中国金融认证中心

电子政务电子认证业务规则

V2.0

2012 年 08 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 CA 之一。

电子认证业务规则（CPS，Certification Practice Statement）是关于认证机构（CA,Certification Authority）在全部数字证书（以下简称证书）服务生命周期（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。此电子认证业务规则专门用于 CFCA 在开展电子政务电子认证活动时的服务内容要求、服务质量保障、具体的服务操作规范及相关法律责任等方面的声明。

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》,《电子政务电子认证服务业务规则》、《电子政务数字证书应用接口规范》及其它的相关规范。

1.2 策略文档管理机构

《电子政务电子认证服务业务规则》由 CFCA 业务部进行维护与管理，其修订与批准程序严格按照 1.4 中所述的流程进行。

CFCA 业务部将会定期对存在的业务风险进行评估，并及时对《电子政务电子认证服务业务规则》进行修订。

该《电子政务电子认证服务业务规则》一经修订后，将会在 10 个工作日内报国家密码管理局进行备案，并在 CFCA 网站上公开发布。

1.3 联系方式

本《电子政务电子认证服务业务规则》的发布地址：CFCA 网站（http://www.cfca.com.cn）.

如对本 CPS 有任何疑问，请联系：

部门：业务部

电话：010-83526220

传真：010-63555032

邮件：zhaoyu@cfca.com.cn

地址：中国北京宣武区菜市口南大街平原里 20-3

1.4 CPS 批准程序

在制订及修订本 CPS 时，业务部牵头组成“电子政务 CPS 编写组”，市场部、运行部、技术支持部、开发部派人参加；总经理也可以根据需要临时设立“电子政务 CPS 编写组”，并指定编写组负责人。

经“电子政务 CPS 编写组”共同讨论后，形成讨论稿（或 CPS 修订内容），并征求公司领导和各部门负责人意见，经讨论、修改达成一致意见后形成送审稿。

“电子政务 CPS 编写组”负责将 CPS 送审稿提交公司法律顾问审阅。在取得法律顾问的意见书后，“CPS 编写组”将经法律顾问审阅过的 CPS 送审稿连同法律顾问的意见书提交业务部，由业务部确定 CPS 文本格式和版本号，形成定稿；定稿经业务部分管领导审阅后，报总经理审批。总经理审批同意后，形成最终的定稿。

总经理审批同意后，业务部负责在 10 个工作日内报国家密码管理局进行备案；备案完成后，方可对外发布。

发布形式应符合行业主管部门等相关主管部门要求，包括但不限于网站公布和向客户或合作对象书面提交。发布工作由业务部协调相关部门完成。网上发布遵照 CFCA 内部制度《网站管理办法》执行。

自本电子政务 CPS 发布之日起，所有以各种形式对外提供的电子政务 CPS 必须与网站公布的版本保持一致。

1.5 术语和定义

● 数字证书 digital certificate

包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

● 数字签名 digital signature

附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来

源及其完整性，防止被人(例如接收者)进行伪造。

● 鉴别 identification

辨别认定证书申请者提交材料真伪的过程。

● 实体鉴别 entity authentication

确认一个实体所声称的身份。

● 验证 authentication

对证书申请材料和申请者之间的关联性进行确定的活动。

● 密码算法 crypto-algorithm / cryptographic algorithm

描述密码处理过程的一组运算规则或规程。

● 电子认证服务 electronic certification service

电子认证服务是指为电子签名相关各方提供真实性、可靠性验证的活动。

● 电子认证服务机构 electronic certification service provider

提供电子认证服务的机构。

● 证书注册机构 certificate registration authority

接收公钥证书的申请、注销和查验申请材料的机构。本规范所述注册机构包括证书注册中心及受理点。

● 证书撤销列表 certificate revocation list

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除了普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

● 证书持有者 certificate holder

有效证书的主体对应的实体。

● 证书申请者 subscriber

从电子认证服务机构接收证书的实体。在电子签名应用中，证书申请者即为电子签名人。

● 证书依赖方 certification relying party

依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是也可以不是一个证书持有者。

1.6 符号和缩略语

PKI	公钥基础设施(public key infrastructure)
CA	认证机构(certification authority)
RA	注册机构(registration authority)
CRL	证书撤销列表(certificate revocation list)
LDAP	轻量目录访问协议(lightweight directory access protocol)
USB KEY	采用 USB 接口的证书存储介质(universal serial bus key)

2 数字证书服务

2.1 服务内容

CFCA 面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供证书申请、证书签发、证书更新、证书撤销以及密钥生成、备份和恢复等服务。

2.2 数字证书类型

CFCA 面向电子政务领域提供以下类型的数字证书：

● 机构证书

用以代表政务机关和参与电子政务业务的企事业单位的身份，如：某部委、某局或参加政府招投标业务的投标企业等。

● 个人证书

为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的证书，用以代表个体的身份，如：某局局长、某局职员或参加纳税申报的个人等。

● 设备证书

为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，包括：服务器身份证书、SSL 服务器证书、VPN 设备证书等。

● 其他类型证书

为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如代码签名证书等。

以上各类数字证书格式符合国家密码管理局颁布的《电子政务数字证书格式规范》的要求，在标识实体名称时，保证实体身份的唯一性，且名称类型支持 X.500 标准协议格式。

2.3 身份标识与鉴别

2.3.1 命名

电子政务数字证书命名符合国家密码管理局颁布的《电子政务数字证书格

式规范》要求，不允许使用匿名或假名。

2.3.2 证书申请人的身份确认

● **证明拥有私钥的方法**

证书持有者的签名私钥（private key）在证书持有者客户端生成，证书持有者发出的数据包中包含用签名私钥进行的数字签名，其他各方（包括 CFCA）用对应的公钥可以验证这个签名。

证书持有者被视作其签名私钥的唯一持有者。CFCA 要求证书持有者妥善保管自己的签名私钥。

在证书持有者委托 CA 机构或其他可信服务商代替证书持有者生成密钥对的情况下，也可认为证书持有者是其签名私钥的唯一持有者。

● **组织机构身份的鉴别**

组织机构在申请证书前应指定并授权证书的申请代表，由证书申请代表向 CFCA 或 CFCA 授权的注册机构（RA）提交组织机构的有效身份证件及其复印件（包括：企业营业执照、组织机构代码证、税务登记证及其它有效证明文件）、证书申请表、组织机构授予证书申请代表的授权书以及证书申请代表的有效身份证件。

CFCA 或其授权的注册机构将复核并验证申请相关的申请材料，并进行批准申请或拒绝申请的操作。批准申请的，将保留相关证明材料的复印件，与申请表一并存档保存。

● **个人身份的鉴别**

个人证书申请者持个人有效身份证件，包括：身份证、军官证、士兵证、

护照、武装警察身份证、户口本、港澳居民往来内地通行证、台湾居民往来内地通行证等（以上可任择其一），填写证书申请表，并接受证书申请的有关条款，向 CFCA 或其授权的注册机构提出证书申请。

当由他人代表本人申请时，须同时出示代理人及被代理人的有效身份证件，以及被代理人签发给代理人的授权书。

当证书申请人为政府部门中的个人时，证书申请人还需提交由所属政府部门签章的证明文件，明确部门的名称并证明申请人属于该部门。

CFCA 或其授权的注册机构将复核并验证申请相关的申请材料，并进行批准申请或拒绝申请的操作。批准申请的，将保留相关证明材料的复印件，与申请表一并存档保存。

2.3.3 密钥更新请求的标识与鉴别

1） 常规的密钥更新请求的标识与鉴别

对于一般正常情况下的密钥更新申请，CFCA 需要证书持有者应提交能够识别原证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。

