it is in conformity with relevant requirements. If

yes, the CPS will be submitted to the approval of the General Manager. Once approved, the CPS will be publicized, and will be reported to the competent department within 20 days following the publication.

13.5.4 CPS Approval Procedures

The CPS Team compiles a draft for discussion, which will be amended according to the opinions of the leaders and managers, resulting in a draft for review.

The CPS Team submits the draft for review to the Security Committee, and amends the draft afterwards according to the opinions of the Committee. The draft then goes to the Risk & Compliance Department, who determines the format and version number of the CPS. At this point, a final version is ready.

After being reviewed by the leaders and managers, the final version is submitted to the General Manager for approval. Once approved, it can be publicized in a form that aligns with the requirements of relevant authorities. The CPS is posted on CFCA website (http://www.cfca.com.cn). Printed CPSs are delivered to the clients and partners. The Risk & Compliance Department coordinates related parties in the publication.

The online publication of the CPS follows the 《CFCA Website Management Methods》. CPSs publicized in other forms should be consistent with the one posted on the website. The Risk & Compliance Department will report the CPS to the competent department within 20 days following the publication.

Periodic (usually annual) reviews are performed by the Risk & Compliance

Department to determine if revision is needed. The other departments can also raise a revision request depending on the demands of business. The CPS can also be modified according to the relevant standards that the CPS complies to.

If pervasive revision is needed, CFCA will adopt the same procedures of making the first version. If minor revision is needed, theRisk & Compliance Department will revise the CPS and submit it to the leaders and managers to review. The CPS, once approved by the General Manager, will be released on the corporate website. Every revised CPS will be reported by the Risk & Compliance Department within 20 days following the publication.

13.6 Definitions and Acronyms

Please refer to Appendix Definitions and Acronyms.

14 Publication and Repository Responsibilities

14.1 Repositories

CFCA provides information services to the subscribers and relying parties through its repositories, which includes but not limited to: Certificates, CRL, CPS, CP, Certificate Service Agreement, Technical Support Manual, CFCA website information and information irregularly released by CFCA.

14.2 Publication of Certification Information

CFCA releases CPS, CP and technical support information on its website.

Subscriber certificates can be obtained on the CFCA Certificate download platform. The certificates issued by CFCA Identity OCA can only be obtained through the repositories. Information of revoked Certificates is available on the CRL website, while the certificate status information (valid, revoked or suspended) is available through OCSP services.

14.3 Time or Frequency of Publication

CPS, CP and relevant documents will be released on the CFCA website within 15 days after they have gone through the procedures stated in Section 1.5.4. They are accessible 7*24 hours. CRL information issued by CFCA Identity OCA will be updated within 24 hours; the frequency of CRL publication can be tailored according to the demands of the subscribers. Manual real-time publication of CRL is also applicable if needed.

14.4 Access Controls on Repositories

Edit and write access is restricted to only authorized stuff. Read-only access is unrestricted.

15 Identification and Authentication

15.1 Naming

15.1.1 Type of Names

Subject name of certificates under CFCA Identity CA can be that of an individual, organization, department and also can be the combination of organization/ department and individual information. The naming follows the X.500 Distinguished Name Standard. Please refer to Section 7.1.4 for details.

15.1.2 Need for Names to be Meaningful

DN (Distinguished Name): A unique X.500 name put in the field of Subject Name on the Certificates to identify the subject. The content put in this field must reflect the authentic identity of the subject, be meaningful and in line with laws.

For document signing certificate, the DN must be the subscriber's personnel or organization/ department real name, this would be authenticated as key information.

CFCA would verify the ID provided.

15.1.3 Anonymity or Pseudonymity of Subscribers

Certificate Requests submitted in anonymity fail to meet the requirement of CFCA, and will not pass the verification. No certificate or service will be provided in this case.

Certificates using pseudonymity are invalid, and will be revoked once the

situation is confirmed.

15.1.4 Rules for Interpreting Various Name Forms

Please refer to Section 7.1.4 for the DN naming rules of CFCA.

15.1.5 Uniqueness of Names

CFCA ensures that the Subject Distinguished Name of the subscriber is unique within the trust domain of CFCA.

15.1.6 Recognition, Authentication, and Role of Trademarks

The subscribers shall warrant to CFCA and provide a statement to relying parties that: the information submitted in certificate application has not, in any form, infringed the Intellectual Property Rights of other, including the ownership of trade name, corporate name and etc. The Certificates issued by CFCA does not contain any trademarks or other information which may infringe other parties' rights.

15.2 Initial Identity Validation

15.2.1 Method to Prove Possession of Private Key

The method to prove possession of a private key by the subscriber is the digital signature in pkcs#10. Before CFCA issues a certificate, the system automatically uses the public key of the subscriber to validate the effectiveness of the signature of the private key, as well as the completeness of application information, and thus

determines whether the subscriber owns the private key.

For importance of document signing certificate, the private key of Advanced Identity certificates(with Adobe Document Signing EKU) shoule be generated in hardwares principally. CFCA could offer the subscriber this PKI-tokens.

15.2.2 Authentication of Subscriber Identity

Prior to applying for a certificate under the CFCA Identity CA System, the subscriber should appoint a representative and issue a written letter of authorization (the personnel subscriber must be him/herself and any agent is forbidden). The requester should provide valid ID proof, certificate application materials, acknowledge relevant stipulation and agree to bear corresponding responsibilities.

After received application from subscriber, CFCA will verify the ID proof and store well. This verifying process is:

Firstly, CFCA customer manager collect the application materials, the business department investigators will verify these materials, then RA operator type apply information into system and RA auditor will verify typed information and help subscriber to download the certificate.

15.2.2.1 Authentication of Individual Identity

When individuals apply for the CFCA Identity CA System certificates, they should provide CFCA authentic and effective proofs of their identities. For individual applicants in organizations, the application materials should bear official

seals or contain letters of authorization. CFCA will verify these organizations.

The following materials should be submitted:

1. Certificate application form;

2. Copies of ID;

3. Authorization of the organization (only applicable to the individuals in organizations).

The investigators verify the completeness and authenticity of the materials. Reliable data source would be used to validate the applicant's identity, address, country and etc.

15.2.2.2 Authentication of Corporate (Organization) Identity

Prior to applying for a certificate, organization subscribers should authorize a staff to propose the certificate request, and provide authentic and effective proof of organization identity.

Following materials should be submitted:

1. Certificate application form;

2. At least one type of organization legal existence proof;

3. The personal ID of the requester;

4. The authorization to the requester.

These materials should bear corporate seals.

15.2.2.3 Applicable IDs

Personal ID Types	Organizational ID Types
Resident Identity Card	Business Registration Certificate
Passport	Business License
Military ID	Certificate of Organizational Code
Foreigner's Permanent Residence Permit	Tax Registration Certificate
Social Security Card	Certificate of Legal Person Code
Armed Police ID	Certificate of Public Institution with Legal Person Status
Mainland Pass for Hong Kong and Macao Residents	Registration Certificate of Social Organization
Mainland Pass for Taiwan Residents	Registration Certificate of Private Non-Commercial Entity
Household Register(Not Advised)	Registration Certificate of a Foreign Resident Office
Temporary Resident ID	Government Approval
Police （Police Official）Certificate	Others
Resident Book	

15.2.3 Non-Verified Subscriber Information

CFCA verifies all the information submitted by the subscribers.

15.2.4 Validation of Authorization

When a person applies for a certificate on behalf of the organization subscriber, enough proofs should be obtained to verify that the person is authorized. CFCA is obliged to verify that authorization, and store the authorization information.

15.2.5 Criteria for Interoperation

CFCA performs identity verification of the applicants for certificates issued by CFCA Identity OCA. No other organization is delegated with this function.

15.3 Identification and Authentication for Renew Requests

Both “Reissuance” and “Renew” are commonly described as “Certificate Renewal”.

1. Certificate Reissuance

Certificate reissuance is the issuance of a new certificate to the subscriber during the validity period of the certificate.

The subscriber may request for certificate reissuance if:

(1) The subscriber certificate is lost or damaged. For example, the storage media of the certificate is damaged;

(2) The subscriber believes the security of the original certificate and key to be compromised (For example, the subscriber suspects the certificate had been stolen or the private key was attacked).

(3) Other reasons recognized by CFCA.

If a certificate reissuance is necessary, the subscriber should make a certificate reissuance request to CFCA. If this happens within three months following the issuance of the original certificate, no more identity verification materials. CFCA verify subscriber’s identity according to the information the subscriber provided in the initial application. CFCA will re-verify the identity of the subscriber if more than

three months after the first application. The process and requirements are the same as to the initial request.

Upon the issuance of the new certificate, the original certificate will be revoked immediately. The new certificate remains valid for the period between its issuance to the expiry date of the original certificate.

2. Certificate Renew

Certificate renew is the application for the issuance of a new certificate within the three months prior to the expiration of the existing certificate or after the expiration. The new certificate is valid between its issuance and the expiry date of the original certificate.

15.3.1 Identification and Authentication for Routine Renew

Same as Section 3.3;

15.3.2 Identification and Authentication for Renew After Revocation

CFCA treats the rekey request after revocation as a new application for certificate, and follows the provisions of Section 3.2.2.

15.4 Certificate Renewal

Certificate renewal is the issuance of a new certificate for an existing key pair. CFCA does not provide certificate renewal service. In other words, when a new certificate is issued, the key pairs must be re-generated

15.5 Identification and Authentication for Revocation Request

The identification and authentication for revocation request follows the procedures stated in Section 4.8.3.

16 Certificate Life Cycle Operational Requirements

16.1 Certificate Application

16.1.1 Certificate Application Entity

Any entity that needs to use the certificate under the CFCA Identity CA System can raise a certificate request.

16.1.2 Enrolment Process and Responsibilities

1. End-User Certificate Subscribers

End-user certificate subscribers refer to the entity applying for the certificates. All end-user certificate subscribers shall manifest assent to the CPS and CP (available on the CFCA website) that state the responsibilities and obligations of the subscribers. They shall also submit authentic and accurate application information following the provisions of Section 3.2.2. According to the 《Electronic Signature Law of the People's Republic of China》, if relying parties, CFCA or RA

designated by CFCA suffer loss because the application information submitted by the subscriber is unauthentic, incomplete or inaccurate, or because of other wrongful acts of the subscriber, the subscriber shall bear corresponding legal obligation and compensation responsibility. The subscribers are also obliged to keep the private keys safe.

2. CA and RA

CFCA is a CA, and performs some of the functions of RA. For example, the subscriber can submit a certificate request directly to CFCA, who will then response to the request and carry out identity verification. Meanwhile, CFCA has authorized some other organizations to accept certificate requests in the capacity of RA. RAs verify the identity of the subscribers according to the requirements stated in Section 3.2.2. CFCA and RA issue certificates to subscribers who have undergone the verification. As a CA, CFCA should properly retain subscribers' application documents, archive relevant information at CFCA within appropriate time limit, and practice the responsibilities and obligations stated in this CPS. No outside RA is allowed in the system of CFCA Identity CA.

