

CnSCA 数字证书运作声明

版本 1.1

2004 年 5 月 18 日

CnSCA CPS

Version 1.1

18th, May, 2004

上证所信息网络有限公司

版权声明

本文版权归中国证券 CA 中心（以下称 CnSCA 或 CnSCA 中心）所有。本文中所涉及的“CnSCA”、“CnSCA 中心”、“中国证券 CA 中心”是由上证所信息网络公司建设的 CA 中心独立持有的专用名称。

未经 CnSCA 中心的书面同意，本文的任何部分不得以任何方式、任何途径进行复制、存储、调入网络系统检索或传播。

然而，在满足下述条件下，本文可以被授权以在非独占性的、免收版权许可使用费的基础上进行复制及传播：

- I . 前文的版权说明和上段主要内容将标于每个副本开始的显著位置。
- II . 副本应按照 CnSCA 中心提供的文件准确、完整地复制。

CnSCA 中心拥有对本文的最终解释权。

目录

| | | |
|----------|----------------|-----------|
| 1 | 引言 | 1 |
| 1.1 | 概述 | 1 |
| 1.2 | CNSCA 认证体系 | 1 |
| 1.2.1 | 认证和管理中心 | 2 |
| 1.2.2 | CA 中心 | 2 |
| 1.2.3 | KM 中心 | 2 |
| 1.2.4 | RA 中心 | 2 |
| 1.2.5 | 业务受理点 | 3 |
| 2 | 基本条款说明 | 4 |
| 2.1 | 服务 | 4 |
| 2.2 | 责任与义务 | 4 |
| 2.2.1 | CnSCA 的责任与义务 | 4 |
| 2.2.2 | 证书主体的责任和义务 | 5 |
| 2.3 | 费用说明 | 6 |
| 2.4 | 审计 | 6 |
| 3 | 认证运作规范 | 8 |
| 3.1 | 证书类型 | 8 |
| 3.2 | 证书生命周期 | 9 |
| 3.3 | 鉴别与授权 | 10 |
| 3.3.1 | CA 与 RA 的鉴别与授权 | 10 |
| 3.3.2 | 用户实体的鉴别 | 11 |
| 3.4 | 证书申请 | 11 |
| 3.4.1 | 申请条件 | 11 |
| 3.4.2 | 申请程序 | 11 |
| 3.4.3 | 申请信息 | 12 |
| 3.4.4 | 再申请条件 | 12 |
| 3.5 | 证书发放 | 12 |
| 3.6 | 证书使用 | 13 |
| 3.7 | 证书注销/过期 | 14 |
| 3.8 | CNSCA 证书费用 | 15 |
| 3.8.1 | 证书申请费用 | 15 |
| 3.8.2 | 证书更新费用 | 16 |
| 3.8.3 | 证书介质更换费用 | 16 |
| 3.8.4 | 证书注销费用 | 16 |
| 3.8.5 | 证书介质解锁费用 | 16 |
| 4 | 安全控制 | 17 |

| | | |
|----------|---------------------|-----------|
| 4.1 | 人员安全控制 | 17 |
| 4.1.1 | 岗位设置 | 17 |
| 4.1.2 | 人员要求 | 19 |
| 4.2 | 物理安全控制 | 20 |
| 4.3 | 流程安全控制 | 20 |
| 4.4 | 技术安全控制 | 21 |
| 4.4.1 | 系统安全控制 | 21 |
| 4.4.2 | 数据安全控制 | 21 |
| 5 | 其他规定 | 23 |
| 5.1 | 适用法律 | 23 |
| 6 | 版本变更 | 24 |
| 6.1 | 变更流程 | 24 |
| 6.2 | 公布策略 | 24 |
| | 附录：术语表 | 25 |

1 引言

1.1 概述

认证机构（国际通称“CA”），是指经营数字认证业务，对数字证书的申请
人发放、管理、取消数字证书同时提供数字签名识别、认证服务等机构，数
字证书（下称“证书”）指存在于计算机上的一个记录，是由 CA 签发的一个声
明，证明证书主体（“证书申请人”被发放证书后即成为“证书主体”）与证书
中所包含的公钥的唯一对应关系。证书包括证书申请人的名称及相关信息、申
请人的公钥、签发证书的 CA 的数字签名及证书有效期等内容。

中国证券 CA 中心（以下称 CnSCA 或 CnSCA 中心）是由上证所信息网络有限
公司所建设并运维的 CA 认证体系，面向证券行业提供服务，为证券行业的互联
网络的交易和作业双方建立信任关系，保证双方主体身份的真实性，为信息的
保密性、完整性及操作的不可抵赖性提供全面的服务。