CFCA 及其注册机构对密钥更新申请的鉴别要求为：

当用户证书已过期时，重新进行与初始身份确认相同的实体鉴别流程；

当用户证书未过期时，用户既可采用与新申请证书相同的流程进行，也可采用在线更新方式；采用在线更新方式的，用户需在线提交更新申请并进行数字签名，CFCA 用原证书上的证书持有者公钥对申请的签名进行验证，以实现对用户身份的实体鉴别。

2） 撤销后的密钥更新的标识与鉴别

证书撤销后不能进行密钥更新。

2.3.4 撤销请求的标识与鉴别

证书撤销请求可以由证书持有者提出，也可以由 CFCA 及其授权的注册机构提出。

证书持有者向 CFCA 及其授权的注册机构申请撤销证书时，身份标识和鉴别使用原始身份验证相同的流程。

如果是因为证书持有者没有履行本 CPS 所规定的义务，由 CFCA 及其授权的注册机构申请撤销证书持有者的证书时，不需要对证书持有者身份进行标识和鉴别。

2.4 数字证书服务操作要求

2.4.1 证书申请

- **申请的提交**

电子政务活动中的个人或组织机构需要在电子政务活动中进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，可向 CFCA 或其授权的注册机构提出证书申请。

个人证书由证书使用者本人提出申请；机构证书由组织机构授权的人员申请；代码签名证书由拥有该软件的组织机构授权的人员提出申请；非证书持有者代表组织进行批量申请时，应同时提供该组织的授权。

申请人可以当面提交证书申请材料（证书申请材料的要求在 2.1.3 中有规定），也可将证书申请材料通过邮寄或传真的方式发送至 CFCA 及其授权的注册

机构。

● **注册过程与责任**

证书申请者须明确表示其愿意接受《CFCA 数字证书服务协议》中所规定的相关责任与义务，并需要完成以下注册过程：

- 填写证书申请表，并提供真实、准确的申请信息；
- 生成或委托生成密钥对；
- 将其公钥通过注册机构或直接传送至 CA；
- 证明其拥有与传送至 CA 的公钥相对应的私钥。

2.4.2 证书申请处理

● **执行识别与鉴别功能**

证书申请者向 CFCA 或其授权的注册机构提交证书申请后，CFCA 或其授权的注册机构将

- 核查证书申请材料是否完整充分；
- 验证证书申请信息的完整性；
- 确认申请行为得到合法授权；
- 对申请材料保密；
- 确认用户接受服务协议。

CFCA 及其授权的注册机构在处理每一个证书申请中，将保留对最终实体身份的证明和确认信息，并保证证书申请者和持有者信息不被篡改、私密信息不被泄漏。

● **证书申请批准和拒绝**

CFCA 或其授权的注册机构对证书申请者提交的申请材料进行鉴别符合要求后，将批准申请，保留证书申请的相关材料并存档保存。

如果申请者未能通过审核，CFCA 或其授权的注册机构将拒绝申请者的申请，并通过电话方式或者邮件方式在 48 小时内通知证书申请者。

● **处理证书申请的时间**

CFCA 及注册机构将在合理的时间内完成证书申请处理。在申请者提交的资料齐全且符合要求的情况下，处理证书申请的时间不超过 48 小时。

2.4.3 证书签发

● **证书签发中 CA 和 RA 的行为**

注册机构将客户信息录入 RA 系统中，并通过安全通道发送至 CFCA。

CFCA 负责验证注册机构的身份与权限， 并验证 RA 的签发请求，经验证无误后根据注册机构提交的申请信息向 RA 系统返回申请者下载证书用的凭证。

● **CA 和 RA 对证书申请者的通告**

证书申请批准后，RA 将证书下载凭证以安全的方式发送给证书申请者，包括：

1） 面对面交付的方式；

2） 密码信封的方式；

3） 其他安全方式。

注册机构有义务告知证书申请者在 CFCA 规定的时间内（即 14 天内）登陆相关网站下载证书。

2.4.4 证书接受

● **构成接受证书的行为**

证书申请者接收载有证书和私钥的介质视为接受证书。

证书申请者接收到证书下载凭证后，应在 14 天内登录相关网站下载数字证书到本地存放介质，如本地计算机、智能密码钥匙或智能 IC 卡等。证书下载完成后视为已经接受证书。

如果证书申请者在 14 天内没有进行证书下载操作，证书下载凭证将失效；

如果证书申请者在下载证书时发生错误，没有得到证书，而系统记录显示证书申请者下载成功，也同样视为客户已经接受证书（CFCA 技术支持人员有义务协助客户正确地获取证书）。

● **电子认证服务机构对证书的发布**

CFCA 在签发证书的同时会将该证书发布到目录系统中进行公开。

对于证书申请者明确表示拒绝发布证书信息的，CFCA 将不发布该证书信息。

● **电子认证服务机构通知其他实体证书的签发**

对于 CFCA 签发的证书，CFCA 和 RA 不对证书持有者和 RA 以外的其他实体进行通告。

2.4.5 密钥对和证书的使用

● **证书持有者私钥和证书的使用**

证书持有者在使用私钥和证书时须遵循以下约定：

1、 证书持有者只能在规定的、批准的范围内使用密钥和证书，签名密钥对用于签名与签名验证，加密密钥对用于加密与解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。密钥对和证书不得应用于其规定的、批准的用途之外的目的，否则其应用不受保障；

2、 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之后才能使用对应的私钥，并且在证书到期或被吊销之后，证书持有者必须停止使用该证书对应的私钥；

3、 证书持有者在使用证书时必须遵守《CFCA 数字证书服务协议》及本 CPS 的要求；

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

● **依赖方对公钥和证书的使用**

在依赖方接受数字签名信息后需要：

1、 获得数字签名对应的证书及信任链；

2、 确认该签名对应的证书是依赖方信任的证书；

3、 证书的用途适用于对应的签名；

4、 使用证书上的公钥验证签名；

5、 确认数字签名对应的证书状态正常，没有进入 CRL 列表。

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。依赖方应将加密证书连同加

密信息一起发送给接受方。

2.4.6 证书更新

● **证书更新的情形**

在证书到期前 30 天内或已到期后 30 天内，如果证书持有者的注册信息没有改变，证书持有者可以进行证书更新。

被撤销的证书不能进行证书更新。

● **更新申请的提交**

证书持有者、证书持有者的授权代表（如：机构证书）或证书对应实体的拥有者（如设备证书等）可以要求更新证书。

当证书已过期时应提交与新申请相同的申请材料进行更新申请，当证书未过期时可在线提交带有证书持有者电子签名的更新申请。

● **处理证书更新请求**

CFCA 及其注册机构对密钥更新申请的鉴别要求为：

当用户证书已过期时，重新进行与初始身份确认相同的实体鉴别流程；

当用户证书未过期时，用户既可采用与新申请证书相同的流程进行，也可采用在线更新方式；采用在线更新方式的，用户需在线提交更新申请并进行数字签名，CFCA 用原证书上的证书持有者公钥对申请的签名进行验证，以实现对用户身份的实体鉴别。

