中金金融认证中心有限公司
全球信任体系
电子认证业务规则

（Certification Practice Statement Of CFCA Global-Trust System）

V1.0

2011 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 全球信任体系下的业务规则。CFCA 的全球信任体系是指用于发放 CFCA 全球服务器证书，建立互联网中权威基础信任关系的证书信任体系。

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)》及 CA 的一般运作规范。

1.2 文档名称与标识

此文档的名称为《CFCA 全球信任体系电子认证业务规则(CFCA Global-Trust CPS)》，对象标识符为 2.16.156.112554.2。

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。

CFCA 的全球信任证书认证系统用于签发 CFCA 全球服务器证书，其名称为 CFCA Global-Trust CA。CFCA 全球服务器证书是指遵循本 CPS 要求签发的，安装在订户的 Web 服务器中，在 Web 服务器和浏览器之间提供身份验证、信息加密等功能。

1.3.2 注册机构

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

CFCA 全球信任体系下的注册机构设在 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。

1.4 证书应用

1.4.1 适合的证书应用

CFCA 全球信任体系下签发的证书主要是指全球服务器证书，适合应用在网上银行、电子商务、电子政务、企业信息化以及公共服务等各领域，用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露；订户或依赖方可以通过服务器证书验证

所访问的网站是否真实可靠，实现网站身份的真实性确认，为建设网络信任环境提供基础性信任服务。

1.4.2 限制的证书应用

CFCA 全球信任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 业务管理部。当需要编写或修订本 CPS 时，由业务管理部牵头组织应用开发部、运行部、技术支持部及综合部的相关人员组成“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 业务管理部联系：

电话：010-83526220

传真：010-63555032

邮件：cps@cfca.com.cn

地址：中国北京西城区菜市口南大街平原里 20-3

1.5.3 决定 CPS 符合策略的机构

“CPS 编写组”拟定初稿或修订稿后，交由公司法律顾问审阅。法律顾问审阅后由各部门负责人及分管领导审阅，并报总经理审批。总经理审批同意后，本 CPS 方可对外发布，并自发布之日起 20 天内向行业主管部门报备。

1.5.4 CPS 批准程序

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

“CPS 编写组”负责将 CPS 送审稿提交公司法律顾问审阅。在取得法律顾问的意见后，“CPS 编写组”据此进行修改并提交业务管理部，由业务管理部确定 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。发布工作由业务管理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。业务管理部负责自发布之日起 20 天内向行业主管部门报备。

业务管理部定期对 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业务管理部提出修订申请。

当修订内容具有重大变更时，CFCA 将按照与初次编写相同的流程进行；当

修订内容变动较小时，由业务管理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业务管理部自发布之日起 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 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。CFCA 信息库包括但不限于以下内容：证书、CRL、CPS、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 根据 X.509 标准在信息库上公布证书的相关信息，并发布证书和 CRL。CPS、CP 以及相关业务规则在 CFCA 网站上发布。

2.3 发布的时间或频率

CPS、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；订户的证书信息实时发布到信息库上；CFCA 将在证书吊销后一小时内在信息库上更新 CRL，根据需要，也可以人工方式实时发布最新 CRL。

2.4 信息库访问控制

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

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

CFCA 全球信任体系下签发的证书采用 X.500 定义的甄别名称（DN）标准来唯一标识证书主体信息。DN 的详细说明见本 CPS 的 7.1.4。

3.1.2 对名称意义化的要求

DN（Distinguished Name）：唯一甄别名，在数字证书的主体名称域中，用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。

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

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

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证明订户拥有私钥的方法是通过 pkcs#10 的数字签名来完成的。订户签名私钥（private key）由订户在订户端生成，订户发出的数据包中包含用签名私钥进行的数字签名，其他各方用对应的验证公钥可以验证这个签名。因此，订户被视作其签名私钥的唯一持有者。

订户在申请 CFCA 全球服务器证书前，需在拟安装服务器证书的 Web 服务器上产生证书私钥，并在生成私钥的同时按照如下格式要求生成证书签名请求（Certificate Signature Request，简称 CSR），由 CFCA 进行审核：