CnSCA 基于公共密钥基础设施（PKI）技术构建，并通过了国家密码主管部
门的安全性审查，具有权威性、可信任性及公正性。

CnSCA 认证体系内的实体和 CnSCA 数字证书持有者，必须完整地理解和执行
本文所规定的条款，并承担相应的责任和义务。

1.2 CnSCA 认证体系

CnSCA 确保整个认证体系均采用一致的证书管理策略，以便能在不同的横
向或纵向信任服务体系之间建立起信任链的互连。全网一致的策略管理功能是
通过认证和管理中心来实现的，该机构负责设计整个 CnSCA 认证体系结构，制
定数字身份证书策略的框架，并指导各级职能 CA 的业务工作。下属的各基准认
证体系 CA 中心的策略管理机构均将按照认证和管理中心所制定的证书策略来
制定本认证子体系内部适用的证书策略（在保证与根证书策略相一致的前提
下），从而保证整个认证体系所采用的信任策略的一致性。

CnSCA 的信任链结构遵循传统的树状结构，即按照认证和管理中心、证书
认证中心（CA 中心）、数字证书审核注册中心（RA 中心）和 CA 业务受理点四级

加以组织。另外，CnSCA 建设密钥管理中心（KM 中心）对密钥进行管理。

1.2.1 认证和管理中心

认证和管理中心：是整个数字证书安全认证子系统的源点，是数字证书安全认证子系统的信任基准点，也是整个信任服务体系最终信任源和最高管理机构。其职责主要包括证书策略的管理、CA 根证书的发放与管理、下级 CA 的设立审核及管理、信任服务体系业务的规范化管理等。

1.2.2 CA 中心

CA 中心是数字证书安全认证子系统核心业务节点，对应于具体证书认证系统。CA 中心的功能主要包括各类证书的发放和管理、证书注销列表的管理、下级 RA 的设立审核及管理。

1.2.3 KM 中心

KM 中心是与 CA 中心相对应的密钥管理和服务机构，其主要职责和功能包括：

- 1、产生证书认证中心签发证书所需的加密密钥对；
- 2、托管所有证书的解密私钥和提供解密私钥历史记录恢复
- 3、为国家有关机构提供解密私钥查询和获取服务

1.2.4 RA 中心

RA 中心是数字证书安全认证子系统核心业务节点的附属服务节点，是与具体的业务逻辑密切相关的服务节点，可以由 CA 中心管理机构根据需求建设，也可由具有设立 RA 中心业务需求的应用单位或其主管部门负责进行建设。RA 中心的职责主要包括证书申请的受理、证书申请的初级审核、业务受理点的设立审核及管理。

1.2.5 业务受理点

业务受理点是认证体系的用户代理节点，作为 RA 中心的附属机构，由各 RA 中心根据需要建设，并报经主管 CA 中心同意并签发相应的证书。CA 业务受理点的具体设立地点和数目由各 RA 中心根据自身的业务发展需求而定。其主要职责是证书请求的接收、用户资料的初级审核与提交、用户证书的物理介质准备等。

.....

2 基本条款说明

2.1 服务

CnSCA 面向证券行业各类用户提供证书发放服务，包括但不限于：

- 1、 证券投资者；
- 2、 会员公司；
- 3、 上市公司；
- 4、 会员公司各营业部；
- 5、 证券市场组织与管理者
- 6、 营业部各交易员；
- 7、 网络设备或服务器；

CnSCA 认证服务内容主要包括：

- 1、 提供信任基础构架和数字证书认证服务；
- 2、 对指定类型的证书申请执行认证程序；
- 3、 按相关管理规定终止和注销证书；

CnSCA 中心承诺不会将证书申请人的信息用于任何商业活动。

2.2 责任与义务

2.2.1 CnSCA 的责任与义务

CnSCA 应承担的责任和义务是：

- 1、 保证 CnSCA 使用的公钥算法在现有技术条件下不会被攻破；
- 2、 保证 CnSCA 的自有私钥在 CnSCA 内部得到安全的存放和保护；
- 3、 CnSCA 建立和执行的安全机制符合国家有关政策的规定。
- 4、 CnSCA 将在为用户发放数字证书之前确认和核对用户的真实身份。

