中国金融认证中心（CFCA）
预植证书策略（CP1）

V1.0

2009 年 5 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的 CA 之一。

证书策略（CP，Certification Policy）是关于认证机构（CA，Certification Authority）制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

本证书策略的适用范围为 CFCA 发放的预植证书，此处的预植证书是指由 CFCA 按照本 CP7.1.4 的规则定义证书 DN 后，预先在安全的存储介质（如 USBKey）中生成并植入的数字证书；订户申领该证书时，发证机构须对订户的身份进行审核，将证书的 DN 信息与订户的身份信息绑定，并与应用系统进行关联。当预植证书与订户身份信息的绑定信息经发证机构和 CFCA 数字签名确认后，该预植证书方可生效。

此处的绑定是指将证书的 DN 信息与订户的身份信息（包括但不限于姓名、证件类型、证件号码）在数据库中建立对应的关系，以便使该证书对应确定的实体。

此外的关联是指将证书的 DN 信息与应用系统的信息（包括但不限于发证机构名称、应用系统类型等）在数据库中建立对应的关系，以便使该证书用于特定的应用当中。

1.2 文档名称与标识

本文档的名称为《CFCA 预植证书策略（CP1）》（“CP”），已注册的对象标识符（OID）为 1.3.6.1.4.1.14433.0。

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、发证机构、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

在预植证书业务中，制证系统设在 CFCA 处，CFCA 按照本 CP7.1.4 的规则定义证书 DN 后，预先在安全的存储介质（如 USBKey）中生成并植入证书，且承担证书查询、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 发证机构

在预植证书业务中，预植后的证书发放给订户的工作由发证机构承担。发证机构须对订户提交的资料进行审核，以决定是否为该订户发放证书；并须将证书 DN 信息与订户的身份信息进行绑定，并与应用系统进行关联后，该证书方可被有效使用。

在成为 CFCA 预植证书的发证机构之前，发证机构须与 CFCA 签署《预植数字证书合作协议》，承担相应的权利和义务。

1.3.3 证书种类与订户

本证书策略的适用范围为 CFCA 发放的预植证书。

订户指使用 CFCA 预植证书的所有终端订户，包括企业和个人。在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方是指基于对电子签名预植证书或者电子签名的信赖从事有关活动的人。依赖方可以是、也可以不是订户。

1.3.5 其它参与者

在预植证书业务中除了电子认证服务机构（CFCA）、发证机构、订户和依赖方以外的参与者称为其它参与者。

1.4 证书应用

1.4.1 适合的证书应用

在证书的 DN 信息与订户的身份信息绑定、并与应用系统关联后，预植证书方能根据应用

系统的要求用于不同的应用领域。

CFCA 预植证书的订户包括企业和个人，例如：

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

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

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

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

1.4.2 限制的证书应用

在证书的 DN 信息与订户的身份信息绑定、并与应用系统关联前，预植证书不能被有效使用。

此外，CFCA 的数字证书不能在如下方面使用：

1、任何与国家或地方法律、法规规定相违背的应用系统；

2、CFCA 不认可的证书应用系统。

1.5 策略管理

1.5.1 策略文档管理机构

本 CP 的制定与修订由 CFCA 业务部负责。业务部组成“CP 编写组”，办公室、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“CP 编写组”，并指定编写组负责人。

1.5.2 联系方式

如对本 CP 有任何疑问，请联系：

部门：业务部

电话：010-83526220

传真：010-63555032

邮件：zhaoyu@cfca.com.cn

地址：中国北京宣武区右安门内新安南里甲 1 号

1.5.3 决定 CP 符合策略的机构

总经理审批同意后，方可对外发布 CP。发布形式应符合行业主管部门等相关主管部门的要求。

1.5.4 CP 批准程序

“CP 编写组”负责起草或修订 CP 形成讨论稿（或 CP 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。

“CP 编写组”负责将 CP 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，“CP 编写组”将经法律顾问审阅过的 CP 送审稿连同法律顾问的意见书提交业务部，由业务部确定 CP 文本格式和版本号，形成定稿。