CN=网站域名或 IP 地址

O=个人：拥有该域名的个人名称

机构：拥有该域名或 IP 地址的机构名称

OU=GTC（注：GTC 为 Global Trust Certificate 的缩写）

C=国别的简称，例如中国为 CN。

3.2.2 订户身份的鉴别

订户在申请 CFCA 全球信任体系签发的证书前应指定并书面授权证书的申请代表，提供有效身份证明文件及证书申请文件，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，并需验证订户是否对于需在 CFCA 全球服务器证书中标识的域名或 IP 地址拥有所有权，验证完成后方可签发证书。

3.2.2.1 个人订户身份的鉴别

个人订户申请 CFCA 全球服务器证书时，应向 CFCA 提供以下任意一种真实有效的个人身份证明文件：

（1）身份证；

（2）护照；

（3）军人身份证件；

（4）武装警察身份证件；

（5）港澳居民往来内地通行证；

（6）台湾居民来往大陆通行证；

（7）户口簿；

（8）法律法规认可的其它身份证明文件。

申请人应出示上述所列示的至少一种身份证件，并出示域名或 IP 地址归属于申请人的相关证明，并向 CFCA 提交 CSR 文件。

CFCA 对于个人订户身份的鉴别流程为：

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

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

（1）对订户提交的身份证明文件与证书申请材料中的信息进行核对，确保其准确性与完整性；

（2）对订户提交的CSR文件进行验证，确认符合3.2.1中规定的格式要求；

（3）对于订户提交的域名信息通过第三方信息渠道进行验证，确认该域名归属于证书申请人所有。

3.2.2.2 机构订户身份的鉴别

机构订户在申请CFCA全球服务器证书前应授权本机构工作人员向CFCA提出证书申请，并向CFCA提供以下任意一种真实有效的机构身份证明文件：

（1）营业执照；

（2）组织机构代码证；

（3）事业单位法人证书；

（4）税务登记证；

（5）社会团体登记证书；

（6）民办非企业登记证书；

（7）外国（地区）企业常驻代表机构登记证；

（8）依照有关法律、行政法规和国家有关规定的其它机构身份证明；

（9）境外机构的身份证件，为符合当地法律、行政法规和该国有关规定的机构身份证件。

申请人应出示上述所列示的至少一种机构身份证件，授权申请人的个人实名身份证件，机构授予申请人的授权证明，以及加盖机构公章的证书申请表（该表格可在 CFCA 网站上下载）；同时，证书申请人还应出示域名或 IP 地址归属于申请机构的相关证明，并向 CFCA 提交 CSR 文件。

CFCA 对于机构订户身份的鉴别流程为：

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

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

（1）对于机构提供的身份证明文件，可通过可靠第三方渠道或 CFCA 的身份信息库验证该机构是否真实存在；

（2）对订户提交的 CSR 文件进行验证，确认符合 3.2.1 中规定的格式要求；

（3）对于申请机构提交的域名信息，通过第三方渠道进行验证，确认该域名归属于证书申请机构所有；对于申请机构提交的 IP 地址信息，若 IP 地址为外网 IP，机构订户需提供有效证明，证明此外网 IP 为该机构所有，内网 IP 不可申请全球服务器证书；若域名或 IP 地址为其它机构授权申请机构使用（例如总公司向分公司授权，总部向分部授权），则还需申请机构提供域名被授权使用证明。

3.2.3 没有验证的订户信息

订户提交的信息都会进行验证，不存在未验证的订户信息。

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

对于申请全球服务器证书时的订户，CFCA 承担对订户身份的鉴别职能，不会委托其他机构行使此职责。对于其他证书发放机构已经审核过的订户身份信息，CFCA 将会重新进行验证。

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（文件）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，订户向 CFCA 重新提交 CSR 即可，CFCA 无需对订户身份进行重新验证；超过三个月后则需对订户身份进行重新验证。

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，换发操作成功时，旧证书立即被吊销。

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 工作人员会通过电子邮件、电话等方式通知用户对证书进行换发操作。