16.2 Certificate Application Processing

16.2.1 Performing Identification and Authentication Functions

1. At least three trusted roles should be set in the processing of certification application: information collection, information authentication and certificate

issuance.

The former two roles can be performed by one person, while the last one must be separated from the former two.

2. For Certificates request, final review of the applicant information should be performed.

1) All the information and documents used to verify the Certificate Request should be reviewed to look for potential conflictive information or information that needs further authentication.

2) If the questions raised by the reviewer need to be further verified, CFCA must obtain more information and evidences from eligible information sources of the applicant, certificate signer and approver.

3) CFCA must ensure that the information and materials collected regarding the certificate request are adequate to ensure that the Certificate will not contain false information that CFCA is or should be aware of. Otherwise, CFCA will reject the certificate request.

4) If parts of or all of the materials used to verify the subscriber identity are not written in the official language of CFCA, it will appoint properly trained and experienced personnel with adequate judgement to complete the final cross-correlation and due diligence. This is done by:

4.1) Relying on translation of the materials;

4.2) Relying on RA with competency of the language in question. CFCA will review the authentication results of the RA and ensure that the self-assessment

requirements in the Certificate standards are met.

3. If CFCA delegates another organization to perform the functions of RA, CFCA is responsible for the final review of the certificate request verified by the RA.

16.2.2 Approval or Rejection of Certificate Applications

CFCA will approve a certificate request if all application materials and identity information have been verified in terms of Section 3.2.2. Otherwise, CFCA will reject the request and timely notice the applicant of the result and the reasons.

16.2.3 Time to Process Certificate Applications

CFCA will complete the processing of certificate requests within a reasonable time. If application materials are complete and in line with the requirements, the request will be processed within 1-3 working day.

16.3 Certificate Issuance

16.3.1 CA and RA Actions during Certificate Issuance

A certificate is created and issued following the approval of a certificate application by CFCA or following receipt of an RA's request to issue the certificate. CFCA creates and issues to a certificate applicant a certificate based on the information in a certificate application following approval of such certificate application.

16.3.2 Notifications to Subscriber by the CA and RA of Issuance of Certificate

CFCA is obliged to notice the subscriber of the results of the certificate request, whether it's approved or rejected. CFCA can do so via phone, email or other channels.

16.4 Certificate Acceptance

16.4.1 Conduct Constituting Certificate Acceptance

The following conducts constitute the subscriber's acceptance of the certificate: filling in the certificate request form, agreeing to the stipulations in this CPS, providing authentic and accurate identity information which is successfully verified by CFCA, and receiving the certificate issued by CFCA. After receiving the certificate, the subscriber should verify the information contained in the certificate before use. If no comments are raised within one working day, it is considered as the subscriber has accepted the certificate.

16.4.2 Publication of the Certificate by the CA

For end-user subscriber certificate, CFCA will publicize the certificate in due form according to the opinion of the subscriber. CFCA will not publicize the end-user subscriber certificate if the subscriber has not requested it to do so.

16.4.3 Notification of Certificate Issuance by the CA to Other Entities

CFCA does not notice the other entity about the certificates it issued. Relying parties may access the certificates in the repositories.

16.5 Key Pair and Certificate Usage

16.5.1 Subscriber Private Key and Certificate Usage

Private key and certificate use shall be consistent with the predetermined and approved usages (refer to Section 1.4.1). The subscribers shall follow this CPS in terms of certificate use, and shall protect their private keys to avoid unauthorized use.

3、 Private Key and Certificate Use by the Subscriber

The subscribers shall only use the private keys when they have accepted the corresponding certificates, shall only use the private keys and certificates in intended functions, and shall cease to use the certificates and private keys when the certificates expire or are revoked.

4、 Public Key and Certificate Use by Relying Parties

When the relying parties receive signature information, they shall:

- ✧ Obtain the corresponding certificates and certificate chains;
- ✧ Assess the validity of the certificates;
- ✧ Make sure that the certificates corresponding to the signatures are

trusted by the relying parties;

- ✧ Verify that one of the intended usages of the certificates is signing;
- ✧ Perform signature verification using the public keys on the certificates.

If relying parties fail to perform any of the above actions, they should reject to signatures.

When relying parties need to send encrypted information to the receiving parties, they should first obtain the encryption certificates of the receiving parties through proper channels, and use the public keys on the certificates to encrypt the information.

16.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance on the trust relationship proved by the certificates issued by the CFCA Identity CA System, relying parties shall:

1. Obtain and install the certificate chains corresponding to the certificates;

2. Verify that the certificates are valid. To do so, relying parties need to obtain the latest CRL released by the CFCA to ensure that the certificates have not been revoked. All the certificates appear in the certificate paths should be assess on their reliability. Validity period of the certificates shall be checked. Relying parties should also review other information that may affect the validity of the certificates.

3. Make sure that the content on the certificates is consistent with the content to be proved.

16.6 Certificate Rekey

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

16.6.1 Circumstances for Certificate Rekey

1. When the subscriber certificate is about to expire or has expired;

2. When the private key has been compromised;

3. When the subscriber knows or suspects that the certificate or private key has been compromised;

4. When the other situations that necessitate certificate rekey happens.

16.6.2 Who May Request Rekey

Subscribers holding certificates issued by CFCA may request certificate rekey.

16.6.3 Processing Certificate Rekey Requests

Same as Section 3.3;

16.6.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2;

16.6.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Same as Section 4.4.1;

16.6.6 Publication of the Rekeyed Certificate by the CA

Same as Section 4.4.2;

16.6.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3;

16.7 Certificate Modification

No certificate modification service is provided by CFCA.

16.8 Certificate Revocation and Suspension

16.8.1 Circumstances for Revocation

CFCA will revoke a certificate it has issued upon the occurrence of any of the following events:

1. The Subscriber requests in writing that the CFCA revoke the Certificate;

2. The Subscriber notifies the CFCA that the original certificate request was not authorized and does not retroactively grant authorization;

3.The CFCA obtains evidence that the Subscriber’s Private Key corresponding

to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the technical requirements;

4. The CFCA obtains evidence that the Certificate was misused;

5. The CFCA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;

6. The CFCA is made aware of any circumstance indicating that use of important information had been changed;

7. The CFCA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

8. The CFCA determines that any of the information appearing in the Certificate is inaccurate or misleading;

9. The CFCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

10. The CFCA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CFCA has made arrangements to continue maintaining the CRL/OCSP Repository;

11. The CFCA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

12. Revocation is required by the CFCA's Certificate Policy and/or Certification Practice Statement;

13. The technical content or format of the Certificate presents an unacceptable

risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CFCA within a given period of time);

14. Other situations stipulated in relevant laws and regulations.

16.8.2 Who Can Request Revocation

All subscribers holding CFCA certificates can request revocation.

At the same time, CFCA can take the initiative to revoke a subscriber certificate if an event described in Section 4.8.1 occurs.

16.8.3 Procedure for Revocation Request

Revocation includes initiative revocation and reactive revocation. Initiative revocation refers to one that put forward by the subscriber, reviewed and performed by CFCA. Reactive revocation refers to one that CFCA initiated to terminate trust services for the certificate, the usage of which has violated relevant regulations and agreements, or the subject of which has extinct.

4.8.3.1 Initiative Revocation

Before the subscriber applies for certificate, it should appoint a requester and provide a written letter of authorization, provide effective identity proofs, accept relevant provisions, and agree to bear corresponding responsibilities.

Upon receiving the application, CFCA should verify whether the certificate

implied is issued by CFCA, is valid, and that the reason for revocation is true. If these verifications come up with satisfactory results, CFCA will perform the revocation.

4.8.3.2 Reactive Revocation

When reactive revocation is planned, CFCA shall inform the subscriber through appropriate channels of the certificate in question, reason and time limit for revocation. CFCA shall only revoke the certificate when it ensures that the subscriber is informed and consents to the revocation.

16.8.4 Revocation Request Grace Period

For initiative revocation, the subscriber should make the request as soon as they identity such a need.

For reactive revocation, the subscriber can submit their arguments within three working days upon receiving the notice. CFCA will assess the arguments. If the arguments are justifiable, the revocation will be redrawing. If the subscriber doesn't response within three working days, or reply that they agree with the revocation, CFCA will go ahead with the revocation.

16.8.5 Time within Which CA Must Process the Revocation Request

For initiative revocation, it will be performed within 24 hours after the revocation request is reviewed.

For reactive revocation, the subscriber can submit their arguments within three working days upon receiving the notice. CFCA will assess the arguments. If the arguments are justifiable, the revocation will be redrawing. If the subscriber doesn't response within three working days, or reply that they agree with the revocation, CFCA will perform the revocation within 24 hours.

16.8.6 Revocation Checking Requirements for Relying Parties

Before any act of reliance, the relying parties shall verify that the certificate has not been revoked.

16.8.7 CRL Issuance Frequency

CFCA update ths CRL of CFCA Identity CA system. The frequency of CRL publication can be tailored according to the demands of the Subscribers. Manual real-time publication of CRL is also applicable if needed.

16.8.8 Maximum Latency for CRLs

The maximum latency of CRL publication is 24 hours.

16.8.9 Online Revocation/Status Checking Availability

OCSP service is viable for 7*24.

Whether to proffer an OCSP inquiry depends completely on the security demands of the relying parties. For applications that high demand on security and

completely rely on the certificates for identity authentication and authorization, the inquiry should be performed before any act of reliance.

The OCSP service of CFCA follows the RFC2560 standard.

When Clients ask for the OCSP service. CFCA will review the inquiry and focus on the following:

- ◆ Verify whether signature is compulsory;
- ◆ Verify the signature using CA Certificate;
- ◆ Verify whether the certificate is valid or expired;
- ◆ Verify whether the sponsor of the certificate is within the list of trusted certificates.

OCSP response should contain the following fields and content:

Field	Value/ Value Restriction
Status	Response status, including success, mal formed request, internal error, try later, sig required, and unauthorized. When the response status is success, following information should be shown.
Version	V1
Signature Algorithm	Algorithm used to sign the OCSP, including sha1RSA, sha256RSA and SM3 SM2.
Issuer	The entity that issue the OCSP. Information

	includes the data value of the issuer's public key and certificate DN.
Response Time	The time that the OCSP response generates.
Certificate Status List	A list that contains the status of the certificates. The status includes certificate identifier, certificate status, and certificate revocation.
Certificate Identifier	Including the data digest algorithm, data value of the certificate DN, the data value of the public key, and certificate serial value.
Certificate Status	Latest status of the certificate, including "good", "revoked" and "unknown".
Certificate Revocation	Revocation time and reason if the returned status is "revoked".