CP 定稿经业务部分管领导审阅后，报总经理审批。总经理审批同意后方可对外发布。发布形式应符合行业主管部门等相关主管部门要求，包括但不限于网站公布和向客户或合作对象书面提交。发布工作由业务部协调相关部门完成，并将 CP 电子版及法律顾问的意见书交办公室存档。

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

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 预植证书信息库包括但不限于以下内容：证书、CRL、OCSP、预植证书管理平台、CPS、CP、预植证书服务协议、技术支持手册、CFCA 网站信息以及 CFCA 不定期发布的信息。CFCA 信息库不会对从 CFCA 发出的任何证书和证书吊销信息进行修改，而只会准确地描述上述内容。

2.2 认证信息的发布

证书状态可以通过预植证书管理平台，OCSP、CRL 获得。

CPS、CP、预植证书服务协议、技术支持手册等信息可从 CFCA 网站（http://www.cfca.com.cn）上获得。

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；预植证书状态信息实时发布到 OCSP 中；预植证书的吊销信息将在证书吊销后一小时内更新信息库，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 的预植证书采用 X.500 定义的甄别名称（DN）标准来唯一标识一个安全的存储介质

（如 USBKey），DN 的详细规则定义见本 CP 的 7.1.4。

3.1.2 对名称意义化的要求

DN（Distinguished Name）：唯一甄别名，在数字证书的主体名称域中，用来唯一标识一个安全的存储介质（如 USBKey）。

DN 的定义有特定的规则，并具有特定的意义，见本 CP7.1.4。

3.1.3 订户的匿名或伪名

无。

3.1.4 解释不同名称形式的规则

DN 的命名规则由 CFCA 定义，详见本 CP 7.1.4 的说明。

3.1.5 名称的唯一性

CFCA 保证其签发的证书，其主题甄别名，在 CFCA 的信任域内是唯一的。

3.1.6 商标的识别、鉴别和角色

无。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

在预植证书业务中,CFCA 制订了严格的管理流程,从技术与制度上保证了在生成证书时，与此张证书相对应的私钥只留存在安全的存储介质中，不会留存任何备份。当订户申领证书时，发证机构须对其身份进行审核，并将证书的 DN 信息与订户的身份信息进行绑定，并与应用系统进行关联后，此证书才能被订户有效使用。此时，订户是其签名私钥的唯一持有者。CFCA 要求订户妥善保管自己的签名私钥。

3.2.2 组织机构身份的鉴别

组织机构订户在申领证书前或在其它发证机构绑定新的应用前应指定并授权证书的申领代表，接受证书申领的有关条款，承担相应的责任。鉴别组织机构的身份时，指定证书申领者须向发证机构审核人员提供有效证明文件，在填写申领表时加盖企业公章以证明该申领的有效性。CFCA 授权的发证机构将复核并验证申领文件的真实性，并进行批准申领或拒绝申领的操作。

3.2.3 个人身份的鉴别

个人订户在申领证书前或在其它发证机构绑定新的应用前应持个人有效身份证件，包括：身份证、军官证、士兵证、护照、武装警察身份证、户口本、港澳居民往来内地通行证、台湾居民往来内地通行证等（以上可任择其一），提出证书申领，并接受证书申领的有关条款，承担相应的责任。CFCA 授权的发证机构将复核并验证申领文件的真实性，并进行批准申领或拒绝申领的操作。

3.2.4 没有验证的订户信息

无。

3.2.5 授权确认

当申请者代表个人或组织机构申请证书时，需要出示足够的证明信息以证明个人或组织机构是否真实存在，申请者是否已获得个人或组织机构的授权。CFCA 或发证机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.6 互操作准则

订户在某个发证机构申领了 CFCA 签发的预植证书后，也可至 CFCA 授权的其它发证机构进行新的注册过程，将原有的证书与新的应用系统进行关联后，可实现一张证书在不同发证机构应用系统中的应用。

3.3 密钥更新请求的标识与鉴别

订户证书到期后，订户需对原有证书进行更新。在更新时产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。在密钥更新时，证书的 DN 未改变。

若为一个现存的加密密钥对申请一个新证书，则称为“证书更新”。

3.3.1 常规密钥更新的标识与鉴别

常规密钥更新的流程详见本 CP 的 4.7。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新等同于订户重新申请证书，订户证书吊销后的密钥更新处理流程见本 CP 的 4.2。