● **通知证书持有者证书的签发**

同证书初次申请时的接受规则。

● **构成接受更新证书的行为**

同证书初次申请时的通知方式。

● CA 对更新证书的发布

CFCA 在签发更新证书的同时会将该证书发布到目录系统中进行公开。

对于证书申请者明确表示拒绝发布证书信息的，CFCA 将不发布该证书信息。

● CA 通知其他实体证书的签发

对于 CFCA 签发的证书，CFCA 和 RA 不对证书持有者和 RA 以外的其他实体进行通告。

2.4.7 证书撤销

1、 证书撤销的条件

认证机构、注册机构及证书持有者应在发生下列情形之一时，申请撤销数字证书：

● 政务机构的证书持有者工作性质发生变化；

● 政务机构的证书持有者受到国家法律法规制裁；

● 证书持有者提供的信息不真实；

● 证书持有者没有或无法履行有关规定和义务；

● 认证机构、注册机构或最终证书持有者有理由相信或强烈的怀疑一个证书持有者的私钥安全已经受到损害；

● 政务机构有理由相信或强烈怀疑其下属雇员的私钥安全已经受到损害；

● 和证书持有者达成的证书持有者协议已经终止；

● 证书持有者请求撤销证书；

● 证书仅用于依赖方主导的系统并由依赖方提出撤销申请的；

● 法律、行政法规规定的其他情况。

2、 证书撤销的发起

以下实体可以请求撤销一个证书持有者证书：

批准证书持有者证书申请的认证机构、注册机构、电子政务机构或依赖方在满足证书撤销条件的前提下，可以要求撤销一个证书持有者证书。

对于个人证书，证书持有者可以请求撤销他们自己的个人证书。

对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书。

对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书。

当出现符合证书撤销条件中的情况时，应及时向发放该证书的注册机构提出书面撤销请求。

3、 证书撤销的处理

证书撤销时按以下流程进行：

1) 证书持有者（或其授权委托人）填写书面申请表并签名或盖章，同时提交与新申请相同的证明材料，向 CFCA 或注册机构提出撤销证书请求。

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

3) CFCA 或其授权的注册机构收到撤销请求并审核完成后，将在 24 小时内撤销符合条件的证书并发布到证书撤销列表。

说明：证书持有者在正式提出证书撤销申请后不得在交易中继续使用此证

书，否则由此产生的后果，由证书持有者自行承担。证书持有者在正式提出证书撤销申请后必须立即将此情况通知与此证书相关的依赖方，以便在交易中停止使用该张证书，否则由此产生的后果，由证书持有者自行承担。

CFCA 及其注册机构在确信出现证书撤销条件中的情况而需要立即撤销证书时，可以立即撤销证书。

证书撤销后，CFCA 将通过电话、短信、网站等方式告知用户或依赖方证书撤销结果。

4、 依赖方检查证书撤销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前应：

- 根据证书标明的发布地址获取证书撤销列表。
- 验证撤销列表的签名，确认其来自于该证书对应的签发机构。
- 验证证书撤销信息，确认证书是否被注销。

5、 CRL 发布频率

CRL 发布频率为 3 小时一次，在发布的同时对原有内容进行更新。

CFCA 目前使用的是 X.509 V2 版本的 CRL。

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。

6、 CRL 发布的最大滞后时间

CFCA 在生成 CRL 的 3 小时内会更新证书撤销列表。

7、 在线的撤销/状态查询的可用性

CFCA 提供在线的撤销/状态查询，该服务 7X24 小时可用。

8、 在线状态查询要求

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，依赖方在信赖一个证书前应：

- 按照查询协议要求，向证书中标明的 OCSP 服务地址提交状态查询请求。
- 查询过程应确保信息传输的机密性和完整性。
- 获得证书状态信息。

9、 撤销信息的其他发布形式

除 CRL 与 OCSP 之外，无其他撤销信息的发布形式。

2.4.8 密钥生成、备份与恢复

证书持有者的签名密钥对由证书持有者的本地计算机或密码设备(如智能密码钥匙或智能 IC 卡)生成,加密密钥对由国家设立的专门密钥管理机构(KMC，密钥管理中心）生成、备份和恢复。目前 KMC 托管在 CFCA，系统每天对数据进行备份。

签名密钥对由证书持有者的密码设备保管。

密钥恢复是指加密密钥的恢复，密钥管理基础设施不负责签名密钥的恢复。密钥恢复分为两类：证书持有者密钥恢复和问责取证密钥恢复。

1)证书持有者密钥恢复：当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可申请密钥恢复。证书持有者向 CFCA 提交申请，经审核后，通过 CFCA 向密钥管理基础设施发送请求；密钥恢复模块接受证书持有者的恢复请求，恢复证书持有者的密钥并下载于证书持有者证书载体中。

2)问责取证密钥恢复：问责取证人员向密钥管理基础设施提交申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

2.5 应用集成支持服务

2.5.1 证书应用接口程序

CFCA 提供证书应用接口程序供应用系统集成和调用。

证书应用接口程序符合《电子政务数字证书应用接口规范》，提供证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能。

证书应用接口程序支持 windows、AIX、Solaris、linux 等多种系统平台，并提供 C、C#、Java 等多种接口形态，可通过 com 组件、java 组件、ActiveX 控件、Applet 插件等多种形态提供服务。

2.5.2 证书应用方案支持

CFCA 具备针对电子政务信息系统的电子认证安全需求分析的能力、电子认证法律法规、技术体系的咨询能力以及设计满足业务要求的电子认证及电子签

名服务方案设计能力。

数字证书应用方案设计可包括：证书格式设计、证书交付、支持服务、信息服务、集成方案、建设方案、介质选型等。

2.5.3 证书应用接口集成

CFCA 具备面向各类应用的证书应用接口集成能力，并达到以下要求：

具备在多种应用环境下进行系统集成的技术能力，包括基于 Java、.NET 等 B / S 应用模式和基于 C、VC 等 C / S 应用模式的系统集成能力。

提供满足不同应用系统平台的证书应用接口组件包，包括 com 组件、java 组件、ActiveX 控件、Applet 插件等。

提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示 DEMO 等。

证书应用接口为上层提供简洁、易用的调用接口，其主要包括密码设备接口和通用密码服务接口。

- 密码设备调用接口

密码设备调用接口包括服务器端密码设备的底层应用接口和客户端证书介质(如：USBkey)的底层应用接口。

服务器端密码设备的底层应用接口在符合国际标准 PKCS#11 技术规范的基础上，符合《公钥密码基础设施应用技术体系密码设备应用接口规范》；客户端证书介质的底层应用接口符合《智能 IC 卡及智能密码钥匙密码应用接口规范》。

- 通用密码服务接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《电子政务电子认证服务应用接口规范》。

其主要包括服务器端组件接口和客户端控件接口。服务器端组件和客户端控件应支持不同电子认证服务机构所签发的符合《电子政务数字证书格式规范》的数字证书。

CFCA 为电子政务应用单位提供证书应用接口程序集成工作。集成工作提供以下服务：

- 证书应用接口的开发包(包括客户端和服务器端)；
- 接口说明文档；
- 集成演示 Demo；
- 集成手册；
- 证应用接口开发培训和集成技术支持；
- 协助应用系统开发商完成联调测试工作。

2.6 信息服务

2.6.1 服务内容

CFCA 提供的信息服务包括：

1） 证书信息服务

CA 系统中签发、更新、重签发的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。CFCA 提交

的数据包括业务类型、电子认证服务机构身份标识、用户基本信息、用户证书信息等。

2） CRL 信息服务

CA 系统签发 CRL 信息后，可实现将 CRL 实时发布到指定的电子政务信息系统中。CFCA 提交的数据包括业务类型、电子认证服务机构身份标识、CRL 文件、同步时间等。