The extensions of OCSP are consistent with that stated in RFC2560 standard.

The OSCP is updated within 24 hours, and the maximum service response is less than 10 seconds. The maximum validity period for OCSP response does not exceed 7 days.

16.8.10 Other Forms of Revocation Advertisements Available

Information on certificate revocation is made available through CRL or OCSP services. CRL information can be obtained from the CRL Address extension.

16.8.11 Special Requirements regarding Key Compromise

If the subscriber discovers or has adequate reasons to believe that the security of the private key is threated, it should make a revocation request as soon as possible.

16.8.12 Certificate Suspension

Not applicable for the certificates under CFCA Identity CA System.

16.9 Certificate Status Services

16.9.1 Operational Characteristics

Certificate status is available through the OCSP service of CFCA.

16.9.2 Service Availability

Certificate status inquiry service is provided 7*24 by the CFCA.

16.10 End of Subscription

The subscription is need when：

1. The certificate has expired;

2. The certificate is revoked.

16.11 Key Generation, Backup and Recovery

To ensure the security of subscriber private keys, subscribers should

independently perform key pair generation in a secure environment and store the encrypted keys in secure media. The subscribers should backup the keys in a timely manner, and prevent the keys from loss The subscribers should apply for certificate rekey once key leakage is known or suspected.

When the subscribers delegate other trustworthy service suppliers to perform key generation for them, they shall require the suppliers to bear confidentiality responsibilities.

17 CA Facility, Management, and Operational Controls

17.1 Physical Controls

Physical and environmental securities of the systems constitute the foundation of the security of entire CFCA system. Physical and environmental controls include infrastructure management, monitoring of the environment, area access control, device security and disaster prevention, etc. The CFCA system is placed in a safe and robust building, and possesses independent software and hardware operation environment. The site selection has fully considered threats, such as water hazards, fire, earthquakes, electromagnetic disruption, radiation, criminal activities and industrial accidents.

17.1.1 Site Location and Construction

The computer room of the CFCA CA system is located in the No.2 Building (China Union Pay Beijing Information Centre), Zhongguancun Software Park, Haitian District, Beijing. Access to the computer room is subjected to a three-layer control. The electromagnetic shielding of the computer room meets the Level "C" requirements of the GJBz20219－94 Standard. The computer room is built to prevent and minimize the impacts of earthquakes, fire and water exposures. The computer room is equipped with temperature and humidity control devices, independent power supply, back-up power generator, access control and camera monitors. These security measures can ensure the continuity and reliability of the certification services.

17.1.2 Physical Access

Victors are subjected to the authentication of the China Union Pay Beijing Information Centre and CFCA and need to go through two layers of access control before they enter into the office area of CFCA. They are also accompanied by CFCA employees.

The access to the comprehensive computer room by operators is controlled by fingerprint authentication and access card authentication, and is monitored by cameras 7*24.

The access to the restricted computer room by operators is controlled by three layers of security controls: the dual person fingerprint authentication, access card

authentication, and dual person access card authentication. The entry and exit of the restricted computer room are recorded in the security system of the monitor room.

17.1.3 Power and Air Conditioning

Two sets of three UPSs supply the power for the computer room. As a result, the power supply for the systems can last for over 30 minutes even if one of the UPSs breakdown. A diesel generator has been put in place to strengthen the power supply stability of the systems. It can be used to power the UPS when the external power supply is cut off.

The computer room is equipped with multiple central air conditioners and ventilation devices to ensure that the temperature and humidity meet the national standards: GBJ19-87 Standards on Heating, Ventilation and Air-Conditioning Design, GB50174-93 Standards on Computer Room Design.

17.1.4 Water Exposures

CFCA employs professional technical measures to prevent and detect water leakage, and is able to minimize the impact of water leakage on the certification systems.

17.1.5 Fire Prevention and Protection

The CFCA computer room is built of fire-proof materials, and is equipped with central fire monitors and automatic gaseous media fire-extinguishing systems. It has undergone the checking of a national authority which proves that it can effectively

lower fire threat.

17.1.6 Media Storage

CFCA has formulated control policies for the management of the storage media of important data. The purpose is to prevent the leakage of important information, intentional compromise and damage.

17.1.7 Waste Disposal

Files (including paper files, disks and floppy disks, etc.) containing sensitive information should be shredded before disposal. Media must be rendered unreadable before disposal. Media containing confidential information should be terrorized in accordance with the guidance of the manufacturers. Cryptographic devices and other important key devices are disposed according to the management methods of cryptographic devices.

17.1.8 Off-Site Backup

CFCA has set up a mechanism for same-city off-site backup of core data.

17.2 Procedural Controls

17.2.1 Trusted Roles

Trusted roles of CFCA include:

Customer service personnel

Security personnel

Key and cryptographic device management personnel

Cryptographic device operation personnel

System administration personnel

Human resources management personnel

17.2.2 Number of Persons Required per Task

CFCA has established rigorous policies to ensure segregation of duties based on job responsibilities. Sensitive tasks, such as the access to and management of CA cryptographic hardware and associated key require three trusted persons.

At least two trusted persons are required to perform other operations, such as certificate issuance.

Policies and procedures are in place to ensure clear segregation of duties for its employees who can balance each other's power and monitor each other.

17.2.3 Identification and Authentication for Each Role

Before employing a trusted role, CFCA performs background check according to the stipulation in Section 5.3.2.

CFCA uses access card and fingerprint verifications to control physical access. It also determines the access rights of the personnel.

CFCA use digital certification and user name/key to identify and verify trusted roles. The system holds independent and complete record of all operations.

17.2.4 Roles Requiring Separation of Duties

Roles requiring segregation of duties include (but are not limited to):

Security personnel, system administration personnel, network management personnel, operators

Subscriber information collection personnel, subscriber identity and information verification personnel, RA information input personnel, RA certificate generation personnel.

17.3 Personnel Controls

CFCA and its RAs should follow the following requirements to manage staff members.

17.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become trusted roles must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities, as well as proof of any government clearance.

17.3.2 Background Check Procedures

Prior to commencement of employment of a trusted role, CFCA conducts background checks which include the following procedures:

(1) The applicants submit required materials.

They are required to submit valid proof of their working experience, highest educational degree obtained, qualifications and ID, etc.

(2) CFCA verifies the identities of the applicants.

CFCA HR department would authenticate the submitted materials through phone calls, letters, internet, face-to-face interviews, and reading of archives.

(3) The applicants undergo a three-month probation period.

CFCA would ask the applicants to take exams and scenarios tests, and would observe the performance of the applicants.

The results of the abovesaid exams, tests and observation should meet the requirement stipulated in Section 5.3.1.

(4) The new employees sign confidentially agreements.

CFCA requires the new employees to sign confidentially agreements.

(5) The employement is commenced.

17.3.3 Training Requirements

CFCA provides ite employees with trainings upon hire. The trainings are arranged according to the job responsibilities and roles of the employees and cover the following topics: PKI concpets, job responsibilities, internal policies and procedures, certification systems and softwares, relevant applications, operation systems, network, ISO9000 quality control mechanism and CPS, etc.

Employees handling Certificate related business must be trained according to the following:

1) Employees responsible for information and identity verification (verification experts) are trained on: basic PKI concepts, validation and verification policies and procedures, major threats during the verification (e.g. network phishing and other social engineering techniques) and EV certificate standards.

2) Training records should be kept and ensure that verification experts meet the technical demands of their jobs.

3) Different certificate issuance rights should be given to the verification experts according to their levels of technical skills. The grading standards of technicial skills should be aligned with the training content and performance evaluation criteria.

4) Before designation of certificate issuance rights, CFCA should make sure all the verification experts of different technical levels are competent of their jobs.

5) All verification experts should be required to pass the internal examination on identity verification of certificates.

17.3.4 Retraining Frequency and Requirements

CFCA provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

17.3.5 Job Rotation Frequency and Sequence

CFCA determines and arranges job rotation frequency and sequence according to the situations.

17.3.6 Sanctions for Unauthorized Actions

Employees who have taken unauthorized actions would be suspended from their jobs and subjected to disciplinary punishements according to relevant administration policies and procedures.

17.3.7 Independent Contractor Requirements

Personnel seeking to become the independent contractors of CFCA need to provide valid proof of ID, diplomas and qualifications, and sign confidentiality agreements with CFCA before the commencement of their employment.

17.3.8 Documentation Supplied to Personnel

CFCA provides its employees the requisite documents needed to perform their job responsibilities.

17.4 Audit Logging Procedures

17.4.1 Types of Events Recorded

Loggs include but are not limited to the following six types:

1. CA key life cycle management events, including key generation, backup, recovery, archival and destruction;

2. The indentity information of the Subscribers recorded in the RA system.

3. Certificate life cycle management events, including certificate requests, rekey and revocation;

4. System and network security records, including the record of the instruder detection system, logs generate during system daily operations, system problem handling forms, system change forms and etc;

5. Access control records;

6. System inspection records.

Log entries include the following elements: date and time of the entry; serial or sequence number of entry; identity of the entity making the journal entry;kind of entry.

17.4.2 Frequency of Processing Log

Type one logs listed above are collected and managed by the key administraters; type two and three are recorded by the database and undergo incremental backup daily, and weekly full backup; type four logs are automatically stored on backup devices daily; type five logs are audited quarterly; type six logs are checked daily.

17.4.3 Retention Period for Audit Log

Audit logs related to certificates shall be retained for at least ten years following the date the certificate expires or is revoked.

17.4.4 Protection of Audit Log

Management policies have been established, while logical and physical controls are in place to restrict operation on audit logs to authorized personnel. The audit logs are under strict protection which fends off any unauthorized manipulation.

17.4.5 Audit Log Backup Procedures

The backup of system, database and transaction logs follows CFCA's Log Management Method and Data Backup Management Methods.

17.4.6 Audit Collection System

Applications, network and operation systems automatically generate audit data and records.

17.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual and organization that caused the event.

17.4.8 Vulnerability Assessments

Using audit logs, vulnerability assessments are periodically on system, physical facilities, operation management, human resources management and other aspects. Actions are taken according to the assessment reports.

17.5 Records Archival

17.5.1 Types of Records Archived

Besides the records stated in Section 5.4.1, CFCA archives:

1. Application documents, identity verification documents, Agreements signed with Subscribers, Subscriber certificates and CRL;

2. CPS, CP and management policies;

3. Employee materials, including employee information, background check document, training, employment and resignation records;

4. Internal and external assessment documents.

17.5.2 Retention Period for Archive

CFCA would retain all archived documents for 7 years after the expiry of corresponding certificates.