3.4 吊销请求的标识与鉴别

证书吊销请求的标识与鉴别流程见本 CP 的 4.9.3。

4 证书生命周期操作要求

4.1 证书申领

4.1.1 证书申领实体

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

个人证书由证书使用者本人提出申请；企业证书由企业、组织机构授权的人员申请。

4.1.2 注册过程与责任

1、最终订户

最终订户须明确表示其愿意接受订户协议中所规定的相关责任与义务（订户协议公布在 CFCA 网站上），并需要提供真实、准确的申请信息；

2、发证机构

发证机构须与 CFCA 签订《预植数字证书合作协议》。

在预植证书业务中，发证机构须对订户提交的资料进行审核，以决定是否为该订户发放证书；并须将证书的 DN 信息与订户的身份信息进行绑定、与应用系统进行关联后，此证书方可被有效使用。

4.2 证书申领处理

4.2.1 执行识别与鉴别功能

证书申领者向发证机构提交初始的证书申领请求，以及申请将证书关联新的应用时，发证机构须按照以下规定对订户的申领材料进行审查:

机构订户：参照 3.2.2 节的规定。

个人订户：参照 3.2.3 节的规定。

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

4.2.2 证书申领批准和拒绝

发证机构对证书申领者提交的申领信息及身份信息进行鉴别，鉴别其是否完整、真实、有效。经鉴别符合要求后，将批准申领。如果申领者未能通过审核，发证机构将拒绝申领者的申领，并通知申领者。

4.2.3 处理证书申领的时间

CFCA 及发证机构将在合理的时间内完成证书申领处理。在申领者提交的资料齐全且符合要求的情况下，处理证书申领的时间不超过 5 个工作日。

4.3 证书签发

4.3.1 证书签发中发证机构和电子认证服务机构的行为

CA 机构按照本 CP7.1.4 的规则定义证书 DN 后，预先在安全的存储介质（如 USBKey）中生成并植入证书。CFCA 制订了严格的管理流程，从技术与制度上保证了在生成证书时，与此张证书相对应的私钥只留存在安全的存储介质中，CFCA 不会留存任何备份。

当订户申领证书时，发证机构需对订户的身份进行审核，审核通过后将订户的身份信息与证书的 DN 信息进行绑定、与应用系统进行关联后，并对绑定和关联后的信息进行数字签名后通过安全的通道传送至 CFCA，CFCA 校验银行签名，记录用户信息和关联信息，并对银行签名信息和时间信息进行数字签名后保存。

4.3.2 电子认证服务机构和发证机构对订户的通告

CFCA 签发证书后，由于该证书尚未与订户身份进行绑定，还无法进行应用，因此 CFCA 对于其签发的证书不会对订户进行通告。

发证机构在审核订户身份后，无论是拒绝还是批准订户的证书申请，发证机构有义务告知订户申请结果。

4.4 证书接受

4.4.1 构成接受证书的行为

当订户填写证书申请表，并提供真实、准确的身份信息经发证机构审核通过，并同意《预植数字证书服务协议》的约定，申领到预植证书后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 在签发预植证书的同时会将该证书发布到公开的信息库和指定的数据库中。在绑定身份、关联应用后会将该信息记录在指定的数据库中，并通过安全的机制向依赖方提供查询服务。

4.4.3 电子认证服务机构对其他实体的通告

证书与证书状态信息向其它实体进行通告。

证书关联的应用信息与绑定的身份信息不对其它实体进行通告。

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 CP1.4 中定义）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《预植数字证书服务协议》及 CFCA CPS 和本 CP 的要求；