除非在有关条款中有明确的声明，除前款明确列出的责任和义务以外，

CnSCA 不承担其它任何形式的任何责任和义务，包括但不限于：

- 1、证书所包含信息的陈述不导致任何责任，只要证书内容充分地遵守本文；
- 2、不对任何软件作出保证。

在实施证书操作和发放证书的过程中，CnSCA 坚持并长期保持严格的条例和政策。CnSCA 保证发放的证书与用户提交信息的一致性，然而，如果因其他任何理由用户不完全满意发放给他的证书，在发放后的 7 个工作日内，用户可以要求 CnSCA 注销证书并退还用户相应的款项，但同时用户必须为该证书的注销生效之前使用证书进行的操作承担责任。

在过了最初 7 个工作日期限后，如果 CnSCA 实质性违约或重大违背了本文所规定的应由 CnSCA 对所有用户或用户证书所负的责任，用户可以要求 CnSCA 注销证书并退还用户相应的款项。在 CnSCA 注销用户的证书以后，CnSCA 将退还用户证书申请时支付的费用。

CnSCA 在进行身份认证或证书制作时，除根据相关法律和内部规则之外，还将充分遵守安全操作流程。如果由于 CnSCA 设备故障、线路中断，导致签发数字证书错误、延迟、中断或者无法签发，且上述情况的出现并非由于 CnSCA 故意或过失造成的，CnSCA 不负任何赔偿责任。

2.2.2 证书主体的责任和义务

一、申请证书

申请证书的用户实体为获取证书提供给授权机构的所有资料和陈述，包括登记人已知的信息和在证书中将要表明的信息，不论该陈述身份为认证机构确认与否，都应在其理解和信赖的范围内保证准确和完整。

二、接收证书

CnSCA 向申请人提供智能密码钥匙作为数字证书的载体。智能密码钥匙是一个 USB 接口的外接设备，其中存放着数字证书及密钥。同时，CnSCA 采用密码信封向申请人发放使用该智能密码钥匙的初始密码。证书申请人领取数字证书时应立即确认密码信封的完好性，如果密码信封破损，证书申请人有权拒绝

接收；证书申请人向下属成员（机构或个人）发放证书的过程中，也应确保密码信封完好无损；如果证书申请人接收密码信封已被开启的数字证书造成损失，所引起的后果由申请人承担。

申请证书的用户实体接收到 CnSCA 发布的证书，应向所有合理依赖证书内容的人证实：

- 申请证书的用户实体正确持有与证书内所列公共密钥相符的私密钥；
- 申请证书的用户实体向 CnSCA 所作的全部陈述以及提及的信息材料真实有效；
- 证书内有关申请证书的用户实体所应了解的信息有效。

三、私钥管理

- 1、 申请证书的用户实体通过 CnSCA 发布的证书，就承担了合理谨慎的义务，以保持与证书内所列公共密钥相符的私密钥的控制，并防止其向未经授权的其他人泄露；
- 2、 上述责任在用户的私钥被安全地销毁之前一直存在。

四、证书注销

证书主体在发生如下情况时应尽快请求 CnSCA 注销该证书：一、证书持有人死亡或者终止；二、数字证书中的信息发生重大变更；三、证书用户的私钥出现损坏、失窃、被更改、泄漏或其它损害等情况。

2.3 费用说明

CnSCA 将对使用 CnSCA 认证服务的投资者用户、会员公司用户、上市公司用户、会员公司营业部用户、交易员用户、网络设备/服务器用户等收取相关的费用，从 CnSCA 处可以获得当前费用的一览表。在 CnSCA 公布服务费用以后的一定期限之内，这些费用应该被交纳。

2.4 审计

CnSCA 将运行和维护可靠的系统用以保持对于所有重要事件的审计记录，

如密钥生成和证书申请、验证、注销。由安全评审机构至少每年一次对 CA 和 RA 进行审计和稽核，以评估其是否符合本文以及其它相关的协议、指导方针、过程和标准。

对于所接受的这些第三方审计稽核报告中，关于 CnSCA 的内容、调查结果和推荐的部分，CnSCA 无需表示认可或赞同。CnSCA 不会对这些报告发表任何观点，也不会对由于 CnSCA 对于这些报告的信任而导致的对任何人的任何损失而负责。

3 认证运作规范

3.1 证书类型

CnSCA 认证系统目前发放的证书有证券投资者证书、上市公司证书、会员公司证书、会员公司营业部证书、交易员证书、管理者证书、网络设备/服务器证书等七种类型。

证券投资者证书是 CnSCA 对需要获得网上证券服务的证券投资者(如股民)个人用户发放的证书,以确认其身份。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

上市公司证书是 CnSCA 对上市公司颁发的证书,能够为该上市公司的存在及名称提供保证,以确认其身份和相关信息。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