订户需对原有证书进行换发更新时，应指定并书面授权证书的申请代表，提供有效身份证明文件及证书更新文件，并接受证书更新申请的有关条款，同意承担相应的责任。CFCA 接受订户的换发更新申请后，需重新对订户的身份真实性进行审核，并需验证订户是否仍然对于需在全球服务器证书中标识的域名或 IP 地址拥有所有权，验证完成后方可为其进行换发操作。

换发操作成功后，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。对于全球服务器证书，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 全球信任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 中所

规定的相关责任与义务（本 CPS 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；

2、认证机构

CFCA 作为认证机构，应对订户提供的身份信息按照 3.2.2 的要求进行鉴别，对通过鉴别后的订户签发证书，同时履行本 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

同 3.2.2。

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符合要求的情况下，处理证书申请的时间不超过 5 个工作日。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

CFCA 按照 3.2.2 的要求对订户的申请信息进行验证且验证通过后方可向订

户签发证书。

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、电子邮件等它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

CFCA 签发出相应的证书后，会在信息库中发布此证书。

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

订户在使用私钥和证书时须遵循以下约定：

1、 订户只能在规定的范围内（在本 CPS1.4.1 节定义）使用私钥和证书，

并对使用行为承担责任；

2、 订户在使用证书时必须遵守本 CPS 的要求；

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

4.5.2 依赖方公钥和证书的使用

依赖方信赖 CFCA 全球信任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

对于全球服务器证书，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)订户申请证书时，提供的资料不真实；

2)订户未履行本 CPS 中约定的义务；

3)订户将证书安装在法律、行政法规定义为非法站点的网站上；

4）证书的安全性不能得到保证，如相信或怀疑密钥泄漏或遭受攻击，存放证书的服务器损坏或被锁定等；

5）订户书面申请吊销数字证书；

6)法律、行政法规规定的其他情形。

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。当出现上述提到的第 1、2、3 种情况时，适用于被动吊销，第 4、5 种情况适用于主动吊销，第 6 种情况则既可能出现被动吊销，也可能出现主动吊销。

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

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

4.8.3.2 被动吊销

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

4.8.4 吊销请求宽限期

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

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

4.8.5 电子认证服务机构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，会立即执行证书

吊销操作。

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

CRL 发布频率为 1 小时一次，在发布的同时对原有内容进行更新。

4.8.8 CRL 发布的最大滞后时间

CFCA 在生成 CRL 的 1 小时后会更新信息库。

4.8.9 在线证书状态查询的可用性

CFCA 提供 LDAP 形式的在线证书状态查询服务，该服务 7X24 小时可用。

订户或依赖方可通过 LDAP 协议查询证书状态。LDAP 请求应当包含的数据包括；查询的 ip 地址，端口，查询内容。

CFCA 会对查询请求进行检查，检查的内容包括；检查 dn 是否合法，dn 节点的上级是否存在，查询匹配的规则及范围等。

若检查通过后则向订户或依赖方返回包含如下内容的证书信息：

通用名称；

证书位置；

证书 DN；

证书状态；

证书类型；

证书序列号；

包含 CA 私钥签名的证书实体对象。

若检查不通过则会向订户或依赖方返回查询条目不存在或 ldap 数据参数错误的出错信息。

4.8.10 吊销信息的其他发布形式

除 CRL 外，尚无其它发布形式。

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

对于全球信任体系下颁发的证书，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 LDAP 目录查询服务获得。

4.9.2 服务可用性

CFCA 提供 7X24 小时不间断证书状态查询服务。

4.10订购结束

以下两种情形将被视为订购结束：

1、 证书到期后即视为订购结束。

2、 证书吊销视为订购结束。

4.11密钥生成、备份与恢复

为保证订户密钥的安全性，订户应独立生成密钥对，及时进行备份，并确保密钥的安全性，以防密钥丢失。在生成密钥对之后与安装服务器证书之前的时期内不应更改服务器的任何配置，以防密钥丢失。在密钥丢失或可能泄漏后，需及时申请密钥更新。

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

5 认证机构设施、管理和操作控制

5.1 物理控制

系统的物理安全和环境安全是整个 CFCA 系统安全的基础，它包括基础设施的管理、周边环境的监控、区域访问控制、设备安全及灾难预防等各方面。为保证 CFCA 系统物理环境的安全可靠，CFCA 系统被放置于安全稳固的建筑物内