3、 订户应当妥善保存其私钥和证书，避免他人未经本人授权而使用本人证书情形的发生。

4.5.2 依赖方公钥和证书的使用

在依赖方接受数字签名信息后需要：

1、 获得数字签名对应的证书及信任链；

2、 确认该签名对应的证书是依赖方信任的证书；

3、 证书的用途适用于对应的签名；

4、 使用证书上的公钥验证签名；

5、 确认数字签名对应的证书状态正常，没有进入 CRL 列表。

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

4.6 证书更新

证书更新是指订户在不改变现有加密密钥的情况下申请一张新证书。目前只对高级证书提供该项服务。

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

证书更新的规定与证书密钥更新的相同。

4.7 证书密钥更新

证书密钥更新是指订户需要生成新密钥并申请为新公钥签发新证书。

4.7.1 证书密钥更新的情形

当订户证书即将到期或已经到期时应当进行证书密钥更新。

4.7.2 请求证书密钥更新的实体

个人证书由证书使用者本人提出申请；企业证书由企业、组织机构授权的人员申请。

4.7.3 证书密钥更新请求的处理

(一)在证书到期之前，订户既可以自行登录 CFCA 提供的预植证书管理平台进行密钥更新，也可以向发证机构提交密钥更新申请。

订户自行登录 CFCA 提供的预植证书管理平台进行密钥更新时，须利用原始证书登录该平台，通过验证后方可进行密钥更新。

订户向发证机构提交密钥更新申请时，发证机构对以下申请材料进行审查:

机构订户：参照 3.2.2 节的规定。

个人订户：参照 3.2.3 节的规定。

审查通过后，发证机构进行密钥更新，并将装有已更新证书的存储介质返还给订户。

（二）在证书到期之后，订户只能向发证机构提交密钥更新申请进行密钥更新，密钥更新请求的处理同上。

4.7.4 颁发更新证书时对订户的通告

订户通过预植证书管理平台更新证书密钥时，订户更新密钥后即可使用新证书，无须 CFCA 对订户进行通告。

订户向发证机构提出密钥更新申请时，发证机构在审核订户身份后，无论是拒绝还是批准订户的密钥更新申请，均有义务告知订户申请结果。

4.7.5 构成接受密钥更新证书的行为

当订户使用原有的证书登录预植证书管理平台，通过验证并完成密钥更新后即构成接受更新密钥的行为；或当订户向发证机构提出证书更新请求，并提供真实、准确的身份信息经发证机构审核通过，发证机构将更新后的证书交还给订户，亦视为订户接受更新证书密钥的行为。

4.7.6 电子认证服务机构对密钥更新证书的发布

密钥更新后的证书会在更新的同时被 CA 机构发布到公开的信息库和指定的数据库中。

4.7.7 电子认证服务机构对其他实体的通告

密钥更新后的证书会在更新的同时被 CA 机构发布到公开的信息库和指定的数据库中，订户和依赖方可以在信息库上自行查询。

此外,CFCA 也会将密钥更新后的证书状态信息向订户进行过新应用绑定的其它发证机构进行通告。

4.8 证书变更

无。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被吊销：

1)订户申领预植证书时，提供的资料不真实；

2)订户未履行证书服务协议约定的义务；

3)订户书面申请吊销数字证书；

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，忘记或泄漏了证书使用口令，存放证书的介质损坏或被锁定等；

5)法律、行政法规规定的其他情况。

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，由发证机构审核通

过后吊销证书的情形；被动吊销是指当发证机构或 CA 确认订户违反证书应用规定、约定或订户主体已经消亡等情况发生时，采取吊销证书的手段以停止对该证书的证明。当出现上述提到的第 1、2 种情况时，适用于被动吊销，第 3 种情况适用于主动吊销，第 4、5 种情况则既可能出现被动吊销，也可能出现主动吊销。

4.9.2 请求证书吊销的实体

在符合本 CP4.9.1 所述的情形下，请求证书吊销的实体与本 CP4.1.1 证书申请实体相同。另外，发证机构或 CFCA 也可以在本 CP4.9.1 所述的情形下主动吊销订户的证书。

4.9.3 请求吊销的流程

最终订户吊销证书时可按以下流程进行：

1) 订户（或其授权委托人）填写书面申请表并签名或盖章，同时提交相应的证明材料，向发证机构或关联过新应用的发证机构提出吊销证书请求。
2) 接到吊销申请的发证机构，验证申请者身份及吊销理由的正当性，并对审核资料进行归档保存。
3) 发证机构在验证吊销申请后吊销证书。
4) CFCA 及时将证书吊销信息发布到 CFCA 信息库中，并且吊销信息会及时通知关联过应用的发证机构。