If required by laws, CFCA shall extend the record retain periods.

The certificate revocation records on CRL and OCSP shall not be deleted during the valid period of the certificate.

17.5.3 Protection of Archive

CFCA has made policies to protect the archives.

For electronic archives, only authorized trusted persons are able to obtain access to them. The archives are protected against unauthorized viewing, modification, deletion, or other tampering during their retention period. To this end, CFCA uses reliable storage media and archive processing applications.

For paper archives, CFCA has made corresponding management methods, and has appointed dedicated libarian to managed the archives. Policie have been formulated to restrict the access to the paper arhives to authorized personnel.

17.5.4 Archive Backup Procedures

Database, operation systems, CRL records and logs are backuped.

Database backup: local and offsite backup, incremental and full backup.

Operation system backup: Backup performed at when the operation system is launched and when there are system changes.

CRL backup: Files are automatically transmitted from FTP to the backup server daily. Manual checks are performed to ensure successful transmission.

17.5.5 Requirements for Time-Stamping of Records

Archives shall contain time and date information. Time and date information shall be added to system generated records according to standards.

17.5.6 Archive Collection System

CFCA has put in place an automatic archive collection system.

17.5.7 Procedures to Obtain and Verify Archive Information

Only authorized trusted persons can have access to arhives. When archives are restored, they should be checked for completeness.

17.6 Key Changeover

CA key pairs are retired from service at the end of their respective accumulative maximum lifetime as defined in Section 6.3.2. Key changeover unfolds according to

the following procedures:

A superior CA should cease to issue new subordinate CA certificates no later than 60 days before the expiry date of its private key (Stop Issuance Date).

Generatie a new key pair, and issue a new superior CA certificate.

Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

17.7 Compromise and Disaster Recovery

17.7.1 Incident and Compromise Handling Procedures

CFCA has established a business continuity plan (BCP). It provides guidance to actions when CFCA is attacked or undergoes communication or network breakdown, computers and devices do not function normally, software is compromised, and when database is tampered.

The BCP is the responsibility of the CFCA Operation Security Committee (Security Committee for short), who's functions include direct and manage information security, approve and release BCPs, launch disaster recovery, etc. The Security Committee is made of leaders and the department heads, and is headed by the General Manager.

Business interruption is classified as emergencies and disaterous events. Emergencies are interruptions with major impacts on services to the client, but the service resumption is not affected by external factors and can be achieved with a short period of time. Disaterous events are interruptions caused by force majeure, such as natural disasters, contagious disease, and political outbreaks, etc.

CFCA has formulated corresponding emergency procedures for emergencies and disaterous events.

When emergency happens, the head of the Security Committee will convene a meeting of the members to evaluate the interruption. The operation department will perform the predetermined procedures. Meanwhile, the marketing department and technical support department will properly handle the affected clients. Afterward, CFCA will evaluate the effectiveness of the risk prevention measures and improve on them.

When a disaterous event happens, it will be handled according to the stipulations stated in Section 5.7.4.

As to normal breakdowns, it will be resolved within two hours; emergencies, 24 hours. As to disaterous events, if normal operations are not possible at the main site for disasters or other force majeure, certification services will be resumed within 48 hours at the backup site using backup data and devices.

Dedicated problem reporting and response capacity have been designated for SSL certificates:

1)CFCA provides subscribers, relying parties, application software vendors,

and other third parties with clear guidance to report complaints or suspected private key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports;

2)CFCA will begin investigation of all Certificate Problem Reports within twenty-four (24) business hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

(i) The nature of the alleged problem;

(ii) Number of Certificate Problem Reports received about a particular Certificate or website;

(iii) The identity of the complainants; and

(iv) Relevant legislation in force.

3) CFCA takes reasonable steps to provide continuous 24/7 ability to internally respond to any high priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an Certificate that is the subject of such a complaint.

17.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurance is classified according to the stipulations in Section 5.7.1 and is acted upon according to its classification.

17.7.3 Entity Private Key Compromise Procedures

CFCA has formulated an emergency plan on root private key leakage, which clearly stipulates the internal processing procedures, responsibilities of personnel and the procedures of external communication.

Once a root private key leakage is confirmed, CFCA will report to the competent department regarding the time, cause of the leakage and corrective actions.

Once a root private key leakage is confirmed, the subscribers and relying parties will be noticed immediately. All the certificates will be revoked. No new certificate will be signed with the private key.

17.7.4 Business Continuity Capabilities after a Disaster

CFCA has set up a data backup center and a corresponding BCP to ensure business conitinuity after a disaster.

If normal operations are not possible at the main site for disasters or other force majeure, certification services will be resumed within 48 hours at the backup site using backup data and devices.

17.8 CA or RA Termination

When CFCA plans to terminate certification services, it will report to the competent department sixty days in advance, and go through the procedures of cancelling certification qualification.

When CFCA plans to suspend or terminate certification services, it will take the

following actions ninety days in advance:

Notice the RA, subscribers, relying parties and other parties about continuation of the services;

Compensate the RA according to the cooperative agreement;

Compensate the subscribers and relying parties according to the service agreements;

Provide the business undertaker with the following and more information: certificate transaction materials, certificate repository, and latest certificate status information.

CFCA will report to the competent department about the suspension or teminaiton of its certification services sixty days in advance, and will make arrangement with the business undertaker.

If CFCA fails to reach an agreement with the other certification service organization about busiess transfer, it can request the competent department to arrange one.

If the competent department has regulations in this aspect, those regulations should be followed strictly.

18 Technical Security Controls

18.1 Key Pair Generation and Installation

18.1.1 Key Pair Generation

2、 CA Signing Key Generation

CA signing key generation is performed within the cryptographic device meeting the requirements of the state cryptography administration. The cryptographic device uses split ownership (secret share) and secret sharing mechanism to backup the key pairs, the fragments of which are held by shareholders (the custodians of the key fragments). The key generation ceremony is performed strictly according to the management methods of cryptographic devices and keys. Five persons are selected and authorized as the custodians, who use the passwords they input to protect the key fragments they are entrusted with. The key fragments are stored in smart IC cards. The CA key generation occurs in the area with the highest security level. Three out of the five custodians perform the ceremony which is monitored by a third party auditor. The CA key generation, storage and password cryptographic modules should meet the requirements of the state cryptography administration.

2. RA Key Generation

Generation of RA key pairs is performed under security controls. The RA certificates are issued by CFCA.

3. Subscriber Key Generation

Generation of subscriber key pairs is performed by the subscribers. They should ensure the reliability of the key pairs and is responsible for protecting the private key, and bears corresponding legal obligations.

Generation of key pairs of pre-generated certificates is performed by authorized personnel. Stringent policies have been made to ensure the security of key pairs when the certificates are delivered to the subscribers.

CFCA is obliged to provide guidance to the subscribers to perform key generation according to correct procedures. CFCA would reject a certificate application with weak keys. When needed, it can designate technical personnel to assist the subscribers in key generation.

Parties other than the subscriber should not archive subscriber's private key.

If CFCA or its RAs obtains the evidence that the private key is communicated to unauthorized parties, CFCA will revoke the public key certificate corresponding to the compromised private key according to relevant standards.

18.1.2 Private Key Delivery to Subscriber

When end-user subscriber key pairs are generated by the end-user subscriber, private key delivery to a subscriber is not applicable.

18.1.3 CA Public Key Delivery to Relying Parties

CA public key that can be used to verify the signature of CFCA is available in

the repository.

18.1.4 Key Sizes

As to key sizes, CFCA follows the explicit regulations and requirements made by the judicial authorities and the competent department.

Following are the current key sizes and algorithms of the CA signing keys under the CFCA Identity CA System:

CFCA Identity CA---RSA-4096/SHA-256、SM2-256/SM3；

CFCA Identity OCA—RSA-2048/SHA-256、SM2-256/SM3

The key size of subscriber keys is RSA-2048 or SM2-256.

18.1.5 Public Key Parameters Generation and Quality Checking

Public key parameters are generated by cryptographic devices approved by the state cryptography administration. The device should possess the credentials issued by the state cryptography administration. The devices should meet the requirements stated in the Specification of Cryptography and Related Security Technology for Certificate Authentication System released by the State Cryptography Administration and other relevant standards and requirements. An example is the quality inspection standard of public key parameters. The built-in protocols and algorithms of the devices should be of satisfactory security levels.

18.1.6 Key Usage Purposes

CA private key is used to sign its certificate, subordinate CA certificate, subscriber certificate and CRL. CA public key is used to verify the signature of private keys. The usages of subscriber keys are as follow:

Certificate Type	Algorithm	Key Size	Maximum Lifetime (Year)	Key Usage	Extended Key Usage	Policy OID
Personal Advanced Document Signing Certificate	RSA-2048/SHA256 SM2/SM3	RSA-2048、SM-2	3	Digital Sign Non-repudiation	Email Protection Document Signing Adobe Document Signing (1.2.840.113583.1.1.5)	**2.16.156.112554.5.1**
Organization Advanced Document Signing Certificate	RSA-2048/SHA256 SM2/SM3	RSA-2048、SM-2	3	Digital Sign Non-repudiation	Email Protection Document Signing Adobe Document Signing (1.2.840.113583.1.1.5)	**2.16.156.112554.5.1**
Personal Document Signing Certificate	RSA-2048/SHA256 SM2/SM3	RSA-2048、SM-2	3	Digital Sign Non-repudiation	Email Protection Document Signing	**2.16.156.112554.5.1**
Organization Document Signing Certificate	RSA-2048/SHA256 SM2/SM3	RSA-2048、SM-2	3	Digital Sign Non-repudiation	Email Protection Document Signing	**2.16.156.112554.5.1**

18.2 Private Key Protection and Cryptographic Module Engineering Controls

18.2.1 Cryptographic Module Standards and Controls

The cryptographic module (cryptographic device) used for key generation is

placed at the core area of CFCA. The module uses high speed host device with complete independent IPR, and is tested and approved by the state cryptography administration. Public key algorithms, like RSA, DSA, SM2, Diffe Hellman, can be used. Optional RSA sizes include 2048 and 4096 bits. Compatible symmetric algorithms include SDBI, DES, TRIPLE-DES, IDEA, RC2, RC4, RC5, SM1, SM4. Strong encryption of 128 bits is supported. Compatible HASH algorithms include MD2, MD5, SHA1, SDHI, SHA256 and SM3.

The public key algorithms for the cryptographic devices used in the CFCA Identity System include RSA-2048, RSA-4096, SM2-256; and HASH algorithms include SHA-256 and SM3. The devices have been granted credentials by the State Cryptography Administration.

CFCA has formulated management methods of cryptographic devices, which enable normative approval and management of the whole process of cyrpotgraphic device usage, including procurement, check and acceptance, installation in the computer room, initialization, activation, usage, backup, maintenance and destruction. The cryptographic devices are linked only to and directly with the application systems, and are sotraged in shielding computer rooms.