3） 服务支持信息服务

CFCA 面向电子政务用户、应用系统集成商、应用系统发布与之相关的服务信息，包括 CPS、常见问题解答、证书应用接口软件包等。

4） 决策支持信息服务等

CFCA 面向电子政务应用单位、政府监管机构提供决策支持信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

2.6.2 服务管理规则

CFCA 在提供信息服务时，有相应的信息隐私保障机制，确保用户的私有信息不被泄漏。

● 私有信息类型的敏感度

以下信息属于私有信息：

(1)个人隐私信息；

(2)商业机密；

(3)政府部门的敏感信息和工作秘密。

证书发行过程中涉及的用户申请信息是敏感信息，而发布的证书和 CRL 信

息不是敏感信息。

● 允许的私有信息采集

CFCA 仅在进行证书发行和管理时才能收集私有信息。除了有特殊要求目的外，CFCA 不会收集更多私有信息。

● 允许的私有信息使用

CFCA 只使用 CA 或者 RA 收集的私有信息。

● 允许的个人信息发布

CFCA 及其注册机构仅面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。

在特别紧急情况下，CFCA 经相关管理机构的同意，可以发布私有信息。

任何特定的私有信息程序的发布遵照相关的法律和政策实行。

● 所有者纠正私有信息的机会

CFCA 允许用户在其证书生命周期内对其私有信息进行更正。

● 证书应用单位访问信息的限定

对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发的证书信息。应用单位管理员对非授权信息的访问，须依照政策管理规定，经上级主管部门批准后方可进行。

● 对司法及监管机构发布私有信息

CFCA 或者注册机构在收到以下命令时，可以执行将私有信息发给获得相应授权的人员：

(1) 司法程序；

(2) 经私有信息所有者同意；

(3)按照明确的法定权限的要求或许可。

对问责程序需要进行的信息访问，CFCA 将严格审核相应的问责人员身份及授权文件，无误后方可进行问责举证。

对监管部门应管理需求进行的信息访问，CFCA 将按照相关的管理规定和调取程序，为其提供信息访问权限。

2.6.3 服务方式

CFCA 的信息服务以网站（http://www.cfca.com.cn）或接口的形式面向应用系统或证书用户提供服务，以接口形式提供的服务符合《电子政务数字证书应用接口规范》的要求。

● **证书信息同步服务**

证书信息同步服务通过采用 Webservice 技术实现 CA 系统与电子政务系统的证书应用同步。电子政务信息系统通过部署统一的 Webservice 接口，CFCA 的 CA 系统通过调用统一的 Webservice 同步接口，实现 CA 系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，可通过对 Webservice 通信数据添加数字签名，以防止数据在传输中被篡改或数据损坏。

● **CRL 信息同步服务**

CRL 信息同步服务通过采用 Webservice 技术实现 CA 系统与电子政务系统的 CRL 同步。CA 系统主动调用该接口，实时将最新的 CRL 文件同步到电子政务信息系统中。

为了提高 CRL 文件传输的安全性，CFCA 对发送的 CRL 数据进行数字签名，

电子政务系统只需要根据 CFCA 的身份标识找到对应的根证书链，验证 CRL 签名的有效性即可确定 CRL 的有效性。

CRL 发布频率为 3 小时一次，在发布的同时对原有内容进行更新。

● **服务支持信息服务**

CFCA 通过网站（http://www.cfca.com.cn）向电子政务用户发布如下信息：

(1) 电子政务电子认证服务业务规则

(2) 证书生命周期服务流程及相关费用

(3) 证书用户操作手册

(4) 证书常见问题解答(FAQ)

(5) 获得证书帮助联系方式(客户服务热线电话、办公地址、邮政编码、投诉电话等)

(6) 其他应该发布的相关信息。

面向电子政务应用系统集成商 CFCA 通过网站（http://www.cfca.com.cn）或直接提供的方式发布如下信息：

(1) 数字证书应用接口软件包；

(2) 数字证书应用接口实施指南

(3) 证书常见问题解答(FAQ)

(4) 获得证书帮助联系方式(客户服务热线电话、办公地址、邮政编码、投诉电话等)

(5) 其他应该发布的相关信息。

面向电子政务应用系统应，CFCA 通过网站（http://www.cfca.com.cn）或

直接提供的方式发布如下信息：

(1) 时间戳服务数据接口；

(2) HTTP 防议的 CRL 发布服务接口：

(3) LDAP 协议的 CRL 发布接口；

(4) LDAP 协议的证书发布接口；

(5) OCSP 服务接口。

● **决策支持信息服务**

CFCA 向应用提供方以服务报告方式提供如下信息服务：

(1) 用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务。

(2) 投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析。

(3) 客户满意度信息：提供面向业务的客户满意度调查信息。

(4) 服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

2.7 使用支持服务

2.7.1 服务内容

CFCA 向证书使用用户及证书应用客户提供的使用技术支持服务包括：数字证书管理、数字证书使用、证书存储介质硬件设备使用、电子认证软件系统使用、电子认证服务支撑平台使用以及各类数字证书应用(如证书登录、证书加密、

数字签名)等贯穿证书使用和应用过程中的所有问题。

● **面向证书持有者的服务支持**

1)数字证书管理

数字证书的导入、导出、客户端证书管理工具的安装、使用、卸载等。

2)数字证书应用

数字证书用于身份认证、电子签名、加解密等应用出现的证书无法读取、签名失败、证书验证失败等应用问题。

3)证书存储介质硬件设备使用

证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

4)电子认证服务支撑平台使用

数字证书在线服务平台应用问题，如：证书更新失败、下载异常、无法提交注销申请等。

● **面向应用提供方的服务支持**

1)电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

2)电子签名服务中间件的应用

解决服务中间件在集成时出现的诸如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

2.7.2 服务方式

● 座席服务

CFCA 提供 7*24 热线服务:400-880-9888。

● 在线服务

CFCA 提供自助信息查询系统、网络实时通讯系统、远程终端帮助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

1)自助信息查询系统

将知识库信息、按照不同的类型、属性、层次等方式、结构进行分类存储，用户可以按照咨询问题或者已知条件在信息系统上进行启发式的检索，查找目标问题的答案。

2)网络实时通讯系统

用户可通过网络实时通讯工具与 CFCA 支持帮助人员取得联系，进行交流。

3)远程终端协助系统

用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软硬件环境，通过同屏显示指导、帮助用户解决应用故障。

4)在线帮助与传统模式的结合

将在线服务系统与电话服务结合，方便客户既可以打电话、也可自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

● 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

● 满意度调查

CFCA 通过多种用户可接受的多种调查方式进行客户回访，包括电话、WEB

网站、邮件系统、短信、传真等，并每月出具用户满意度调查报告。

CFCA 将用户回访中产生的相关文档进行归档、保存。

● 投诉受理

用户可通过 400-880-9888 客户热线、专用投诉电话（010-83519756）、电子邮件、及时通讯工具等方式进行投诉，CFCA 将在投诉受理过程中记录投诉问题，将投诉受理中产生的相关文档进行归档、保存，并将结果及时反馈给用户。

● 培训

培训方式可以由 CFCA 与客户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答(FAQ)、操作手册等。

2.7.3 服务质量

CFCA 的热线服务（400-880-9888）为 7*24 小时热线服务；

在线服务、现场服务为 5*8 小时服务；

在有应急服务需求的特殊情况下，CFCA 提供及时的服务。

CFCA 对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定了响应处理流程和机制，确保服务的及时性和连续性。技术支持响应时间以最大程度不影响客户使用为准则。

3 认证机构设施、管理和操作控制

3.1 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。CFCA 的物理环境按照《证书认证系统密码及其相关安全技术规范》的要求严格实施，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。