4.9.4 吊销请求宽限期

订户一旦发现需要吊销证书，应及时向发放该证书的发证机构或关联过新应用的发证机构提出吊销请求。

4.9.5 电子认证服务机构处理吊销请求的时限

CFCA 或其授权的证书发证机构从收到吊销请求并审核完成后，会立即将证书吊销。

说明：订户在正式提出证书吊销申请后不得在交易中继续使用此证书，否则由此产生的后果，由订户自行承担。

4.9.6 依赖方检查证书吊销的要求

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

4.9.7 CRL 发布频率

CRL 发布频率为 1 小时一次，在发布的同时对原有内容进行更新。

4.9.8 CRL 发布的最大滞后时间

CFCA 在生成 CRL 的 1 小时后会更新信息库。

4.9.9 在线的吊销/状态查询的可用性

CFCA 提供在线的吊销/状态查询，该服务 7X24 小时可用。

4.9.10 在线的吊销查询要求

依赖方在信赖一张证书前须确定证书的状态，查询方式为检查 CRL 或 OCSP，CFCA 没有设置任何读取权限。

4.9.11 吊销信息的其他发布形式

除 CRL 与 OCSP 之外，尚无其它发布形式。

4.9.12 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，应及时地提出证书吊销请求。

4.9.13 证书挂起

CFCA对于预植证书目前无此业务。

4.10 证书状态服务

4.10.1 操作特征

证书状态可以通过预植证书管理平台，OCSP、LDAP 的目录查询服务获得。

4.10.2 服务可用性

CFCA 提供 7X24 小时不间断证书状态查询服务。

4.11 订购结束

以下三种情形将被视为订购结束：

1、 证书到期后即视为订购结束。

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

3、 被动吊销视为订购结束。

4.12 密钥生成、备份与恢复

在预植证书业务中,CFCA 制订了严格的管理流程,从技术与制度上保证了在生成证书时，与此张证书相对应的私钥在存储介质中生成且只留存在存储介质中，不会留存任何备份。

5 认证机构设施、管理和操作控制

证书预植操作被放置在 CFCA 机房中的单独区域中，具有物理三层保护。

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。

所有访问均有日志记录，并做到全程可审计。

其余要求均与 CPS 相同。

6 认证系统技术安全控制

本章规定参见 CPS。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 版本号

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

7.1.2 证书扩展项

X.509 V3 证书的扩充部分主要包括:

7.1.2.1 颁发机构密钥标识符

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

7.1.2.2 主题密钥标识符

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

7.1.2.3 密钥用法

密钥用法指明已认证的公开密钥用于何种用途，该项定义遵照 RFC3280 之规定。

7.1.2.4 Basic constraints:基本限制

基本限制项用来标识证书的主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长，该项定义遵照 RFC3280 之规定。

7.1.2.5 CRL 分布点

系统签发的证书包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL。该扩展项的 criticality 项设为 FALSE。

7.1.2.6 主题备用名称

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

7.1.3 算法对象标识符

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

7.1.4 名称形式

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

(1) CN

CN 部分包括 16 个字符，由数字和字母组成，字母区分大小写：

前 6 位由各发证机构自行定义；

后 9 位的首位用于区分证书类型，若为“9”开头则表示是企业证书，其余数字开头则表示是个人证书，后 8 位表示各发证机构发放的证书数量，按照各发证机构发放证书的顺序，逐渐累加；

最后 1 位为随机产生的校验码。

示例：CN=95561e9000001925，CN=1001010000152453

(2) OU[2]

OU[2]部分，用来表示证书类型。详细命名规则如下表：

	个人 普通证书	个人 高级证书	企业 普通证书	企业高级证书
OU=	Customers	Business Customers	Enterprises	Units

注：代表证书类型中的每个英文单词，第一个字母大写，其余小写。

(3) OU[1]