会员公司证书是 CnSCA 对经中国证监会依法批准设立,具有法人地位,并取得证券交易所会员资格的证券经营机构颁发的证书,能够为该会员公司的存在及名称提供保证,以确认其身份和相关信息。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

会员公司营业部证书是会员公司为其下属各证券营业部向 CnSCA 申请的证书,能够为营业部的存在及唯一名称提供保证,以确认其身份和相关信息。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

证券市场组织与管理者证书是 CnSCA 对证券市场组织或管理机构部门颁发的证书,如针对证券交易系统中场务用户和监察用户等。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

交易员证书是会员公司为其下属各营业部的交易员向 CnSCA 申请的证书,可以确认交易员的身份。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

设备证书是 CnSCA 对服务器、网络设备等发放的证书,以确认互联网上服务器、网络设备的实体身份。在证书发放前,需对申请人提供的证书申请表及有关证明文件进行审核。

3.2 证书生命周期

CnSCA 有完整的证书生命周期的管理,该管理流程适合于 CnSCA 签发的全部证书。

证书管理生命周期,应按下图所示的过程进行。

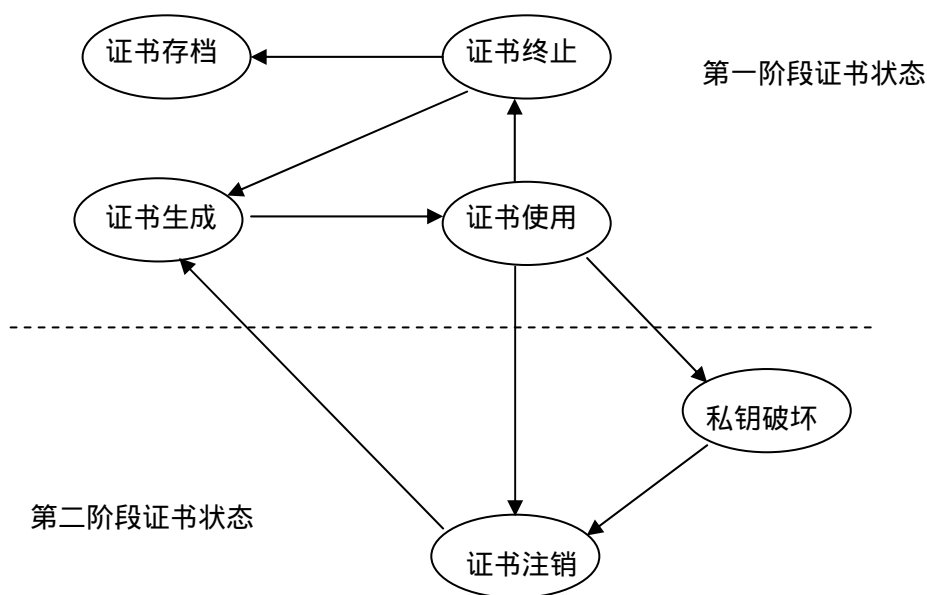


图 1 证书管理生命周期

CnSCA 证书管理主要分两大阶段：第一阶段和第二阶段。

第一阶段有证书生成、证书使用、证书终止和证书存档；第二阶段有私钥被破坏或泄密和证书注销或过期。

对上述证书管理生命周期中每个阶段都指定了相应的管理措施，规定了具体办法。

3.3 鉴别与授权

3.3.1 CA 与 RA 的鉴别与授权

PKI CA 的基本概念是其操作基础可信任，信任必须建立在每一个服务操作之上。CnSCA 负责谨慎地挑选可靠的成员去操作 CA 和 RA，以提供可信任的服务。

一、 CA 初始注册

CA 系统的设立必须由认证和管理中心根据 CA 中心设立的条件，经过严格的人员、物理设备等各方面考核之后设置。

由 CnSCA 认证和管理中心给 CA 签发证书，获取信任基础，CA 负责设置操作人员即 CA 管理员，该管理员经选择后授权。

CA 为了应用操作服务，可以用户法定名称（个人用户为其有效身份证件上所载姓名、机构用户为其依法登记使用的名称）作为注册名字。

二、 RA 初始注册

RA 的设立，由 CA 中心根据业务需要提出需求，或者由希望设立 RA 的机构向 CA 中心提出申请，CA 中心管理人员经过考核之后批准。

RA 被批准设立之后，由 CA 审查批准签发 RA 证书，获取信任基础。RA 负责设置 RA 管理员，该管理员在 CA 注册后，经挑选后授权。

RA 可以用户法定名称（个人用户为其有效身份证件上所载姓名、机构用户为其依法登记使用的名称）作为注册名字。

三、 注册详细内容

包括但不限于下列信息：

- 1- 通信地址；
- 2- 电子邮件地址；
- 3- 电话/传真号码；
- 4- 授权法人代表；
- 5- 指定管理员的联系方式；

3.3.2 用户实体的鉴别