18.2.2 Private Key (n out of m) Multi-Person Control

CFCA CA keys are stored in the cryptographic devices, the keys of which are splitted into five fragments that stored in five IC cards. Each of the IC cards is hold by one authorized security personnel (shareholders), and stored in the safes in the

shielding computer rooms in the area of the highest security level. The activation of the CA private key requires the present of the three shareholders out of the five. This ensures the security of sensitive operations through technologies and policies.

18.2.3 Private Key Escrow

CA private keys are not escrowed.

18.2.4 Private Key Backup

The CA private keys are generated in cryptographic devices with dual backups. The cryptographic devices are stored in environment that prevents high temperature, high humidity and maganetic affects. The backup operation of the cryptographic devices requires the present of at least three (including three) operators.

The subscriber private keys are generated by the subscribers, who are recommended to backup the keys, and protect the backups by using passwords and other access controls. The purpose is to prevent unauthorized edit or leakage.

18.2.5 Private Key Archival

Upon expiration of the CFCA CA key pairs, they will be securely retained for a period of at least ten years using hardware cryptographic modules described in Section 6.2.1. These CA key pairs are prevented by the CFCA key management policies and procedures to be used in any production system. At the end of the archival periods, CFCA will destroy the key pairs according to the methods stated in Section 6.2.10..

18.2.6 Private Key Transfer Into or From a Cryptographic Module

CFCA generates CA key pairs on the hardware cryptographic modules. In addition, CFCA has eastablished backup cryptographic devices. Backup CA key pairs are transported off-line in encrypted form.

Subscriber private keys generated by hardware cannot be exported from the cryptographic modules. The subscriber private keys generated in the other ways can be exported in encrypted form.

18.2.7 Private Key Storage on Cryptographic Module

The private keys are stored in hardware cryptographic modules as encrypted key fragments as cipher-text.

18.2.8 Method of Activating Private Key

1. Activation of Subscriber Private Key

If the subscriber private key is generated and stored by software, it's stored in the software cryptographic module of the application and protected by passwords. When the application is started up, the software cryptographic module is loaded. Once the module has verified the passwords, the subscriber private key is activated.

When the subscriber private key is generated and stored by hardware cryptographic module, it's protected by the passwords (or pin code) of the hardware. When the cryptographic module is loaded, and verifies the passwords, the subscriber

private key is activated.

2. Activation of CA Private Key

CFCA uses hardware (cryptographic devices) to generate and store CA private key. The activation data is splitted according to the provisions stated in Section 6.2.2. Once the CA private key is activated, it will stay activated until the CA log off.

18.2.9 Method of Deactivating Private Key

The subscriber private key is deactivated upon application termination, system log off or power-off of the system.

The CA private key is deactivated upon power-off or re-initialization of the hardware cryptographic module.

18.2.10 Method of Destroying Private Key

Where required, CFCA will archive the CA private key according to the provisions stated in Section 6.2.5. The other CA private key backups will be destroyed in a secure manner. At the end of the archival period, the archived private key will be destroyed when at least three trusted personnel are presented.

The subscriber private key should be destructed after authorization. At the end of the life cycle of the private key, all corresponding key copies and fragments should be destroyed.

18.2.11 Cryptographic Module Rating

CFCA uses high speed host cryptographic devices with complete independent

IPR that have been certified and approved by the State Cryptography Administration.

18.3 Other Aspects of Key Pair Management

18.3.1 Public Key Archival

The archival of public keys follows the same requirements as that of certificates, including requirements on retention period, storage and security measurses. Please refer to Section 5.5 for the requirements.

18.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period of CA certificates is 30 years. The validity period of subscriber certificates issued by CFCA Identity CA is one to three years.

The operational period for key pairs is the same as that for associated certificates. However, the public keys of signing certificates may continue to be used for verification of signatures generated during the validity period of the certificates. This is so until the private keys are compromised, or the key pairs are at risk of decryption. An example of such risks is the decryption of encryption algorithm. For encryption certificates, the private key may continue to be used to ensure successful decryption of information encrypted during the validity period of the certificate.

18.4 Activation Data

18.4.1 Activation Data Generation and Installation

1. The generation of CA private key follows the requirements stated in Section 6.2.2.
2. For subscribers, the activation data is the passwords that protect the private keys. For subscribers of pre-generated certificates, the activation data contains the binding identity information. CFCA recommends the subscribers to select strong passwords to protect their private keys.
   - The passwords need to contain at least six characters.
   - Subscribers are recommended not to use information that can be easily guessed or decrypted, such as birthday or simple and repeated numbers.

18.4.2 Activation Data Protection

1. CFCA shareholders are required to safeguard their secret shares and sign an agreement acknowledging their shareholder responsibilities.

2. The RA is required to store their Administrator/RA private keys in encrypted form using password protection.

3. Subscribers are required to store their private keys in encrypted forms and are recommended to protect their private keys by using double-factor verification (e.g. hardware and strong password).

18.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

The cryptographic devices and related IC cards containing CA private keys are usually stored in the area with the highest security level, and are not allowed to be taken out of CFCA. If special circumstances necessitate the transmission, it should be witnessed by the security personnel and shareholders.

The passwords for private key activation transported through networks should be in encrypted forms to prevent loss.

6.4.3.2 Activation Data Destruction

CFCA destroys the activation data of CA private key by device initialization.

When the activation data of subscriber private key is no longer needed, it shall be destroyed. The subscriber should make sure that no other party can restore the data directly or indirectly through the residual information or the storage media.

18.5 Data Security Controls

18.5.1 A Security Plan made for Data Protection

1. CFCA adopts access controls and encryption signature to: ensure controls on CA; protect the confidentiality, completeness and serviceability of the data relating to certificate request, and the procedures relating to Certificate; restrict access, usage,

disclosure, edit and destruction of the above data to authorized and legitimate personnel; protect the above data from accidental loss, destruction and compromise; prevent the above data from forseeable threats and compromise.

2. CFCA takes actions to verify the condifentiality, completeness and serviceability of the “Certificate data”, and the key, software and procedures used in certificate issuance, repository maintenance and certificate revocation.

3. CFCA ensures that the data it maintained are in line with the security demands of relevant laws and regulations.

18.5.2 Periodic Risk Assessment of Data Security

1. CFCA carries out periodic risk rating to identify the forseeable internal and external threats that may subject “Certificate data” and “Certificate procedures” to unauthorized acess, use, disclosure, edit and destruction;

2. According to the sensitivity of the “Certificate data” and “Certificate procedures”, the risk rating assesses the possiblitiy of the identified threats and the harm they are expected to cause.

3. Annual reviews are carried out on the controls to determine the comfort they bring, including the policies, procedures, information systems, technologies and other relevant factors.

18.5.3 Security Plan

Based on the above risk assessments, a security plan is made to address the

making, implementing and maintaining security procedures and measures, and products designed for data security. Proper management and controls will be applied on identified risks according to the sensitivity of the “Certificate data” and “Certificate procedures”, as well as the complexitiy and scopes of the procedures.

The security plan should contain administrative and organizational structure, technical and physical controls adaptive to the scale, complexity, nature and scope of the “Certificate data” and “Certificate procedures”. The design of security controls should consider available technologies in the future and corresponding costs. The controls should be aligned with the potential harm caused by the absence of the controls, and the nature of the data to be protected.

18.6 Computer Security Controls

According to the regulations on system security management, CFCA requires the CA and RA to use trustworthy and secure operation systems to provide services. The corporate clienst are required to do the same.

18.6.1 Specific Computer Security Technical Requirements

CFCA practices information security management that is in line with relevant national regulations. Key security technologies and controls include: secure and trustworthy operation systems, stringent identity authentication and access control policies, multi-layer firewall, segregation of duties, internal controls, and business continuity plans, etc.

18.6.2 Computer Security Rating

The CFCA Global Trust System has undergone the security appraisal of the State Cryptographic Administration and other relevant departments.

18.7 Life Cycle Technical Controls

18.7.1 Root Key Controls

The root key generation ceremony should be witnessed by a qualified auditor, who then issue a report opiniong that CFCA, during its root key and certificate generation process:

1) Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the “Root Key Generation Script”) for the Root CA;

2) Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script;

3) Performed, during the root key generation process, all the procedures required by its Root Key Generation Script;

4) A video of the entire key generation ceremony will be recorded for auditing purposes.

These stipulations are also applicable for the controls of other keys.

18.7.2 System Development Controls

The developers of CFCA's systems meet relevant national security standards and possess manufacturing licenses of commercial cryptographic products. The development process also meets the requirements of the State Cryptographic Administration.

18.7.3 Security Management Controls

CFCA follows the norms made by the competent department in practicing information security management of its systems. Any system change must udergo stringent tests and reviews before implementation and use. At the same time, CFCA has set up strong management policies based on the ISO9000 quality management system standards. Core data is backuped daily according to a scheduled timetable by dedicated personnel. Data recovery is performed monthly by dedicated personnel to test the serviceability of the data.

18.7.4 Life Cycle Security Controls

The developers of CFCA's systems meet relevant national security standards and possess manufacturing licenses of commercial cryptographic products. The development process also meets the requirements of the State Cryptographic Administration. The source code of the systems is backuped at the State Cryptography Administraion to ensure system continuity.

18.8 Network Security Controls

CFCA employs the following measures to protect its networks from unauthorized access and hostile attacks:

1. Screen external access information through the router;

2. Place servers with independent functions at different network segments;

3. Set up multi-layer firewall, spilt the network, and implement robust access control technologies;

4. Protect data through verification and access controls;

5. Install intruder detection products in the network to protect the network through inspection and monitoring, so that CFCA can be alerted of and respond to intruders as soon as possible;

6. All terminals should be installed with anti-virus software, which is updated regularly;

7. Adopt redundancy design.

18.9 Time-Stamping

Certificates, CRLs, OCSP, and electronic certification system logs shall contain time and date information. Such time information should be consistent with the national standard time.

19 Certificate, CRL, and OCSP Profiles

19.1 Certificate Profile

The format of Certificates issued by CFCA conforms to the digital certificate standard GM/T 0015-2012 and contains the following fileds.Please refer to Appendix B for the fields contained in EV SSL certificates.

19.1.1 Version Number(s)

CFCA certificates are X.509 V3 certificates. This information is contained in the “Version” field of the certificates.

19.1.2 Certificate Extensions

Certificate extension is an extended sequence for one or more certificates, and is targeted for a specific type of certificates or specific users. The certificates issued by CFCA contain private extensions, which are set as non-critical extensions. The extensions of root CA certificate follow the RFC 5280 standard except four extensions: Basic Constraints, Key Usage, Certificate Policies and Extended Key Usage.