OU[1]部分用来表示此证书为预制证书的类型，具体表示为：

OU[1]＝yuzhi

(4) O

O 部分：用来表示 CA 系统的英文简称，表示为：

O=CFCA Operation CA2

(5) C

C 部分用来表示中国的英文简称，全部大写。

C=CN

7.1.5 名称限制

CFCA 签发的预植证书，其名称须严格按照 7.1.4 的规则来定义。

7.1.6 证书策略对象标识符

已注册的对象标识符（OID）为 1.3.6.1.4.1.14433.0。

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

同 CPS。

7.3 在线证书状态协议

同 CPS。

8 认证机构审计和其它评估

同 CPS。

9 法律责任和其他业务条款

9.1 费用

同 CPS。

9.2 财务责任

同 CPS。

9.3 业务信息保密

同 CPS。

9.4 个人信息私密性

同 CPS。

9.5 知识产权

同 CPS。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

1、 CFCA 确保预植证书私钥是唯一的。

2、 当预植证书与订户身份信息的绑定经发证机构和 CFCA 数字签名确认后，该预植证书即可生效。

3、 CFCA 向发证机构提供预植证书绑定信息的查询。

4、 CFCA依法制定和修订《电子认证业务规则》(简称CPS)、《预植证书策略》(简称CP)，并公布于CFCA网站（www.cfca.com.cn)，明确CFCA预植证书的功能、使用证书、各方的权利、义务以及CFCA的责任范围，前述CPS及本CP自通过CFCA网站（www.cfca.com.cn）公布之日起对发证机构、订户及依赖方具有法律约束力，但本CP第 9.12.2 款除外。

5、 CFCA 为订户提供 7X24 小时热线支持服务（4008809888)，5 X 8 小时服务监督电话（010-83519756)，CFCA 将在 1 个工作日内对订户的意见和建议做出响应。

6、 在订户通过数字证书对交易信息进行加密和签名的条件下，CFCA 保证交易信息的保密性和完整性。如果发生纠纷，CFCA 将依据不同情况承担下述义务：

1）提供签发数字证书的 CA 证书。

2）提供数字证书在交易发生时，在或不在 CFCA 发布的数字证书废止列表内的证明。

3）提供数字证书在交易发生时，是否与该订户信息绑定的证明。

4）对数字证书及绑定、数字签名、时间戳的真实性、有效性进行技术确认。

7、 对于下列情况之一，CFCA 有权吊销所签发的数字证书：

1) 订户申领预植证书时，提供的资料不真实；

2) 订户未履行本 CP 约定的义务或者订户违反本 CP 中所做的陈述和/或保证的；

3) 订户书面申请吊销数字证书；

4) 证书的安全性不能得到保证；

5) 法律、行政法规及规章等规范性法律文件规定的其他情况。

8、 CFCA 不保证订户与依赖方所从事的具体民事活动的真实性、合法性，也不保证相关协议能否履行或能否实现有关方的交易目的。

9.6.2 发证机构的陈述与担保及义务

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，通过审查确保预植证书与确定的实体进行绑定，并将与预植证书绑定的用户身份信息进行数字签名后传送至 CFCA；

2、 发证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订户使用；

3、 如发证机构对订户的证书申请材料审查没有通过，发证机构有向订户进行告知的义务；

4、 发证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不超过 5 个工作日；

5、 发证机构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；

6、 发证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；

7、 发证机构有义务通知订户阅读 CFCA 发布的 CP、CPS 和《预植证书服务协议》以及其它相关规定，在订户完全知晓并同意 CP、CPS 和《预植证书服务协议》内容的前提下，为订户办理数字证书。

9.6.3 订户的陈述与担保及义务

1、 订户应遵循诚实、信用原则，申领预植证书时，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发证机构。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，造成的损失由订户自己承担。

2、 订户须使用经合法途径获得的相关软件。

3、 订户应合法使用 CFCA 数字证书，并对使用数字证书的行为负责。

4、 订户应当妥善保管含有预植证书的 USBKey。如因故意或过失导致他人盗用、冒用预植证书时，订户应承担由此产生的责任。

5、 如订户使用的预植证书的 USBKey 丢失或密码泄漏，或者订户不希望继续使用数字证书，或者订户主体不存在，订户或法定权利人应当立即申请吊销该数字证书。

6、 订户应在发证机构或指定网站进行证书更换或展期。

7、 订户通过本 CP 进行的任何行为（“该行为”）应当符合法律及任何行政法律和规章等规范性法律文件的规定，CFCA 对该行为不承担任何法律责任。

9.6.4 依赖方的陈述与担保及义务

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 CFCA 的 CPS 及本 CP 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、本 CP 中关于 CFCA 责任限制的规定；