用户实体（证券投资者/会员公司/上市公司/会员公司营业部/组织与管理者/交易员/设备服务器）首次注册必须亲自或授权代表前往 RA 处，并提交身份证明，注册人必须提交一份完整的并经申请用户签字（对机构用户，包括盖章）的申请表格。经 RA 确认后，RA 将告知申请用户如何索取证书。注册内容主要包括：

- 实体身份证明：各种身份证书、护照等；或者机构证明；网络设备证明
- 通信地址；
- Email 地址；
- 其他证书申请表所要求的信息。

3.4 证书申请

3.4.1 申请条件

希望获得 CnSCA 签发的证书的申请人必须提交证书申请并接受和同意本文的相关规定。

3.4.2 申请程序

所有用户实体的证书申请流程如下：

（一）申请人或授权代表首先到业务受理点申请证书服务，按照受理点提供的申请表要求提交证书申请信息；

（二）认证系统将生成一个密钥对，并把公钥列入证书申请信息。

（三）RA 中心审查通过后，将申请人的申请信息发送 CA 中心，由 CA 中心复核并签发证书；

（四）证书被发送到 CA 的目录服务器上；

（五）申请人领取证书。

3.4.3 申请信息

证书申请信息有投资者个人证书、会员公司证书、上市公司证书、会员公司营业部证书、管理者证书、交易员证书和设备/服务器证书之分。

证书申请人必须按照 CnSCA 各类证书申请表来提供证书申请信息，并确保相应信息的真实可靠性。

1. 申请投资者证书的申请人，应由申请人本人在《CnSCA 数字证书申请责任书》和《CnSCA 数字证书申请表》后签字确认，并携带有关证件前来申请。
2. 对申请上市公司证书、会员公司证书、会员公司营业部证书、证券市场组织与管理者证书、网络设备证书的申请人，应由申请机构（会员公司）在《CnSCA 数字证书申请责任书》和《CnSCA 数字证书申请表》后加盖公章确认，并由办理人携带有关证件前来申请。
3. 对申请交易员证书的申请人，应由申请机构（会员公司）在《CnSCA 数字证书申请责任书》和《CnSCA 数字证书申请表》后加盖公章确认，并由办理人携带有关证件前来申请。

3.4.4 再申请条件

当证书因过期或其他事由被注销后，满足本文规定的申请条件的客户可再申请以获得证书。

3.5 证书发放

证书申请批准后，CnSCA 将发放证书。在通过 CnSCA 审核和制作后，用户即可获得存放所申请的数字证书的介质载体和存放证书初始密码的密码信封。证书的发放意味着 CnSCA 完全并最终地正式批准了证书申请。

没有证书申请人的同意，CnSCA 将不发放证书。申请人一旦提交了申请，就被视为是同意 CnSCA 向其发放证书，尽管事实上其可能还没有接受证书。

如果证书申请人提供了虚假信息，或者不符合本文中规定的对证书申请人

的要求，CnSCA 可以拒绝给申请人发放证书，并且不会对因此而导致的任何损失或费用负担任何责任和义务。在 CnSCA 拒绝发放证书以后，CnSCA 应立即将证书申请人已付的相关费用归还，但证书申请人提交欺骗性或虚假信息致使 CnSCA 拒绝申请人的除外。

CnSCA 一旦收到了所有的相关信息并确认，将在下面的时间期限内向最终用户发放证书：

| 证书类别 | 发放期限 |
|-----------|------------|
| 证券投资者证书 | 即刻到 1 个工作日 |
| 会员公司证书 | 1-5 个工作日 |
| 上市公司证书 | 1-5 个工作日 |
| 会员公司营业部证书 | 1-5 个工作日 |
| 组织与管理者证书 | 1-5 个工作日 |
| 交易员证书 | 即刻到 3 个工作日 |
| 设备/服务器证书 | 1-5 个工作日 |