并具备独立的软硬件操作环境，充分考虑了水患、火灾、地震、电磁干扰与辐射、犯罪活动以及工业事故等的威胁。

5.1.1 场地位置与建筑

CFCA CA 系统的运营机房位于北京市海淀区中关村软件园区 22 号楼（中国银联北京信息中心楼内）内，进入机房须经过三道审核，机房电磁屏蔽效能满足 GJBz20219－94 标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

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；加密设备在抛弃前要根据生产商的指导做归零处理。

5.1.8 数据备份

目前 CFCA 已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。

5.3 人员控制

5.3.1 资格、经历和无过失要求

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

5.3.2 背景审查程序

CFCA 在开始一个可信任角色的雇佣关系前会依据以下流程对其进行审查：

（1）应聘者应提交的个人资料

履历、最高学历毕业证书、学位证书、资格证及身份证等相关的有效证明。

（2）应聘者个人身份的确认

CFCA 人力资源部门通过电话、信函、网络、走访、调阅档案等形式对其提供材料的真实性进行鉴定。

（3）三个月的试用期考核

通过现场考试、日常观察、情景考验等方式对其考察。

以上三方面的审查结果必须符合第 5.3.1 节中规定的要求。

（4）签署保密协议

与到岗人员签署保密协议。

（5）上岗工作

5.3.3 培训要求

CFCA 对录用人员按照其岗位和角色安排培训。培训内容有：PKI 的相关知识、岗位职责、内部规章制度、认证系统软件、相关应用软件、操作系统与网络、ISO9000 质量控制体系、CPS 等。

5.3.4 再培训周期和要求

CFCA 每年至少向员工提供一次业务培训机会以不断提高其职业技能，以保持其完成工作所需要的职业水平。同时，当 CA 系统更新升级时也会对其员工进行相应的培训。

5.3.5 工作岗位轮换周期和顺序

CFCA 根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

5.3.6 未授权行为的处罚

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

5.3.7 独立和约人的要求

CFCA 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。

5.3.8 提供给员工的文档

CFCA 向其员工提供完成其工作所必须的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

CFCA 记录的日志信息包括但不限于以下类型：

1、CA 密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁。

2、RA 系统记录的证书订户身份信息，包括订户名称、证件号码、域名或 IP 地址、邮箱、联系人、联系地址等信息。

3、证书生命周期中的各项操作，包括证书申请、证书密钥更新、证书吊销等事件；

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

5、人员访问控制记录；

6、系统巡检记录。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

5.4.2 处理日志的周期

CFCA 每日对全球信任体系认证系统各服务器上的系统日志、数据库日志和相关业务日志进行转存，一份保存在本地的硬盘中，同时还上传一份至集中备份服务器。

在需要归档时，采用刻光盘形式对 CA 和 RA 日志进行归档，每季度刻一次光盘，归档保存期限为 5 年。

5.4.3 审计日志的保存期限

密钥和证书信息档案至少保存到证书失效后 5 年。

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 每天进行一次数据备份操作。

5.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

5.4.7 对导致事件主体的通告

对于审计收集系统中记录的事件，对导致该事件的个人、机构等主体，CFCA 不进行通告。

5.4.8 脆弱性评估

根据审计记录，CFCA 定期进行系统、物理设施、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

5.5 记录归档

5.5.1 归档记录的类型

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

1、 与证书订户的协议、订户证书、CRL 等；

2、 电子认证业务规则、证书策略、管理制度等；

3、 员工资料，包括员工信息、背景调查、培训、录用离职等资料；

4、 各类外部、内部审查评估文档。

5.5.2 归档记录的保存期限

CFCA 将对过期的或者吊销了的订户证书进行归档，归档记录将会保存至少 5 年以上；其他信息归档期至少为 5 年。如果法律需要，CFCA 将延长记录保存期限。

CRL 文件采用刻光盘的形式进行归档，每月刻一次光盘，归档时间为 5 年。

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：每季度进行一次备份，或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。每月刻光盘进行备份。