3.1.1 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，进入机房须经过五道审核，机房电磁屏蔽指标达到国家 BMB3 B 级标准。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

按照国家相关建筑标准实施，机房场所设置区域防护，根据业务功能划分监控区、综合服务区（非屏蔽机房）、安全区（屏蔽机房）、离线安全区各功能区域对应的安全级别为控制区、限制区、敏感区、机密区，安全等级和要求逐级提高。安全等级要求越高，安全防护措施和配套设施要求越严格。

3.1.2 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 办公区域要经过三道门禁系统，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。

操作人员自办公区进入安全区机房，须经过三道门禁系统，均需要双人指纹加门禁卡认证，并且所有门禁的进出信息都会在监控室的监控系统中记录。

3.1.3 电力与空调

CFCA 上地机房采用银联提供的 UPS 供电，由两组每组两台共四路独立 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。为了保证系统的可靠运行，银联还备有柴油发电机，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》）。

3.1.4 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。

3.1.5 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。

3.1.6 介质存储

CFCA CA 系统使用的存储介质被放置在防磁、防静电干扰的环境中，并处于 24 小时录像监控下，可以防止由于环境变化和人为故意产生的危害和破坏。

3.1.7 废物处理

敏感的文件资料（包括纸介质、光盘或软盘废物等）抛弃前要进行粉碎处理；对于存储或传输信息的介质，在抛弃前要做不可读取处理；加密设备在抛弃前要根据生产商的指导做归零处理。

3.2 操作过程控制

3.2.1 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

3.2.2 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。

3.2.3 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 3.3.2 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 使用数字证书和证书持有者名/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。

3.2.4 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。

3.3 人员控制

3.3.1 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。

3.3.2 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

3.3.3 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。

3.3.4 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。

3.3.5 工作岗位轮换周期和顺序

CFCA 根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

3.3.6 未授权行为的处罚

员工一旦被发现执行了未经授权的操作时，将被立即中止工作并受到纪律惩罚，其处理办法根据 CFCA 相关的管理规范执行。

3.3.7 独立和约人的要求

CFCA 在雇用独立和约人时，会要求提供身份证等相关的身份有效证明，并与 CFCA 签署保密协议。

3.3.8 提供给员工的文档

CFCA 向其员工提供完成其工作所必须的培训和相关的文档。

3.4 审计日志程序

3.4.1 记录事件的类型

1、CA 密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁。

2、RA 系统记录的证书证书持有者身份信息，包括企业（个人）姓名、证件号码、地址、邮箱、联系人等信息。

3、证书生命周期中的各项操作，包括证书申请、证书密钥更新、证书吊销等事件；

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

5、人员访问控制记录；

6、系统巡检记录。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

3.4.2 处理日志的周期

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

对于系统安全事件和系统操作事件日志，CFCA 每周进行一次检查、处理。

对于物理设施的访问日志，CFCA 每月进行一次检查、处理。

3.4.3 审计日志的保存期限

审计文档至少保存 10 年。

3.4.4 审计日志的保护

CFCA 建立完善的管理制度，并采取物理和逻辑的控制方法确保只有经 CFCA 授权的人员才能对审计日志进行操作。审计日志处于严格的保护状态，严禁未经授权的任何操作。

3.4.5 审计日志备份程序

CFCA 每天进行一次数据备份操作,并根据运营情况适时调整备份策略。

3.4.6 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。

3.4.7 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。

3.4.8 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。

3.5 记录归档

3.5.1 归档记录的类型

CFCA 归档记录的类型见本 CPS 的第 4.4.1 节。除此之外，对证书持有者证书、CA 证书也进行归档。

3.5.2 归档记录的保存期限

面向企事业单位、社会团体、社会公众的电子政务电子认证服务，信息保存期为证书失效后五年。

面向政务部门的电子政务电子认证服务，信息保存期为证书失效后十年。

3.5.3 归档文件的保护

CFCA 有相应的内部制度对存档记录进行妥善保存，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。

3.5.4 归档文件的备份程序

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

3.5.5 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。

3.5.6 归档收集系统

CFCA 有自动的电子归档信息的存放系统。

3.5.7 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。

3.6 电子认证服务机构密钥更替

当 CA 密钥对到期时，CFCA 将采取与系统根密钥初始化生成相同的流程和

方法对密钥进行更替，并采取如下方式确保用户和依赖方能够可靠地验证 CA 机构根证书以及确保证书信任链的有效性。

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（或最终证书持有者）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。

3.7 数据备份

CFCA 建立有完善的数据备份管理办法，根据数据备份策略定期进行数据备份。

针对系统备份：当系统建成或升级后，立即进行全备份；当系统的配置发生变化后，立即备份配置文件。

对数据库的备份：每天进行增量备份，每周进行全备份，并将备份数据转存在备份服务器上。

对重要的目录单独进行备份；

对于 CRL 备份：定期进行 CRL 备份，每季度将备份的 CRL 刻盘归档。

针对应用日志、系统日志备份：CFCA 每天自动备份应用日志及系统日志，并将备份的日志转存到备份服务器中。

对于手工日志备份：CFCA 指定专员备份手工日志，并保管手工日志的安全访问。

CFCA 建立有同城数据备份中心，正在建设同城灾备系统。

3.8 损坏与灾难恢复

3.8.1 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《普通事件应急预案》、《CFCA 系统故障报告与处理流程》、《CFCA CA 签名私钥泄漏紧急预案》、《CFCA CA 签名私钥泄漏的紧急处理流程》等相关规章制度采取合理措施。

3.8.2 计算资源、软件和/或数据的损坏

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

3.8.3 实体私钥损害处理程序

当实体私钥发生泄漏时，CFCA 将依据《CFCA CA 签名私钥泄漏紧急预案》、《CFCA CA 签名私钥泄漏的紧急处理流程》（以上为保密文档）进行处理。

3.8.4 灾难后的业务连续性能力

CFCA 正在考虑筹建同城灾备系统，以具备灾难后能迅速恢复业务的连续性能力。

3.8.5 业务持续计划的保障方案

CFCA 制订了相应的《业务持续计划》，确保 CA 业务的可持续性。

3.9 电子认证服务机构或注册机构的终止

当 CFCA 及其 RA 需要停止其业务时，将会严格按照《电子政务电子认证服务管理办法》的相关规定执行：

电子认证服务机构拟暂停或者终止认证服务的，应当在暂停或者终止认证服务六十个工作日前，选定业务承接电子认证服务机构，就业务承接有关事项作出妥善安排，并在暂停或者终止认证服务四十五个工作日前向国家密码管理局报告。

不能就业务承接事项作出妥善安排的，应当在暂停或者终止认证服务六十个工作日前，向国家密码管理局提出安排其他电子认证服务机构承接业务的申请。

4 认证系统技术安全控制

4.1 密钥对的生成和安装

4.1.1 密钥对的生成

1、 CA签名密钥的生成

CA的签名密钥在加密机内部产生，加密机通过国家密码主管部门的批准和许可。在生成CA密钥对时，CFCA按照详细的密钥产生控制流程，在机房的最安全取，由授权的三名安全管理员，在全程监控状态下产后CA密钥对。CA私钥不能以明文方式离开加密机。CA密钥的生成、保存和密码模块符合国家密码主管部门的要求，并通过了国家密码主管部门的鉴定。