19.1.2.1 Authority Key Identifier

CFCA populates the Authority Key Identifier extension subscriber certificates and CA certificates. This extension is used to identify the corresponding public key

of the private key that signed the certificate, and thus distinguish the different keys used by the same CA. It's a non-critical extension.

19.1.2.2 Subject Key Identifier

The subscriber certificates are populated with the Subject Key Identifier, which marks the public key contained in the certificate, and is used to distinguish the different keys used by one subscriber (e.g. certificate rekey). Its value is exported from the public key or by generating a unique value. This is a non-critical extension.

19.1.2.3 Key Usage

The Key Usage extension defines the usages of the public key contained in the certificate, including certificate signing and CRL issuing. It's a critical extension for CA certificates, and a non-critical extension for subscriber certificates.

19.1.2.4 Basic Constraints

Basic Constraints is used to label whether a certificate subject is a CA, and determine the possible certification path length.The extension follows the RFC3280 standards. It's a critical extension for CA certificates, and a non-critical extension for subscriber certificates.

19.1.2.5 Extended Key Usage

This extension is used to indicate the one or more uses that are supplements or

substitutes of the uses stated in the Key Usage extension.

For document signing certificate, this could be one or combination of client authentication, codesigning, safe e-mail, time stamping.

19.1.2.6 CRL Distribution Points

Certificates include the CRL Distribution Points extension which can be used to locate and downlown a CRL. This extension MUST present and MUST NOT be marked Critical. (As in BR Appendix B)

19.1.2.7 Subject Alternative Names

The Subject Alternative Names extension contains one or more alternative names (can be in any name form) for the certificate subject. CA binds the subject with the public key contained in the certificate. The extension is populated in accordance with the RFC3280 and RFC 2459 standards.

All information contained in the filed must be verified by CFCA.

19.1.3 Algorithm Object Identifiers

The certificates of CFCA Identity CA System issued by CFCA are signed using SHA-256 RSA and SM2-SM3 algorithms, and comply with RFC 3280 standards.

The OID of SM2 algorithm is 1.2.840.10045.2.1, extra parameter is 1.2.156.10197.1.301.

19.1.4 Subject Name

This section describes the entity's situation corresponding to the subject field in the pulic key. CFCA follows the X.500 standards on distinguished name (DN). DN is used to describe the corresponding entity of the public key. CFCA makes sure that the DN is unique by establishing the CFCA Certificate DN Rule.All information contained in the certificate is verified by the CFCA.

The following 4 parts must be included in the CFCA Identity Certificate Issuance:

5、 CN：the legal name of subscriber.

6、 OU： If any entity name or its abbreviation appears in OU, CFCA would verify accordingly.

7、 O：Indicates legal name of applicants.

8、 C：Indicates the abbreviation of the country of the applicant, all in capital form. For example, Chinese subscriber would be indicated as C=CN.

The country, province and city names in the DN must be those listed in the standards released by authorities (e.g. ISO 3166-2013 Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes).

For the document signing certificate, the uppers should be included, CN part should be the real name of subscriber. Before the application, CFCA advises subscribers to generate CSR following this and CFCA will issue the certificate after authentication.

19.1.5 Name Constraints

Subscribers are not permitted to use anonymity or pseudonymity. The names must be distinguished names with clear meaning. When English names are used, they must be able to identify the entities.

19.1.6 Certificate Policy Object Identifier

When the Certificate Policies extension is used, the “certificate Policies: policy Identifier” field should be set to “anyPolicy”.

Certificate Policy OIDs of subscriber certificates are as follow:

Document Signing Certificate Policy OID = 2.16.156.112554.5.1

19.1.7 Usage of Policy Constraints Extension

Not applicable.

19.1.8 Policy Qualifiers Syntax and Semantics

Not applicable.

19.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

19.2 CRL

19.2.1 Version Number(s)

CFCA uses X.509 V2 CRL.

19.2.2 CRL and CRL Entry Extensions

CRLs conform to RFC 5280 and contain fields and contents specified below:

1. Version

The version of the CRL

2. Issuer

The distinguished name of the CA that issues the CRL.

3. This Update

Issue date of the CRL.

4. Next Update

Date by which the CRL will be issued.

5. Signature Algorithm

6. Revoke Certificates

Listing of revoked certificates, including the serial number of the revoked certificate and the revocation date.

19.3 OCSP Profile

CFCA Identity CA system provides Online Certificate Status Protocol services.

On a network working normally, CFCA ensures adequate resources to provide

the result for an inquiry on CRL and OCSP within a reasonable span of time.

20 Compliance Audit and Other Assessments

20.1 Frequency and Circumstances of Assessment

Following are the assessment performed:

4、 Assessments and inspections by the competent department based on the Electronic Signature Law of the People's Republic of China, the Methods for the Administration of Electronic Certification Services, the Methods for the Administration of Cipher Codes for Electronic Certification Services.

5、 Regular assessments carried out by external accounting organizations.

6、 Webtrust audits carried out by third party accounting firms.

Assessment frequency:

1、Annual assessment: the competent department carries out annual reviews on CFCA.

2、Pre-issuance assessment: Before launching a new system, it must be reviewed and signed off by the competent department.

3、Regular assessment: Regular assessments are carried out by external auditors according to relevant international or domestic standards and requirements.

4、Annual Webtrust assessments are carried out with the reports released within three months after period end.

20.2 Identity/Qualifications of Assessor

Compliance audits are performed on CFCA by an experience accounting firm that demonstrates profiency in IT operation management, public key infrastructure technology, relevant laws, regulations and standards.

The external auditors should:

Be with an independent accounting firm that is qualified to provide third party certification on information science and technology, information security, PKI and system audit;

Hold valid qualifications Webtrust assurance when the services are provided;

Be the members of AICPA or other association with clear qualification standards for its members.

20.3 Assessor's Relationship to Assessed Entity

The assessor should have no business relationship, financial interest or any other interest relation with CFCA.

20.4 Topics Covered by Assessment

Assessment topics should include but are not limited to the following:

1. Physical environment and controls
2. Key management operations
3. Basic controls
4. Certificate life cycle management

5. Certificate Practice Statement

20.5 Actions Taken as a Result of Deficiency

CFCA management should review the audit reports and take corrective actions on significant exceptions and omissions identified in the audits within 20 days after audit completion.

20.6 Communications of Results

The competent department will release the assessment results on CFCA after their inspections and reviews.

CFCA will release the results of external audits on its website.

Results of internal audits are communicated inside CFCA.

20.7 Other Assessment

CFCA controls the service quality through continual self-assessments, on a quarterly basis. Compliance to relevant policies and rules are assessed during the assessment period. During the period in which it issues Certificates, CFCA will control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the Certificates it has issued in the period beginning immediately after the last sample was taken. For EV certificates, compliance to EV certificates standard would be examined, and the sample selected would not be less than 3% of the certificates issued in the period.

21 .Other Business and Legal Matters

21.1 Fees

21.1.1 Certificate Issuance or Renewal Fees

At the point of certificate purchase, CFCA informs the subscribers of the fees for certificate issuance and renewal, charged according to the regulations of the marketing and management departments.

21.1.2 Certificate Access Fees

CFCA does not charge a fee for this service, but reserves the right to do so.

21.1.3 Revocation or Status Information Access Fees

CFCA does not charge a fee for this service, but reserves the right to do so.

21.1.4 Fees for Other Services

CFCA reserves the right to charge a fee on the other services it provides.

21.1.5 Refund Policy

A refund shall no be provided unless CFCA has breached the responsibilities and obligations under this CPS.

CFCA shall not be held responsible for loss or consequence caused by the incomplete, unauthentic or inaccurate certificate request information submitted by

the subscribers.

21.2 Financial Responsibility

21.2.1 Insurance Coverage

CFCA determines its insurance policies according to its business development and the business of domestic insurance companies. As for EV certificates, CFCA has undergone financial auditing provided by third party auditors, and has reserved insured amount for planned customers.

21.2.2 Other Assets

CFCA shall have sufficient financial resources to maintain its operation and perform their duties, and must be reasonably able to bear the responsibilities to subscribers and relying parties.

This clause is applicable for the subscribers.

21.2.3 Insurance or Warranty Coverage for End Entities

If according to this CPS or other laws and regulations, or judged by the judicial authorities, CFCA shall bear compensation and reimbursement obligations, CFCA would make compensation and reimbursement according to relevant laws and regulations, the ruling of the arbitral bodies and court decisions.

21.3 Confidentiality of Business Information

21.3.1 Scope of Confidential Information

Information that shall be kept confidential and private includes but is not limited to the following:

1. Information contained in the agreements signed between CFCA and the subscribers, and relevant materials, which has not been publicized. Unless demanded by laws, regulations, governments and law enforcement agencies, CFCA shall not publicized or reveal any confidential information other than the certificate information.
2. Private keys held by the subscribers. The subscribers are responsible to custody the private keys according to the stipulations in this CPS. CFCA will not be held responsible for the private key leakage caused by the subscribers.

21.3.2 Information Not Within the Scope of Confidential Information

Following is information not considered confidential:

1. Information on the certificates issued by the CFCA, and on the CRL.
2. Data and information known by the receiving party piror to their release by the supplying party.
3. Information that becomes publicly known through no wrongful act of the

receiving party, upon or after the supplying party reveals the data or information.

4. Data and information that are publicly known.
5. Data and information released to the receiving party by rightful third party.
6. Other information that can be obtained from open and public channels.

21.3.3 Responsibility to Protect Confidential Information

Stringent management policies, procedures and technical instruments have been employed by CFCA to protect confidential information, including but is not limited to business confidential information and client information. No employee of CFCA has not been trained on handling confidential information.

21.4 Privacy of Personal Information

21.4.1 Privacy Plan

CFCA respects all the subscribers and their privacy. The privacy plan is in conformity with valid laws and regulations. The acceptance of certification service indicates the subscribers' acceptance of the privacy plan.

21.4.2 Information Treated as Private

CFCA treats all information about subscribers that is not publicly available in the content of a certificate, and certificate status information as private. The

information will be used only by CFCA. Private information shall not be revealed without the consent of the subscribers, or demands of judicial or public authorities raised pursuant to legitimate procedures.

21.4.3 Information Not Deemed Private

Content on the certificates and certificate status information are not deemed private.

21.4.4 Responsibility to Protect Private Information

CFCA, RAs, subscribers, relying parties and other organizations and individuals are obliged to protect private information according to the stipulations in this CPS. CFCA is entitled to disclose private information to specific parties in response to the demands raised by judicial and public authorities pursuant to legitimate procedures, and shall not be held responsible for the disclosure.

21.4.5 Notice and Consent to Use Private Information

3、 The subscribers consent that CFCA is entitled to use all information within its business practices according to the privacy policies stipulated in this CPS, and is not obliged to inform the subscribers.