5.5.5 记录的时间戳要求

归档的记录都需要标注时间；系统产生的记录按照要求添加时间标识。

5.5.6 归档收集系统

CFCA 有自动的电子归档信息的存放系统。

5.5.7 获得和检验归档信息的程序

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

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。

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。在生成CA密钥对时，三名具有密钥管理及操作权限的人员必须同时到达CFCA最安全区同时进行操作，任何人无法独立完成。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的签名私钥在加密机内部产生，RA证书由CFCA签发。

3、订户密钥的生成

订户的密钥对由订户在服务器上使用相应的软件产生，订户应确保其密钥产生软件的可靠性，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。

CFCA有义务指导订户按照正确的流程生成密钥，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

订户的私钥无论是由订户自己生成还是订户申请由 CFCA 代为生成，均只会在订户端的服务器中进行，订户私钥不会离开生成该私钥的服务器设备，不会进行传送。

6.1.3 公钥传送给证书签发机构

订户在其服务器设备上生成密钥对后，应当将包含公钥信息的证书签名请求文件（CSR）通过电子邮件的形式发送给 CFCA。

6.1.4 电子认证服务机构公钥传送给依赖方

用于验证 CFCA 签名的验证公钥（证书链）可从 CFCA 的信息库获得。

6.1.5 密钥的长度

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

CFCA 用于签名的密钥长度为 2048 位；

RA 密钥的长度为 2048 位；

订户密钥的长度为 2048 位。

6.1.6 公钥参数的生成和质量检查

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

6.1.7 密钥使用目的

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

订户的密钥对可用于安全服务，例如身份认证、建立安全通道等。

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 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 512、768、1024、2048 比特；支持 SDBI、DES、TRIPLE-DES、IDEA、RC2、RC4、RC5、SM1 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 全球信任体系使用的加密机其公钥算法为 RSA、SM2，RSA 模长为 2048 比特，HASH 算法为 SHA1、SHA256，具有国家密码主管部门颁发的产品资质证书。

6.2.2 私钥多人控制（m 选 n）

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

6.2.3 私钥托管

对于 CA 私钥,CFCA 无托管业务。

6.2.4 私钥备份

CA 的私钥由加密机产生，加密机有双重备份，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 5 年。归档的 CA 密钥对保存在本 CPS6.2.1 所述的硬件密码模块中，并且 CFCA 的密钥管理策略和流程都确保了归档后的 CA 密钥对不会再被用于生产系统中。当归档 CA 密钥对达到归档保存期限之后，CFCA 将按照本 CPS6.2.10 所述的方法进行安全地销毁。

CFCA 不对订户的私钥进行归档。

6.2.6 私钥导入、导出密码模块

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

6.2.7 私钥在密码模块的存储

私钥以密文的方式分段加密存放在硬件加密模块中。

6.2.8 激活私钥的方法

1、激活订户私钥

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

码模块验证口令完成后，私钥被激活。

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

2、激活 CA 私钥

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

6.2.9 解除私钥激活状态的方法

对于订户私钥，当服务程序被停止、系统注销或系统断电后私钥进入非激活状态。

对于 CA 私钥，当硬件密码模块断电、重新初始化时，私钥进入非激活状态。

6.2.10 销毁私钥的方法

当 CA 的生命周期结束后，CFCA 将根据本 CPS 6.2.5 之相关规定将 CA 私钥进行归档，其它的 CA 私钥备份将被安全销毁。归档的私钥在其归档期结束后，需要在 3 名以上可信人员参与下进行安全地销毁。

订户根据实际情况自行保存并销毁私钥。

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 证书的有效期为 15 年，CFCA 能够发放的订户证书有效期为 1-5 年。订户可根据实际情况申请有效期在 5 年以内的证书。

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

6.4 激活数据

6.4.1 激活数据的产生和安装

1、 CFCA 的 CA 私钥产生遵循本 CPS6.2.2 中的要求。

2、 对于订户，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 6 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 IC 卡和加密设备，通常被保存在 CFCA 最安全区机房，不能携带离开 CFCA。如在某种特殊情况下需要进行传输时（如建设灾备系统时），其传送过程需要在 CFCA 安全管理人员和密钥管理人员共同监督的情况下进行。