最终期限取决于证书申请人及时提交完整准确的信息、响应 CnSCA 的管理要求，包括提供适当和正确的支付信息以及其认可。

一经 CnSCA 发放和用户接受，所有的证书将被认为有效。所有的证书的使用有效期于发放之时始。

3.6 证书使用

相关方（CnSCA 和用户）已被通告下列控制其各自的权利和义务的规章，这些规章被视为得到了相关方的同意，并通过以下方式对该相关方产生约束力：

- 一、对 CnSCA 而言，就是本文发布后；
- 二、对申请人或用户而言，就是提交证书申请单后；

三、对于证书接受者或信赖方而言，就是信赖某证书、或信赖按照与证书中所列的公钥验证后的数字签名后。

进行数字签名的验证是为了确认数字签名是用签名者证书中所列的公钥相对应的私钥创造的，并且保证数字签名创建后，相关信息没有被更改。

这样的验证将在与本文保持一致的基础上进行，验证方式如下所述：

- 一、 为数字签名建立证书链；
- 二、 确保此证书链与该数字签名是最相配的；
- 三、 检查 CnSCA 公布的信息，看链上的证书是否被注销和中止；
- 四、 数字签名附加的界定数据；
- 五、 显示创造数字签名的时间和日期；
- 六、 建立签名者想要的担保；
- 七、 确保链上的所有证书都批准最终用户私钥的使用；
- 八、 证书链的确认。

3.7 证书注销/过期

证书申请人或其继承人、清算人在发生如下情况时应尽快请求 CnSCA 注销该证书：

- 一、 证书申请人死亡或者终止；
- 二、 数字证书中的信息发生重大变更；
- 三、 证书用户的私钥出现损坏、失窃、被更改、泄漏或其它损害等情况；
- 四、 用户（或授权代表）适时地请求注销证书。

CnSCA 将在如下情况下注销申请人的证书：

- 一、 证中的相关主体（CnSCA 或用户）违背了本文中的规定，包括：
 1. 申请注册时，提供不真实材料；
 2. 没有按照规定缴纳认证费用、证书更新费用或其他相关费用；
 3. 违反国家法律或者其他规章制度，不应签发数字证书的；
 4. 其他情况。这些情况可以是因法律或政策的要求，CnSCA 采取的临

时作废措施。

二、用户根据本文应承担的义务，由于不可抗力、自然灾害、法律、条例、规章或其它法令改变、政府行为、造成他人信息受到或可能受到实质性的威胁或危及安全等原因而无法履行或按时履行；

三、由于认证机构过错造成数字证书的安全性得不到保证；

注销证书后，CnSCA 必须发布注销信息。CnSCA 将在下一次公布证书注销名单（CRL）时（CnSCA 发布证书注销列表的间隔最多不超过两个自然日），指明注销的证书。

对被注销的证书，证书使用有效期将被认为立即暂停或永久中止。

证书的注销不影响在本文下规定的任何基本职责。各当事方仍应遵守本文的规定。

注销证书里的公共密钥所对应的私密钥，在整个注销后的适用保持期内，除非已经被销毁，否则用户仍应运用可信的方法进行维护，以避免安全风险。

当用户的证书即将过期时，CnSCA 将通知用户。此通知的目的仅为方便用户的重新注册或更新过程。

证书的过期并不影响在本文规定的任何基本责任的有效性。

用户更新和重新注册时与初始申请的步骤完全相同，只需提交更新的或更改过的信息。重新注册和更新的要求将按照 CnSCA 的判断而决定是否被接受。

3.8 CnSCA 证书费用

3.8.1 证书申请费用

个人用户证书申请的费用为：介质费 200 RMB；服务费 200RMB/年；

机构用户（包括会员公司、上市公司、媒体机构等）证书申请的费用为：介质费 200 RMB；服务费 600RMB/年；

会员公司营业部证书申请的费用为：介质费 200 RMB；服务费 600RMB/年；

服务器证书申请的费用为：介质费 200 RMB；服务费 1000RMB/年；

3.8.2 证书更新费用

CnSCA 证书用户更新证书时，不另收取介质费。证书服务费仍按 3.8.1 的规定收取。

3.8.3 证书介质更换费用

CnSCA 证书用户在证书介质损毁，需要更换介质时，收取 200 元 RMB 介质费。证书服务费仍按 3.8.1 的规定收取。

3.8.4 证书注销费用

CnSCA 为证书用户提供证书注销服务，不单独收取证书注销费用。

3.8.5 证书介质解锁费用

CnSCA 证书用户在连续输入错误口令到一定次数，导致证书介质锁死，需要 CnSCA 提供证书介质解锁服务时，CnSCA 收取 50 元 RMB/次的介质解锁费用。