4、 The subscribers consent that, CFCA may disclose private information when demanded to do so by judicial and public authorities, and is not obliged to inform the subscribers.

21.4.6 Disclosure Pursuant to Judicial or Administrative Process

Other than in the following occasions, CFCA shall not disclose confidential information to any other individual or third party organization:

4、 Legitimate applications have been proposed by judicial, administrative departments, and other departments authorized by laws and regulations, according to laws, regulations, decisions, orders and etc.

5、 Written warrants have been provided by the subscribers.

6、 Other occasions stipulated in this CPS.

21.4.7 Other Information Disclosure Circumstances

CFCA, subscribers, CA and other organizations and individuals are obliged to protect private information according to the stipulations in this CPS. CFCA is entitled to disclose private information to specific parties in response to the demands raised by judicial and public authorities pursuant to legitimate procedures, or when written warrants have been provided by the subscribers, and shall not be held responsible for the disclosure.

21.5 Intellectual Property rights

CFCA owns and retains all intellectual property rights, including the copyrights and patent application rights on the certificates, software and data it provides. The CPS, CP, technical support manual, certificates and CRL are the exclusive properties

of CFCA, who owns their intellectual property rights.

21.6 Representations and Warranties

21.6.1 CA Representations and Warranties

CFCA provides certification services using information security infrasture approved by relevant administrative authorities.

CFCA's operation is in conformity with the Electronic Signature Law of the People's Republic of China and other laws and regulations. It accepts the governance of the competent department. CFCA is legally responsible for the certificates it issues.

CFCA's operation is in conformity with this CPS, which is amended as the business changes.

According to the requirements of the Managing Rules for Electronic Certification, CFCA is responsible for auditing the delegated parties' compliance with the CPS and relevant requirements on an annual basis. CFCA retains the rights and responsibilities to keep and use subscribers' information.

21.6.2 RA Representations and Warranties

As registration authority of CFCA, It's responsible for verifying the identity of the applicants, determining whether to accept or reject the certificate requests, inputting subscriber information into the RA systems, and deliver the requests infomation to the CA systems vir secure channel.

As the RA, CFCA represents and warrants that:

1、 It obides by its strategies and administrative regulations, verifies the certificate request materials for the completeness and accuracy of the information they contain. It's entitled to accept or reject the certificate requests.

2、 RAs should design an appropriate business process that the pre-generated certificates are kept properly before issuing to the subscriber and that the certificate will not be used before it is bound to an entity.

3、 If CFCA rejects a certificate request, it's obliged to inform the corresponding subscriber. If CFCA accepts a certificate request, it's obliged to inform the corresponding subscriber, and assist the subscriber in obtaining the certificate.

4、 Certificate requests are handled in a reasonable period of time. Requests are handled within 1-3 working days provided the application materials are complete and meet the requirements.

5、 RAs properly retains the information about the subscribers and the certificates and transfers the documents to CFCA for archival. RAs should cooperate with CFCA according to relevant agreements for compliance audit.

6、 RAs should make subscribers aware of the meaning, function, scope and method of using the third-party digital certificates as well as key management, result and response measures for key compromise, and legal responsibilities.

7、 CFCA informs the subscribers to read its CPS and other regulations. A certificate will only be issued to a subscriber who fully understand and consent the

stipulations of the CPS.

21.6.3 Subscriber Representations and Warranties

Subscribers represent and warrant that:

They have read and understood the entire CPS and relevant regulations, and consented to be bound by this CPS.

They honor the principles of honesty and credibility; that accurate, complete and authentic information and materials are submitted in certificate application; that CFCA will be informed timely of any change in these information and materials.Loss caused by unauthentic information submitted intentionally or accidentially, or failure of the subscribers to inform CFCA when the information changes are borne by the subscribers.

They use the key pairs in trustworthy systems to prevent the keys from being attacked, leaked or misused. They properly protect the private keys and passwords of the certificates issued by CFCA, and do not trust the other parties with the keys. If, accidentally or intentionally, the private keys or passwords are known, stolen or falsely used by others, the subscribers bear the corresponding responsibilities.

The subscribers or legal representatives request for certificate revocation at the original RA as soon as possible, and observe the procedures described in this CPS, if the private keys or passwords of the certificates have been leaked or loss, or the subscribers wish to terminate the usage of the certificates, or the subjects stop to exist,

The subscribers use the certificates in functions that are legitimate and consistent with this CPS.

The subscribers bear the responsibilities for using the certificates.

Subscribers will indemnify CFCA for:

1) Falsehood/incompleteness/misrepresentation of facts by the subscribers on the certificate application. Failure to give timely notice to CFCA when the facts change.

2) Failure to inform all relevant parties and revoke the certificates when the private keys are known to be or may have been lost.

3) Other wrongful acts or failure to honor the agreements.

Subscribers are obliged to pay certification service fee timely. Please consult the Marketing Department for charge standards.

CFCA is entitled to inform the subscribers to change their certificates as the technologies progress. Subscribers shall submit certificate rekey request witin specified periods when they receive the notices. CFCA is not liable if the subscribers do not change their certificates timely.

21.6.4 Relying Party Representations and Warranties

Relying parties represent and warrant that:

1. They obtain and install the certificate chains corresponding to the certificates;

2. They verify that the certificates are valid before any act of reliance. To do so,

relying parties need to obtain the latest CRL released by the CFCA to ensure that the certificates have not been revoked. All the certificates appear in the certificate pathes should be assessed on their reliability. Validity period of the certificates shall be checked. Relying parties shall also review other information that may affect the validity of the certificates.

3. They make sure that the content on the certificates is consistent with the content to be proved.

4. They obtain sufficient knowledge of this CPS and the usage of certificates, and use the certificates within the scope stipulated by this CPS.

5. They accept the limitation of CFCA's liability described in this CPS.

21.6.5 Representations and Warranties of Other Participants

The unidentified participants should observe the stipulations in this CPS.

21.7 Disclaimers of Warranties

1. CFCA is not liable for a dispute occur in the usage of the certificate, if the corresponding subscriber has intentionally not, or failed to provide accurate/authentic/complete information on the certificate application.

2. CFCA is not liable for loss caused by certificate failure, transaction interruption or other incidents, which are caused by device and network breakdown that has happened through no wrongful act of CFCA.

3. CFCA is not liable if the certificate has been used in functions not intended or prohibited by CFCA.

4. CFCA is not liable if parts of or all of the certification services of CFCA have been suspended or terminated becaused of force majeure.

5. CFCA is not liable for using services other than CFCA's service of digital signature verification in online transactions.

6. CFCA is not liable for the breach of agreement caused by a patner's ultra vires behavior or other mistakes.

21.8 Limitations of Liability

If according to this CPS or other laws and regulations, or judged by the judicial authorities, CFCA shall bear compensation and reimbursement obligations, CFCA would make compensation and reimbursement according to relevant laws and regulations, the ruling of the arbitral bodies and court decisions.

21.9 Indemnities

9.9.1 Unless otherwise stipulated or agreed, CFCA is not liable for any loss not caused by the certification service stated in this CPS.

9.9.2 CFCA shall compensate, according to this CPS, the subscriber or relying party, who suffers loss caused by the certification service provided by CFCA. However, CFCA shall not be deemed faultful if it can prove that it has provided services according to the Electronic Signature Law of the People's

Republic of China, the Methods for the Administration of Electronic Certification Services and the CPS filed to the competent department, and shall not be required to bear any compensation and reimbursement responsibility towards the subscriber or relying party.

9.9.3 CFCA is not liable for the following, whether it has infringed this CPS or not:

(1) Any indirect loss, direct or indirect loss of profit or income, compromise of reputation or goodwill, loss of business opportunities or chances, loss of projects, loss or failure to use data, device or software;

(2) Any loss or damage caused directly or indirectly by the above loss.

9.9.4 If according to this CPS or other laws and regulations, or judged by the judicial authorities, CFCA shall bear compensation and reimbursement obligations, CFCA would make compensation and reimbursement according to relevant laws and regulations, the ruling of the arbitral bodies and court decisions.This is so whether or not this CPS contains contradictive or different regulations.

21.10 Term and Termination

21.10.1 Term

This CPS becomes effective upon publication on CFCA's official website (http://www.cfca.com.cn). Unless otherwise announced by CFCA, the previous CPS is terminated.

21.10.2 Termination

CFCA is entitled to terminate this CPS (including the revisions). This CPS (including the revisions) shall be terminated upon the 30th day after CFCA posts a termination statement on its official website.

The CPS shall remain in force until a new version is posted on CFCA's official website.

21.10.3 Effect of Termination and Survival

Upon termination of this CPS, its provisions on auditing, confidential information, privacy protection, intellectual property rights, and the limitation of liability remain valid.

21.11 Individual Notices and Communications with Participants

To learn more about the service, norms and operations mentioned in this CPS, please contact CFCA at 010-83526220.

21.12 Amendments

CFCA is entitled to amend this CPS and will release the revised version on its official website.

21.12.1 Procedure for Amendment

The procedure for amendment is the same as Section 1.5.4 “CPS Approval Procedure”.

21.12.2 Notification Mechanism and Period

CFCA reserves the right to amend any term and provision contained in this CPS without notice. But the revised CPS will be posted on the CFCA website in a timely manner. If the subscriber doesn’t request for certificate revocation within seven days after the publication, it will be deemed to have accept the amendment.

21.12.3 Circumstances under Which CPS Must be Amended

CFCA shall amend this CPS if: the rules, procedures and relevant technologies stated in this CPS can no longer meet the demands of CFCA’s certification business; the governing laws and regulations of this CPS have changed.

21.13 Dispute Resolution Provisions

If a subscriber or relying party discover or suspect that leakage/tampering of online transaction information has been caused by the certification service of CFCA, it shall submit a dispute resolution request to CFCA and notice all related parties within three months.

Dispute resolution procedures:

1. Notice of dispute

When a dispute occurs, the subscriber should notice CFCA before any

corrective action is taken.

2. Resolution of dispute

If the dispute is not resolved within ten days following the initial notice, CFCA will set up an external panel of three external certificate experts. The panel will collect relevant facts to assist the resolution of the dispute. Panel opinion should be formed within ten days following the foundation of the panel (unless the parties concerned agree to extend this period) and delivered to the parties. Panel opinion is not binding on the parties concerned. The signing of the panel opinion by the subscriber of relying party constitutes acceptance of the opinion. As a result, the dispute will be solved according to the panel opinion. The panel opinion will then be reviewed as the agreement between CFCA and the subscriber on the resolution of the dispute and is legally binding. Thus, if the subscriber wants to pull out of the agreement, and submit the dispute to arbitration, it will be bound by the panel opinion to do so.