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

6.4.3.2 激活数据的销毁

CFCA 通过对设备初始化的方式来销毁 CA 私钥的激活数据。

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

6.5 计算机安全控制

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

6.5.1 特别的计算机安全技术要求

CFCA 的信息安全管理符合国家相关规定，主要安全技术和控制措施包括：采用安全可信任的操作系统、严格的身份识别和人员访问控制制度、多层防火墙设置、人员职责分割、内部操作控制、业务持续计划等各方面。

6.5.2 计算机安全评估

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。

6.6 生命周期技术控制

6.6.1 系统开发控制

CFCA 的系统由符合国家相关安全标准和具有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。

6.6.2 安全管理控制

CFCA 认证服务系统的信息安全管理，严格遵循行业主管部门的规范进行操作，系统的任何变更都经过严格的测试验证后才能进行安装和使用。同时，按照 ISO9000 质量管理体系标准建立了严格的管理制度。对于核心数据（CA 数据、

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

6.6.3 生命期的安全控制

CFCA 的系统由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。

6.7 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。

6.8 时间信息

证书、CRL、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

7.1.1 版本号

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

7.1.2 证书扩展项

X.509 V3 证书的扩充部分主要包括:

7.1.2.1 颁发机构密钥标识符

CFCA 全球服务器证书及中级 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。

该密钥标识符项由 BIT STRING subjectPublicKey 值的 160-bit SHA-1 散列值组成(去掉标签、长度和若干不使用的字节)。该扩展项为非关键项。

7.1.2.2 主题密钥标识符

全球服务器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，该扩展项为非关键项。

CFCA 发放的全球服务器证书密钥用法包括：数字签名（digitalSignature），不可否认(nonRepudiation)，密钥加密(keyEncipherment)，数据加密(dataEncipherment)，密钥协商(keyAgreement)。

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。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。

全球服务器证书中此项的定义为“服务器验证 =1.3.6.1.5.5.7.3.1”，表明该证书用于 Web server 鉴别。该扩展项为非关键项。

7.1.2.6 CRL 分布点

系统签发的证书包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL。该扩展项为非关键项。

7.1.2.7 主题备用名称

主题备用名称包含一个或多个可选替换名（可使用多种名称形式中的任一个）供实体使用，CA 把该实体与认证的公开密钥绑定在一起。该扩展项的使用符合 RFC3280 之规定,为非关键项。

7.1.3 算法对象标识符

CFCA签发的全球服务器证书符合RFC 3280标准，采用SHA-1 RSA算法签名。

7.1.4 名称形式

CFCA 全球信任体系下签发的证书为全球服务器证书，采用 X.500 定义的甄别名称（DN）标准来唯一标识证书的相关信息。DN 必须包括以下四部分：

1、 CN 部分：

CN 部分为网站域名或 IP 地址信息。

2、 OU 部分：用于表示 CFCA 全球信任服务器证书的名称简称：

OU=GTC （为 Global Trust Certificate 的缩写）

3、 O 部分：用于表示证书申请者的真实名称，如：

O=北京金科信安科技有限公司

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

订户在申请证书前，应严格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。

7.1.5 名称限制

CFCA 全球信任体系下签发的证书，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。

7.1.6 证书策略对象标识符

证书策略对象标识符为 2.16.156.112554.2。

7.1.7 策略限制扩展项的用法

未使用本扩展域。

7.1.8 策略限定符的语法和语义

未使用本扩展域。

7.1.9 关键证书策略扩展项的处理规则

未使用本扩展域。

7.2 CRL

7.2.1 版本号

CFCA 目前使用的是 X.509 V2 版本的 CRL。

7.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义如下：

1、版本（Version）

显示 CRL 的版本号。

2、CRL 的签发者（Issuer）

指明签发 CRL 的 CA 的甄别名。

3、CRL 发布时间（this Update）

4、预计下一个 CRL 更新时间(next update)