6、依赖方依赖本 CP 进行的任何行为（“该行为”）应当符合法律及任何行政法律和规章等规范性法律文件的规定，CFCA 对该行为不承担任何法律责任。

9.6.5 其它参与者的陈述与担保

其他参与者应遵循本 CP 的规定。

9.7 免责条款

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 签发的预植证书，订户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订户造成的损失，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。

9.8 有限责任

CFCA 依据本 CP 承担的赔偿责任是有限的。

9.9 CFCA 承担的赔偿责任的限制

9.8.1 除非有另外的规定或约定,对于非因本CP项下的认证服务而导致的任何损失,CFCA 不向订户和/或依赖方承担任何赔偿和/或补偿责任。

9.8.2 订户或依赖方进行的民事活动因 CFCA 提供的认证服务而遭受的损失，CFCA 将依据本 CP 的相关条款给予赔偿。但无论如何，如果 CFCA 能够证明其提供的服务是按照《电

子签名法》、《电子认证服务管理办法》、CFCA 向主管部门备案的 CPS 和本预植证书 CP 实施的，则不视为 CFCA 具有任何过错，也不对订户或依赖方承担任何赔偿或补偿责任。

9.8.3 无论本 CP 是否有相反或不同规定，就以下损失或损害，CFCA 不承担任何赔偿和/或补偿责任：

（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；

9.8.4 无论本 CP 是否有相反或不同规定，如果 CFCA 根据本 CP 或任何法律规定须承担赔偿和/或补偿责任的，CFCA 对预植的企业数字证书订户及其依赖方的赔偿上限总共为人民币伍拾万元整，即￥500,000.00 元；CFCA 对预植的个人数字证书订户及其依赖方的赔偿上限总共为人民币贰万元整，即￥20,000.00 元。

9.10 有效期限与终止

9.10.1 生效及有效期限

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

9.10.2 终止

CFCA 有权终止本 CP（包括其修订版本），本 CP（包括其修订版本）自 CFCA 在其官方网站公布终止声明的 30 日后终止。

9.10.3 效力的终止与保留

CP 中涉及的审计、保密信息、隐私保护、知识产权等方面，以及涉及赔偿的责任限制条款，在本 CP 终止后继续有效。

9.11 对参与者的个别通告与沟通

参与者如需要进一步了解任何本 CP 中提及的服务、规范、操作等信息，可以通过电话联系 CFCA，联系电话：010-83526220。

9.12 修订

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

9.12.1 修订程序

修订程序与本 CP1.5.4 “ CP 批准程序 ” 相同。

9.12.2 通知机制和期限

CFCA 有权修订本 CP 中的任何术语、条款，事前无需通知订户，但在修订之后会及时公布在 CFCA 网站上。如在修订发布后 7 个工作日内，订户没有申请对其证书进行吊销，将被视为同意该修改。

9.12.3 必须修改业务规则的情形

当本 CP 描述的规则、流程和相关技术已经不能满足 CFCA 电子认证业务要求或本 CP 依据的法律法规和部门规章变更时，CFCA 将依照有关规定修改本 CP 的相关内容。

9.13 争议处理

同 CPS。

9.14 管辖法律

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

9.15 与适用法律的符合性

CFCA的各项策略均遵守并符合中华人民共和国各项法律法规和国家信息安全主管部门要求。若本CP的某一条款被主管部门宣布为非法、不可执行或无效时，CFCA将对该不符合性条款进行修改，直至该条款合法和可执行为止。本CP某一个条款的不可执行性不会导致其它条款的不可执行性。

9.16 一般条款

9.16.1 本 CP 的完整性

本 CP 将替代所有以前的或同时期的、与预植证书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

无。

9.16.3 分割性

无。

9.16.4 强制执行

无。

9.16.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的的客观情况。构成不可抗力的事件包括战争、恐怖行动、罢工、自然灾害、传染性疾病、互联网或其它基础设施无法使用等。但各方都有义务尽合理的努力建立灾难恢复和业务连续性机制。

9.17 其它条款

无。