3. Formal Resolution of Dispute

If the panel fails to put forward effective opinion in the time agreed upon, or the opinion doesn't enable the two parties to agree on the resolution, the parties shall submit the dispute to the Beijing Arbitration Commission.

4. Time Limit for Claim

If the subscriber or relying party plans to make a claim on CFCA, it shall do so within two years after it becomes aware or should be aware of the loss. After this period, the claim is invalid.

21.14 Governing Law

Governing laws of the CFCA CPS include the Contract Law of the People's Republic of China, the Electronic Signature Law of the People's Republic of China and other relevant laws and regulations. If any clause in this CPS is in conflict with

the above laws and regulation, or is unenforceable, CFCA shall amend the clause in question till this situation is resolved.

21.15 Compliance with Applicable Law

All the policies of CFCA are in compliance with applicable laws, regulations and requirements of the People's Republic of China and the state information security authorties. In the event that a clause or provision of this CPS is held to be illegal, unenforceable or invalid by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid. CFCA will amend that clause or provision until it's legitimate and enforceable.

21.16 Miscellaneous Provisions

21.16.1 Entire Agreement

The CPS renders invalid the written or verbal explanations on the same topics during the previous or same periods. The CPS, CP, Subscriber Agreement, Relying Party Agreement and their supplement agreements constitute the Entire Agreement for all participants.

21.16.2 Assignment

The CA, subscribers and relying parties are not allowed to assign their rights or obligations in any form.

21.16.3 Severability

In the event that a clause or provision of this CPS is held to be illegal, unenforceable or invalid by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid. CFCA will amend that clause or provision until it's legitimate and enforceable.

21.16.4 Enforcement

Not applicable.

21.16.5 Force Majeure

Force majeure refers to an objective situation that is unforeseeable, unavoidable and irresistible. Examples of force majeure include: war, terrorist attack, strike, natural disaster, contagious disease, and malfunction of internet or other infrastructure. But all pariticipants are obliged to set up disaster recovery and business continuity plan.

21.17 Other Provisions

CFCA warrants observing the latest verion ofWebtrust Certification Authority Audit Principles and Rules. Should there be any inconsistency between the CPS and the above ducument , the latter shall prevail.

22 Appendix A Definitions and Acronyms

Table of Acronyms

Term	Definition
ANSI	The American National Standards Institute
CA	Certificate Authority
RA	Registration Authority
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocal
CP	Certificate Policy
CPS	Certificate Practice Statement
CSR	Certificate Signature Request
IETF	The Internet Engineering Task Force

Definitions

Term	Definition
Certificate Authority	An authority trusted by the subscribers to generate, issue and manage public keys and certificates; and generate private keys for the subscribers in some occasions.
Registration Authority	An entity responsible for handling the application, approval and management of certificates.
Certificate	An electronic file that contains the indentity and public key of the Subscriber, and is digitally signed by the CA.
Certificate Revocation List	A list issued periodically under stringent requirement, digitally signed by the CA, and indicates the certificates that are no longer trusted by the CA.
Online Certificate Status Protocal	A protocol issued by IETF providing information of certificate status.
Certificate Policy	A certificate policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate the applicability of a type of certificate for the B-to-B trading of goods or services within a given price range.

Certification Practice Statement	A certification practice statement is a statement of practices that the CA employs in certificate issuance, management, revocation and renewal (or renewing the private key of the certificate).
Subscriber	。 An entity applying for the certificate.
Relying Party	A relying party is an individual or organization that acts on reliance of the trust relations proved by the certificate.
Private Key	An encryption key generated through arithmetical operation (kept by the holder) to create digital signature, and/or to decrypt electronic records or files that were encrypted with the corresponding public key (to ensure information confidenetiality).
Public Key	An encryption key generated through arithmetical operation made public by the holder, and that is used to verify the digital signature created with the corresponding private key, and/or to encrypt messages or files so that they can be decrypted only with the holder's corresponding private key.
Distinguished Name	A distinguished name is contained in the Subject name field on the certificate and is the unique indentifier of the subject. The distinguished name should follow the X.500 standard, reflect the authentic identity of the subject, is of practical meaning, and in conformity with laws.

23 Appendix B Certificate Format

Format of Personal Advanced Document Signing Certificate		
Field	**Value**	
Version	V3	
Serial Number	Contains 20 non-serial digits	
Algorithm	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
Issuer	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
Valid from		Certificate Valid from
Valid to		Certificate Expiry date
Subject	CN = zhang san	Legal Name on ID
	OU = business department	Name of the department(Alternative)
	O = China E-banking network	Personal name or organization legal name if the person can prove that he/she is an employee of the organization
	L = Beijing	City, State, and Country Info
	S = Beijing	
	C = CN	
	SERIALNUMBER = 110000006499259	ID number
Public Key	RSA（2048）	1.2.840.10045.2.1（SM2 Algorithm identifier）
Authority Information Access	[1]Authority Info Access Access Method=on-line certificate protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtc.cfca.com.cn/identityoca/identityoca.cer	
Authority Key Identifier		

Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	2.16.156.112554.5.1 is the identifier of document signing certificate issued by CFCA, http://www.cfca.com.cn/us/us-17.htm is the Document Signing Certificate Policy address
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/IdentityOCA/RSA/crl1.crl	CRL distribution point of Document Signing Certificate
Key Usage	Digital Signature, Non-Repudiation	
Subject Alternative names	Other names: Main name=Legal Name	Persistent identification name
Subject Key Identifier		
Enhanced Key Usage	Email Protection Document Signing Adobe Document Signing (1.2.840.113583.1.1.5)	

Format of organization Advanced Document Signing Certificate		
Field	**Value**	
Version	V3	
Serial Number	Contains 20 non-serial digits	
Algorithm	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
Issuer	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
Valid from		Certificate Valid from
Valid to		Certificate Expiry date
Subject	CN = Legal Name	Compulsory and contains only domain name
	OU = E-banking network	Name of the department(Alternative)
	O = China E-banking network	Legal organisation name. If unofficial name is used, it should correctly reflect the organisation name and no misleading interpretation are caused. If the name exceeds 64 bytes, abbreviation

		should be used, but no misleading interpretation should be caused.
	L = Beijing S = Beijing C = CN	Business Address: including Country, State or Province, City or Village, Street, Postcode. Country, State or Province,City or village are compulsory, and street and postcode are optional.
	SERIALNUMBER = 110000006499259	ID number (eg. Orgniasation code, Business certificate code, tax registration code). Or date of establishment if no registered ID number provided.
Public Key	RSA（2048）	1.2.840.10045.2.1（SM2 Algorithm identifier）
Authority Information Access	[1]Authority Info Access Access Method=on-line certificate protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtc.cfca.com.cn/identityoca/indentityoca.cer	
Authority Key Identifier		
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	2.16.156.112554.5.2 is the identifier of document signing certificate issued by CFCA, http://www.cfca.com.cn/us/us-17.htm is the Document Signing Certificate Policy address
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/IdentityOCA/RSA/crl1.crl	CRL distribution point of Document Signing Certificate
Key Usage	Digital Signature, Non-Repudiation	

Subject Alternative names	Other names: Main name=Legal Name	Persistent identification name
Subject Key Identifier		
Enhanced Key Usage	Email Protection Document Signing Adobe Document Signing (1.2.840.113583.1.1.5)	

Format of Personal Document Signing Certificate		
Field	**Value**	
Version	V3	
Serial Number	Contains 20 non-serial digits	
Algorithm	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
Issuer	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
Valid from		Certificate Valid from
Valid to		Certificate Expiry date
Subject	CN = zhang san	Legal Name on ID
	OU = business department	Name of the department(Alternative)
	O = China E-banking network	Personal name or organization legal name if the person can prove that he/she is an employee of the organization
	L = Beijing	City, State, and Country Info
	S = Beijing	
	C = CN	
	SERIALNUMBER = 110000006499259	ID number
Public Key	RSA（2048）	1.2.840.10045.2.1（SM2 Algorithm identifier）
Authority Information Access	[1]Authority Info Access Access Method=on-line certificate protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtc.cfca.com.cn/identityoca/indenti	

	tyoca.cer	
Authority Key Identifier		
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	2.16.156.112554.5.3 is the identifier of document signing certificate issued by CFCA, http://www.cfca.com.cn/us/us-17.htm is the Document Signing Certificate Policy address
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/IdentityOCA/RSA/crl1.crl	CRL distribution point of Document Signing Certificate
Key Usage	Digital Signature, Non-Repudiation	
Subject Alternative names	Other names: Main name=Legal Name	Persistent identification name
Subject Key Identifier		
Enhanced Key Usage	Email Protection Document Signing	

Format of organization Document Signing Certificate		
Field	**Value**	
Version	V3	
Serial Number	Contains 20 non-serial digits	
Algorithm	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
Issuer	CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	CN = CFCA Identity SM2 OCA O = China Financial Certification Authority C = CN
Valid from		Certificate Valid from
Valid to		Certificate Expiry date
Subject	CN = Legal Name	Compulsory and contains only domain name
	OU = E-banking network	Name of the department(Alternative)
	O = China E-banking network	Legal organisation name. If unofficial name is used, it should correctly reflect the organisation

		name and no misleading interpretation are caused. If the name exceeds 64 bytes, abbreviation should be used, but no misleading interpretation should be caused.
	L = Beijing	Business Address: including Country, State or Province, City or Village, Street, Postcode. Country, State or Province,City or village are compulsory, and street and postcode are optional.
	S = Beijing	
	C = CN	
	SERIALNUMBER = 110000006499259	ID number (eg. Orgniasation code, Business certificate code, tax registration code). Or date of establishment if no registered ID number provided.
Public Key	RSA（2048）	1.2.840.10045.2.1（SM2 Algorithm identifier）
Authority Information Access	[1]Authority Info Access Access Method=on-line certificate protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtc.cfca.com.cn/identityoca/identityoca.cer	
Authority Key Identifier		
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-17.htm	2.16.156.112554.5.4 is the identifier of document signing certificate issued by CFCA, http://www.cfca.com.cn/us/us-17.htm is the Document Signing Certificate Policy address
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/IdentityOCA/RSA/	CRL distribution point of Document Signing Certificate

	crl1.crl	
Key Usage	Digital Signature, Non-Repudiation	
Subject Alternative names	Other names: Main name=Legal Name	Persistent identification name
Subject Key Identifier		
Enhanced Key Usage	Email Protection Document Signing	

24 Appendix C

Data Source Accuracy (comply with Baseline Requirement)

Prior to using any data source as a Reliable Data Source, the CFCA will evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CFCA will consider the following during its evaluation:

1. The age of the information provided;

2. The frequency of updates to the information source;

3. The data provider and purpose of the data collection;

4. The public accessibility of the data availability;

5. The relative difficulty in falsifying or altering the data.