2、RA密钥的生成

RA的签名私钥由自己产生，CFCA推荐使用加密机等硬件加密设备产生密钥，亦可在具有一定安全防护措施的情况下，使用软件产生密钥。RA的加密密钥由KM产生。

3、证书持有者密钥的生成

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

证书持有者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。

证书持有者的加/解密密钥对由国家设立的专门密钥管理机构（KMC，密钥管理中心）生成、备份和恢复

4.1.2 私钥传送给证书持有者

在证书持有者委托 CFCA 或其它可信服务商代替生成密钥对的情况下，CFCA会从技术和制度上保证被委托方不会留存私钥的备份。私钥会通过离线或在线的安全方式传送给证书持有者。

高级证书证书持有者的加/解密密钥对由国家设立的专门密钥管理机构（KMC，密钥管理中心）生成，其中的私钥会通过离线或在线的安全方式传送给证书持有者。

4.1.3 公钥传送给证书签发机构

证书持有者使用其签名密钥签名对应的公钥及证书信息，并通过安全的方式提交给 CA。CFCA 将验证该证书申请信息。

4.1.4 电子认证服务机构公钥传送给依赖方

用于验证 CFCA 签名的验证公钥（证书链）可从 CFCA 的信息库（目录服务或网站）获得。

4.1.5 密钥的长度

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

CFCA 目前提供 RSA-2048 位密钥长度和 SM2-256 密钥长度。

4.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理机构许可的加密设备生成，这些设备遵从国家密码管理机构的有关规范和标准，如对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求。

4.1.7 密钥使用目的

CA 私钥用于签发自身证书、下级 CA 证书、证书持有者证书和 CRL，CA 的公钥用于验证私钥签名。

证书持有者的签名密钥对可用于安全服务，例如身份认证、不可抵赖性和

信息的完整性，加密密钥对可以用于信息加密和解密。

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

对于 X.509 证书，这些目的需要映射到第三版证书的密钥用途标识位。

4.2 私钥保护和密码模块工程控制

4.2.1 密码模块标准和控制

密码模块（加密机）安置在 CFCA 核心区域，使用通过国家密码管理机构鉴定并批准使用的具有完全自主知识产权的高速主机设备，支持 RSA、SM2 等公钥密码算法，RSA 模长可选 512、768、1024、2048 比特；支持 SM4 等对称算法，支持 128 比特高强度加密；支持 MD2、MD5、SHA1、SDHI、SM3 等 HASH 算法。

4.2.2 私钥多人控制（m 选 n）

CFCA 从技术及制度上保证了敏感的加密操作需要在多个可信角色的共同参与下才能完成。在操作现场，必须有 5 人中的 3 人（包括 3 人)具备权限的密钥管理人员和操作人员，同时对加密机中的密钥进行操作，任何人无法独立完成操作。

4.2.3 私钥托管

对于 CA 私钥,CFCA 无托管业务；对于证书持有者加密私钥的托管，CFCA 将根据国家相关部门之规定执行。

4.2.4 私钥备份

1、CA 的私钥保存在防高温、防潮湿及防磁场影响的环境中，对私钥的备份操作须 3 人以上(包括 3 人)才可完成。私钥备份目前是以密文、分割密钥的形式存放。

2、CFCA 每天对 CA 的全部私钥（包括证书持有者的加密私钥）进行备份。

3、RA 的私钥由 RA 产生，由 RA 自行备份。

4、证书持有者的私钥由证书持有者产生，建议证书持有者自行备份，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。

4.2.5 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 CPS4.2.1 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 CPS4.2.10 所述的方法进行安全地销毁。私钥归档以密文、分割密钥的形式存放。目前没有到期，没有执行过归档。

CFCA 不对 RA 和证书持有者的私钥进行归档。

4.2.6 私钥导入、导出密码模块

CFCA 通过硬件模块生成 CA 密钥对，并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。

除备份操作外，私钥不能被导入或导出密码模块。

4.2.7 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。

4.2.8 激活私钥的方法

（1）个人和机构证书

个人和机构证书证书持有者的私钥可以存放在证书持有者计算机软件密码模块中，也可以存放在硬件密码模块中。当私钥存放在计算机软件密码模块中时，证书持有者需要采取合理的措施防止其他人在非授权情况下使用该机器。当密码模块完成对私钥保护口令的验证后，意味着私钥被激活，可以使用。

（2） CA 私钥

CFCA 采用硬件设备（加密机）产生、保存 CA 私钥，其激活数据按照本 CPS6.2.2 进行分割。一旦 CA 私钥被激活，激活状态将保持到 CA 离线。

4.2.9 解除私钥激活状态的方法

对于个人和机构证书，当软（硬）件密码模块被下载、证书持有者退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。

对于 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。

4.2.10 销毁私钥的方法

当 CA 的生命周期结束后，CFCA 将根据本 CPS 4.2.5 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，按照加密机密钥管理办法，在 3 名以上可信人员参与下进行安全地销毁。

证书持有者根据实际情况自行保存并销毁私钥，销毁私钥的方式包括交出令牌、销毁令牌或者重写密钥。(在加密私钥到期后一定期限内建议证书持有者继续保存该私钥，以便解开前期加密的信息。)

4.2.11 密码模块的评估

CFCA使用国家密码管理机构鉴定并批准使用的具有自主知识产权的高速主机加密设备，接受其颁布的各类标准、规范、评估结果等各类要求。密钥操作性能如下：

测试项目	指标	测试结果
1024 位 RSA 密钥对生成速度	50 对/秒	64.24
1024 位 RSA 签名速度	5500 对/秒	5518
1024 位 RSA 验证速度	22000 对/秒	20744
2048 位 RSA 密钥对生成速度	10 对/秒	9.86
2048 位 RSA 签名速度	600 对/秒	610.81
2048 位 RSA 验证速度	15000 对/秒	18973.87
256 位 SM2 密钥对生成速度	350 对/秒	358.74
256 位 SM2 签名速度	650 对/秒	711.89
256 位 SM2 验证速度	180 对/秒	181.85
256 位 SM2 加密速度	170 对/秒	174
256 位 SM2 解密速度	300 对/秒	297
SM3 杂凑算法	22.625M/S	55.56
SM1 算法加密速度	13.75M/S	13.63
SM1 算法解密速度	13.75M/S	13.67
SM4 算法加密速度	13.75M/S	13.86
SM4 算法解密速度	13.75M/S	14.06

4.3 密钥对管理的其它方面

4.3.1 公钥归档

作为 CFCA 备份策略的一部分，CA、注册机构和证书持有者的证书都已经归档保存。

4.3.2 证书操作期和密钥对使用期限

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

CA 密钥对使用期限和 CA 证书的有效期保持一致，均为 15 年。证书持有者证书的密钥对和证书持有者证书的有效期保持一致。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，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。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

4.4 激活数据

4.4.1 激活数据的产生和安装

1、 CFCA 的 CA 私钥产生遵循本 CPS4.2.2 中的要求。

2、 对于注册机构和证书持有者，激活数据是保护私钥的密码。CFCA 推荐注册机构和证书持有者使用强口令来保证私钥的安全性。

3、 CA 私钥和证书持有者证书私钥的激活数据一般是口令，这些口令必须：

- 由用户产生；
- 至少 8 位字符；
- 至少包含一个字符和一个数字；
- 至少包含一个小写字母；
- 不能包含很多相同的字符；
- 不能和操作员的名字相同；
- 不能包含用户名信息中的较长的子字符串。

4.4.2 激活数据的保护

1、 CFCA 的密钥管理者须保护他们所维护的秘密份额，并且须签署协议来承诺所承担的责任。

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

3、 证书持有者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。

4.4.3 激活数据的其他方面

（1） 激活数据的传输

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

对于证书证书持有者，通过网络传输用于激活私钥的口令时，需要采取保护措施，以防丢失。

（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。

证书持有者私钥的激活数据在不需要时由证书持有者自行销毁，证书持有者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。