4 安全控制

4.1 人员安全控制

4.1.1 岗位设置

CnSCA 明确执行 CA 关键职能的岗位设置，包括：

一、CA 策略服务初始化人员（5 人）

1. “五选三”产生系统根证书，备份根证书；
2. “五选三”产生业务 CA 根证书，并备份业务 CA 根证书。

二、CA 系统管理员

1. 导入业务 CA 根证书；
2. 增加业务管理员；
3. 注销业务管理员；
4. 业务管理员权限设置；
5. 修改业务管理员权限。

三、CA 业务管理员

1. 增加业务操作员；
2. 注销业务操作员；
3. 业务操作员权限设置；
4. 修改业务操作员权限。

四、CA 业务操作员

1. 对证书载体的初始化；
2. 为用户签发数字证书；
3. 用户信息，日志访问，审计查询等操作；
4. 证书服务模板设置；
5. 证书发布，黑名单发布；
6. 注册产生 RA 中心，并产生 RA 服务器证书。

五、KM 系统管理员

1. 导入 KM 的根证书；

2. 增加业务管理员；
3. 注销业务管理员；
4. 业务管理员权限设置；
5. 修改业务管理员权限。

六、KM 业务管理员

1. 增加业务操作员；
2. 注销业务操作员；
3. 业务操作员权限设置；
4. 修改业务操作员权限。

七、KM 业务操作员

1. 密钥生成操作；
2. 证据访问操作、日志访问操作；
3. 密钥管理（当前密钥，备份密钥，历史密钥，密钥销毁）。

八、RA 系统管理员

1. 导入 RA 服务器证书；
2. 同步 CA 数据，包括证书服务模板；
3. 增加业务管理员；
4. 注销业务管理员；
5. 业务管理员权限设置；
6. 修改业务管理员权限。

九、RA 业务管理员

1. 增加业务操作员；
2. 注销业务操作员；
3. 业务操作员权限设置；
4. 修改业务操作员权限。

十、RA 业务操作员

1. 录入用户注册信息；
2. 审核用户信息；
3. 为用户产生证书请求；

4. 下载证书到证书载体；
5. 用户信息修改，注销，查询等操作；
6. 日志审计操作。

设置上述岗位是为了确保责任能够分担明确，建立有效的安全机制，保证内部管理和操作的安全。

CnSCA 对于其运行和操作相关的职能有明确分工，贯彻互相牵制的安全机制。

4.1.2 人员要求

一、 人员背景审查

CnSCA 员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工。员工需要有 3 个月以上的考察期，根据考察的结果安排相应的工作或者辞退并且剥离岗位。

CnSCA 会对其关键的 CA 职员进行严格的背景调查。

CnSCA 员工受到合同和 CnSCA 章程的约束，不许泄露 CnSCA 认证体系的敏感信息。所有员工与 CnSCA 签订保密协议，合同期满后如离职一段时间内不得从事与 CnSCA 类似的工作。

二、 人员培训

CnSCA 根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

CnSCA 对 CnSCA 员工进行以下内容的综合性培训：

- 1、 岗位职责；
- 2、 安全原则和机制；
- 3、 相关的政策、标准、法规和管理办法；
- 4、 使用软件的介绍；
- 5、 操作的系统和网络；
- 6、 其他 CnSCA 认为需要对员工进行的培训；

三、 相关要求

1、 岗位分离

CnSCA 严格遵照各关键岗位分离的原则，系统管理员、业务管理员和业务操作人员承担不同的责任。

2、 未授权的行为制裁

当 CnSCA 员工被怀疑，或者已进行了未授权的操作，CnSCA 在得到信息后立刻中止该员工进入 CnSCA 认证体系。并根据情节严重程度，实施包括提交司法机关处理等措施。

4.2 物理安全控制

CnSCA 机房的建设和管理严格按照国家相关主管部门的有关规定进行，机房的设计对温湿度、照度、噪声要求、水患防护、火灾防护、电磁屏蔽与静电防护、雷电防护、接地与等电位连接系统、区域及设备防护、电源要求、装饰材料要求、监控系统要求等各方面进行了考虑，采用高安全性的监控技术，包括红外报警监测、门禁（含指纹识别）、视频监控、精密空调监控、UPS 监控、漏水检测、温湿度检测等监控技术，以确保 CnSCA 物理环境的安全。

CnSCA 机房供电得到充分保障，使用不间断电源（UPS），避免电源波动。保证系统的 7×24 小时不间断运行。机房采用专用精密空调，保证机房内温湿度在一定范围内保持恒定，保证系统的正常稳定运行。机房内的消防和防雷设施已通过国家有关部门的验收。