5、签名算法

6、列出吊销的证书，包括吊销证书的序列号和吊销日期。

7.3 在线证书状态协议

目前不提供此项服务。

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。

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。

8.2 评估者的资质

若需邀请外部审计机构对 CFCA 进行评估，CFCA 将选择熟悉 IT 运营管理、具有多年审计经验的审计机构对 CFCA 的运营管理进行一致性审计。在进行审计前，审计机构必须熟悉公钥基础设施技术及相关的法律法规、标准规范要求。

8.3 评估者与被评估者的关系

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

8.4 评估内容

评估的内容包括但不限于以下方面：

1、CA 物理环境和控制

2、密钥管理操作

3、基础 CA 控制

4、证书生命周期管理

5、CA 业务规则

8.5 对问题与不足采取的措施

CFCA 管理层将对审计报告进行评估，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。

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

当订户向 CFCA 订购全球服务器证书时，CFCA 将会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，非经订户同意或有关法律法规、公共权力部门根据合法的程序要求，不会任意公开。

9.4.3 不被视作隐私的信息

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

9.4.4 保护隐私的责任

CFCA、订户、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。

9.6.2 注册机构的陈述与担保

CFCA 同时承担注册机构的职责，负责审核申请人的身份并决定接受或拒绝申请人申请、负责在 RA 系统中录入订户信息，并将证书申请信息安全地传送到 CA 系统。

CFCA 作为注册机构的声明和承诺为：

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

2、 如 CFCA 对订户的证书申请材料审查没有通过，CFCA 有向订户进行告知的义务，如证书申请被批准，CFCA 有义务通知订户并且指导订户得到证书；

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

5、 证书签发及被吊销时及时通知订户。

6、 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；

7、 通知订户阅读 CFCA 发布的 CPS 和其他相关规定，在订户完全知晓并同意 CPS 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。

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。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，造成的损失由订户自己承担。

订户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；订户应当妥善保管 CFCA 签发的数字证书的私钥和密码，不得泄漏或交付他人。

如因故意或过失导致他人知道、盗用、冒用数字证书私钥和密码时，订户应承担由此产生的责任。

如订户使用的数字证书私钥和密码泄漏、丢失，或者订户不希望继续使用数字证书时，或者订户主体不存在，订户或法定权利人应当立即到原注册机构申请废止该数字证书，相关手续遵循本 CPS 的规定。

订户应将证书用于合法目的并符合本 CPS。

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，在这些信息变更时未及时通知 CFCA；

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

3） 订户有其他过错或未履行双方约定。

订户有按期缴纳数字证书服务费的义务，费用标准请咨询 CFCA 市场部。

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

其他参与者应遵循本 CPS 的规定。

9.7 担保免责

1、证书申请人或订户故意提供或未按照要求提供不准确和/或不真实和/或不完整的信息而获得 CFCA 签发的证书，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、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。

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

9.9.1 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 不向订户和/或依赖方承担任何赔偿和/或补偿责任。

9.9.2 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。

9.9.3 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）订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、或失去或无法使用任何数据、设备或软件；

（2）由上述损失相应生成或附带引起的损失或损害；

9.9.4 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。

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

争议处理流程为：

1、 争议解决的通知：

当争议发生时，在采取任何解决途径之前，订户应首先通知 CFCA。

2、 争议解决的方式：

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

3、 正式争议解决：

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

4、 索赔时限

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

9.14 管辖法律

CFCA CPS 和协议中条款的制定遵守《中华人民共和国合同法》和《中华人民共和国电子签名法》及相关法律规定。如 CPS 中某项条款与上述法律条款或其可执行性发生抵触，CFCA 将会对此条款进行修改，使之符合相关法律规定。

9.15 与适用法律的符合性

CFCA的各项策略均遵守并符合中华人民共和国各项法律法规和国家信息安全主管部门要求。若本CPS的某一条款被主管部门宣布为非法、不可执行或无效

时，CFCA将对该不符合性条款进行修改，直至该条款合法和可执行为止。本CPS某一个条款的不可执行性不会导致其它条款的不可执行性。

9.16 一般条款

9.16.1 本 CPS 的完整性

本 CPS 将替代所有以前的或同时期的、与相同主题相关的书面或口头解释。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、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

无。

附录 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。