4.5 计算机安全控制

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

CFCA 确保包含 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。此外，CFCA 只允许有工作需求的必要人访问产品服务器，一般的应用用户在产品服务器上没有账户。

CFCA 的生产系统网络与其它部分逻辑分离。这种分离可以阻止除指定的应用程序外对网络访问的访问。CFCA 使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有认证系统操作与管理组中的、有必要工

作需要、访问系统的可信人员可以直接访问 CFCA 的认证系统数据库。

系统口令符合口令安全管理要求。

4.6 生命周期安全控制

4.6.1 CA系统开发控制

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

4.6.2 CA系统运行管理

CFCA 认证服务系统的信息安全管理，严格遵循行业主管部门的规范进行操作。系统的任何变更都经过严格的测试验证后才能进行安装和使用。同时，按照 ISO9000 质量管理体系标准建立了严格的管理制度。对于核心数据（CA 数据、目录数据、日志信息），系统自动进行备份恢复，每天安排专人定时检查备份恢复情况，以验证数据的有效性。

CFCA 制定有严格的 CA 系统操作流程。CA 系统（包括软件、网络等方面）的变更需经管理层批准，经批准的变更实行前必须通过测试，并进行记录。可能对系统的安全性有影响的改动必须事先得进行风险评估，改动前应进行备份并得到管理层的明确批准。

CA 中心的测试系统、运营系统、网络设施等，具有专门的操作维护人员，并有相应明确的授权。

操作维护人员定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平。

系统有相应的检测和防护控制来防止病毒和恶意软件，并能提供适当的报警信息。

CFCA 建立了相应的监控流程，确保记录并报告发现的或怀疑的、对系统或服务有威胁的安全缺陷，建立了并执行系统故障报告、处理流程。

CFCA 有相应的制度，对 CA 系统相关的媒介(包括设备、证书介质、文档等)进行妥善保管，避免非授权的访问。

4.6.3 CA系统的访问管理

CFCA 有相应的 CA 系统访问策略，内容包括：访问角色及相关权限，认证及鉴别的方法，分权机制，CA 特殊操作的人数(密钥生成时 m / n 规则)等。

CFCA 对 CA 系统访问人员角色职能进行了合理的定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略。

CFCA 有相应的网络安全策略，并制定了访问网络的控制策略。

CFCA 制定了操作系统及 CA 软件的安全访问策略。

CFCA 建立了对各种 CA 系统访问的审计措施。

4.6.4 CA系统的开发和维护

CFCA 有相应的 CA 系统软件修订控制流程，对系统新增或修改进行管理。

CFCA 严格控制对 CA 系统的源代码及测试数据的访问。

操作系统升级变更时，应用系统软件需要重新测试。

在 CA 系统中，购买、使用或修改的软件，需要进行严格检查，避免木马或病毒等攻击。

4.7 网络的安全控制

CFCA 认证系统通过以下手段来防止网络受到未授权的访问和抵御恶意攻击：

1、由路由器对来自外部的访问信息进行过滤控制；

2、将功能独立的服务器放置在不同的网段；

3、多级异构防火墙划分不同网段，并采用了完善的访问控制技术；

4、通过验证和存取访问权限控制进行数据保护；

5、在 CFCA 网络系统中，采用入侵检测产品，从检测与监听等多方面对网络系统进行防护，及时发现入侵者并报警，并实施事件响应；

6、所有终端安装防病毒软件，并定期升级；

7、提供冗余设计。

4.8 时间戳

CFCA 所有服务器使用同一时间源，证书、CRL、认证服务系统日志均包含时间信息，该信息无需加密保存。

5 法律责任和其他业务条款

5.1 费用

5.1.1 证书签发和更新费用

关于证书费用问题请咨询有关注册机构或 CFCA 市场部。

5.1.2 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。

5.1.3 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。

5.1.4 其它服务费用

CFCA 保留收取其他服务费的权利。

5.1.5 退款策略

除非 CFCA 违背了本 CPS 所规定的责任，证书持有者可以要求退款。否则，CFCA 对证书持有者收取的费用均不退还。

证书持有者应当提供符合 CFCA 要求的完整、真实、准确的个人信息，否则 CFCA 对此造成的损失和后果不承担任何责任。

5.2 财务责任

5.2.1 保险范围

CFCA 根据监管机构的要求、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。

5.2.2 其它资产

机构证书持有者需具有足够的财务实力来维持其正常经营并保证相应义务

的履行，他们必须合理地承担对证书持有者及对依赖方的责任。

此要求对 CFCA 同样适用。

5.2.3 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。

5.3 业务信息保密

5.3.1 保密信息范围

保密信息包括但不限于以下内容

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

2、 证书持有者私钥属于机密信息，证书持有者应该根据本 CPS 的规定妥善保管，如因证书持有者自己泄漏私钥造成的损失，证书持有者应自行承担。

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

4、 有关认证系统的运营信息、技术手册等资料属于保密信息。

5、 除非法律明文规定或政府、执法机关等的要求，CFCA 承诺不对外公布或透露证书持有者证书信息以外的任何个人隐私信息；同时，CFCA 在同所有注册机构签署授权协议时，都将此条作为协议条款。

5.3.2 不属于保密的信息

不属于保密的信息包括：

1、CA 系统签发的证书和 CRL 中的信息。

2、在提供方披露数据和信息之前，已被接受方所持有的数据和信息。

3、在提供方披露数据和信息时或在披露数据和信息之后，非由于接受方的原因而被披露的信息。

4、经公开或通过其他途径成为公众领域的一部分数据和信息。

5、有权披露的第三方披露给接受方的数据和信息。

6、其他可以通过公共、公开渠道获得的信息。

5.3.3 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。

5.4 个人信息私密性

5.4.1 隐私保密方案

CFCA 尊重所有证书持有者和他们的隐私，个人隐私信息保密方案遵守现行法律和政策。任何人选择使用 CFCA 的任何服务，就表明已经同意接受 CFCA 的隐私保护制度。

5.4.2 作为隐私处理的信息

CFCA 在管理和使用证书持有者提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该证书持有者的基本信息将被视为隐私处理，非经证书持有者同意或有关法律法规、公共权力部门根据合法的程序要求，不会任意公开。

5.4.3 不被视作隐私的信息

证书持有者持有的证书信息，以及证书状态信息不被视为隐私信息。

5.4.4 保护隐私的责任

CFCA、证书持有者、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。

5.4.5 使用隐私信息的告知与同意

1、 证书持有者同意，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证书持有者信息，无论是否涉及到隐私，CFCA 均可以不用告知证书持有者。

2、 证书持有者同意，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 均可以不用告知证书持有者。

5.4.6 依法律或行政程序的信息披露

除非符合下列条件， CFCA 不会将证书持有者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、 证书持有者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。

5.4.7 其它信息披露情形

CFCA、证书持有者、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证书持有者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。

5.5 知识产权

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

5.6 陈述与担保

5.6.1 电子认证服务机构的陈述与担保

CFCA 采用经过国家有关管理机关审批的信息安全基础设施为进行网上业务的各方提供信息安全保障。

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

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

CFCA 的运作遵守《中华人民共和国电子签名法》等法律，接受行业主管部门的领导，CFCA 对签发的数字证书承担相应法律责任。

CFCA 的运营遵守 CPS 并随着业务的调整对 CPS 进行修订。

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

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

1） 提供签发该张证书持有者数字证书的 CA 证书。

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

3） 对数字证书、数字签名、时间戳的真实性、有效性进行技术确认。

5.6.2 注册机构的陈述与担保

CFCA 通过注册机构向证书持有者发放 CFCA 数字证书， 注册机构通过 LRA 面向证书证书持有者，负责审核申请人的身份并决定接受或拒绝申请人申请、负责录入证书持有者信息，并将证书申请信息安全地传送到 CA。