CnSCA 机房内划分区域构建专用电磁屏蔽机房，存放 CnSCA 关键设备，保证 CnSCA 产生和传送的重要关键数据不会通过电磁方式被窃取或泄露。屏蔽机房的相关指标已通过国家有关部门的检验。

4.3 流程安全控制

CnSCA 内部制定严格的流程控制和管理制度。

- 1、 机房内部原则上禁止参观，只有经过 CnSCA 授权的人员才能进入授权的部位和工作地点；
- 2、 非 CnSCA 员工由于必要的原因（如物理修理、消防、设备故障等），需要进入 CnSCA 的特定区域时，必须有 CnSCA 授权的专门人员陪同

- 进入并完成全部操作；
- 3、 进入 CnSCA 区域的人员须严格遵守 CnSCA 的相关规定和操作流程；
 - 4、 相关的进入和操作行为都被详细记录并由相关的责任人签字确认。

4.4 技术安全控制

4.4.1 系统安全控制

一、 系统安全

CnSCA 通过以下途径保证 CnSCA 系统的安全：

- 1、 保证 CnSCA 系统的物理通道和逻辑通道的安全；
- 2、 对 CnSCA 承担工作的角色进行分类，建立安全分散和牵制机制；
- 3、 任何与 CnSCA 的关键部分的通信都采用加密机制；
- 4、 定期对所有涉及安全的事件进行审查；
- 5、 参照国家有关系统安全的规定执行。

二、 系统控制

- 1、 CnSCA 认证体系中的配置，以及任何修改和升级都会记录在案，并予以控制。
- 2、 CnSCA 在不影响正常提供服务和遵守国家有关规定的前提下，及时进行技术更新。
- 3、 CnSCA 采用各种网络安全技术，实施访问控制；

4.4.2 数据安全控制

一、 密钥安全

CnSCA 产生的所有密钥对，均采用国家许可的硬件加密机生成。CnSCA 不对称密钥对采用至少 1024 位 RSA 生成。

CnSCA 严格规定密钥的产生、发放、管理、备份等操作的流程和证书与密钥的使用范围。

二、 敏感数据安全

CnSCA 采用多种方式保护敏感数据，以避免未经授权的使用。包括物理通

道的严格管理和使用加解密机制等。

5 其他规定

5.1 适用法律

CnSCA 认证服务服从于中国的法律，包括且不限于：中华人民共和国刑法、中华人民共和国人大常委会颁发的关于互联网安全防护措施的决定、中华人民共和国计算机安全管理条例、中华人民共和国商用密码管理条例。

6 版本变更

6.1 变更流程

CnSCA 有权不断变更 CnSCA CPS (预期的和非预期的)。

在 CnSCA CPS 作出任何变动之前，CnSCA 将对变更建议进行研究，作出变更决定，并形成决议。

CnSCA 在决定形成决议后，向用户公布变更后的 CPS。

CnSCA 对 CnSCA CPS 进行严格的版本控制。

6.2 公布策略

CnSCA 有权把变更结果以 CPS 的修订版的形式通过适当的方式向用户公布。

附录：术语表

1、CA

证书授权中心 (Certificate Authority), 主要负责各类数字证书的发放和管理、证书注销列表的管理、下级 RA 的设立审核及管理。

2、中国证券 CA 中心、CnSCA 中心、CnSCA

指上证所信息网络有限公司建设并运维的 CA 系统, 面向证券行业提供证书发放等相关服务。

3、CPS

证书运作声明 (Certificate Practice Statement), 是包含 CA 数字证书相应政策、详细操作说明和操作步骤等相关内容的声明。

4、PKI

公开密钥基础设施(public key infrastructure), 是一种密码管理的框架体系, 用以保证电子交易和作业的操作者身份的真实性、操作的不可抵赖性和传输数据的保密性。

5、RA

注册管理中心 (Register Authority), 主要负责证书申请的受理、证书申请的初级审核、业务受理点的设立审核及管理。

6、KM

密钥管理中心 (Key Management), 是与 CA 中心相对应的密钥管理和服务机构, 负责产生 CA 签发证书所需要的加密密钥对, 并托管所有证书的密钥, 为国家授权机构和得到批准的用户提供密钥的查询和恢复功能。

7、CRL

证书注销列表(certification revocation list), 用于标识 CA 中心宣布注销的证书。

8、RSA

一种加密算法 (Rivest Shamir Adleman), 是在数据保密技术中使用的一种通用关键字密码方法, 是基于大数作因子分解的难度而建立的方法。