注册机构声明和承诺：

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

2、 如注册机构对证书持有者的证书申请材料审查没有通过，注册机构有向证书持有者进行告知的义务，如证书申请被批准，RA 有义务通知证书持有者并且指导证书持有者得到证书；

3、 RA 应在合理的时间内完成证书申请处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过 5 个工作日。

4、 RA 须对证书持有者的信息及与认证相关的信息妥善保存，保存期限为数字证书失效后五年。

5、 RA 应使证书持有者明确地知道关于使用第三方数字证书的意义、数字证书的功能、使用范围、使用方式、密钥管理以及丢失数字证书的后果和处理措施、法律责任限制。

6、 基于 CFCA 规定的信息传输协议和标准与 CA 交换数据；

7、 证书签发及被吊销时及时通知证书持有者。

8、 在接到具有授权的申请人关于证书管理的有效请求时，进行相应证书管理操作，并保留全部操作记录和日志；

9、有义务通知证书持有者阅读 CFCA 发布的 CPS 和《CFCA 数字证书服务协议》和其它相关规定，在证书持有者完全知晓并同意 CPS 和《CFCA 数字证书服务协议》内容的前提下，为证书持有者办理数字证书。

10、保留证书持有者的信息及与认证相关的信息，保存期限为数字证书失效后五年。

5.6.3 证书持有者的陈述与担保

证书持有者声明和承诺：

证书持有者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。

证书持有者应遵循诚实、信用原则，在申请数字证书时，应当提供真实、完整和准确的信息和资料，并在这些信息、资料发生改变时及时通知 CFCA 或原注册机构。如因证书持有者故意或过失提供的资料不真实或资料改变后未及时通知 CFCA 或原注册机构，造成的损失由证书持有者自己承担。

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

证书持有者应将证书用于合法目的并符合 CFCA 证书策略和本 CPS；

证书持有者应对使用证书的行为承担责任。

证书持有者应使用可信系统产生密钥对，防止密钥遭受攻击丢失、泄漏和误用；证书持有者应当妥善保管 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，证书持有者应承担由此产生的责任。

如证书持有者使用的数字证书私钥和密码泄漏、丢失，或者证书持有者不希望继续使用数字证书时，或者证书持有者主体不存在，证书持有者或法定权利人应当立即到原注册机构申请废止该数字证书，相关手续遵循注册机构的规定。

由于以下情况证书持有者损害 CFCA 利益的，证书持有者须向 CFCA 赔偿全部损失。这些情况是：

1） 证书持有者在申请数字证书时没有提供真实、完整、准确的信息，在这些信息变更时未及时通知 CFCA；

2） 证书持有者知道自己的私钥已经失密或者可能已经失密未及时告知有关各方、并终止使用；

3） 证书持有者有其他过错或未履行双方约定。

证书持有者有按期缴纳数字证书服务费的义务，费用标准请咨询注册机构。

随着技术的进步，CFCA 有权要求证书持有者更换数字证书。证书持有者在收到数字证书更换通知后，应在规定的期限内到原数字证书注册机构更换。因证书持有者逾期没有更换数字证书而引起的后果，CFCA 不承担责任。

5.6.4 依赖方的陈述与担保

依赖方声明和承诺：

1、使用适当的软件和/或硬件进行数字签名的验证或其它操作；

2、确信在交易前检查 CRL 获知证书状态和验证签名；

3、只在符合相关策略和本 CPS 规定的证书应用范围内信任该证书；

4、确认证书链的合法性；

5、同意 CPS 中关于 CFCA 责任限制的规定。

5.6.5 其它参与者的陈述与担保

其他参与者应遵循本 CPS 的规定。

5.7 担保免责

1、证书申请人或证书持有者故意提供或未按照要求提供不准确和/或不真实和/或不完整的信息而获得 CFCA 签发的预植证书，证书持有者在使用该证书时引起的责任，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，若证书被超范围使用或被用于其他不被 CFCA 允许的用途，CFCA 不承担任何法律责任。

4、CFCA 在法律许可的范围内，根据有关法律法规的要求，如实提供电子交易和网络交易中产生的数字签名的验证信息（“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。

5、对于明显由于 CFCA 的合作方或代理方的越权行为或其他过错行为所引发的违反约定义务而对证书持有者造成的损失，CFCA 不承担赔偿和/或补偿责任。

6、由于不可抗力因素导致 CFCA 暂停、终止部分或全部数字证书服务，CFCA 不承担赔偿和/或补偿责任。

5.8 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。

5.9 CFCA承担赔偿责任的限制

5.9.1 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 不向证书持有者和/或依赖方承担任何赔偿和/或补偿责任。

5.9.2 证书持有者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，也不对证书持有者或依赖方承担任何赔偿或补偿责任。

5.9.3 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）证书持有者和/或依赖方的任何间接损失、直接或间接的利润或收

入损失、信誉或商誉损害、任何商机或契机损失、失去项目、或失去或无法使用任何数据、设备或软件；

（2）由上述损失相应生成或附带引起的损失或损害；

5.9.4 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。

5.10 有效期限与终止

5.10.1 有效期限

本 CPS 自 CFCA 在其官方网站公布之日起生效，除非 CFCA 特别声明 CPS 提前终止。

5.10.2 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。

5.10.3 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。

5.11 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。

5.12 修订

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

5.12.1 修订程序

修订程序与本 CPS1.4“CPS 批准程序”相同。

5.12.2 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，证书持有者没有申请对其证书进行吊销，将被视为同意该修改。

5.12.3 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 电子政务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。

5.13 争议处理

证书持有者或依赖方在发现或怀疑由 CFCA 提供的认证服务造成证书持有者的网上交易信息的泄漏和/或篡改时，应在有效期内向 CFCA 提出争议处理请

求并通知有关各方，有效期为 3 个月。

争议处理流程为：

1、 争议解决的通知：

当争议发生时，在采取任何解决途径之前，证书持有者应首先通知 CFCA 及注册机构。

2、 争议解决的方式：

如果争议在最初通知的 10 天内未被解决，CFCA 将召集由 3 名安全认证专家组成的外部专家小组。外部专家小组以协助解决争议为目的，收集相关事实。专家小组应在成立后 10 天内（除非当事人同意将此段时限延长至一特定时段）完成建议并向当事人传达。专家小组的建议对当事人无约束力。但当事人一方若签署表示同意该建议则争议的双方即按照建议的内容解决争议。如果证书持有者事后反悔并将争议提交仲裁，那么该建议将视为 CFCA 与证书持有者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

任何证书持有者或依赖方欲向 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。

5.14 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》、《电子政务电子认证服务管理办法》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。

5.15 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的相关要求，如国家密码管理局相关密码技术、产品标准规范;《电子政务电子认证服务管理办法》等。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。

5.16 一般条款

5.16.1 本CPS的完整性

本 CPS 将替代所有以前的或同时期的、与相同主题相关的书面或口头解释。CP、CPS、证书持有者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。

5.16.2 转让

无。

5.16.3 分割性

无。

5.16.4 强制执行

无。

5.16.5 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。

5.17 其它条款

无。