

中国互联网络信息中心（CNNIC）  
可信网络服务中心  
证书业务规则

版本号：2.07

有效期：2010-04-07 至 2011-04-07

中国互联网络信息中心（CNNIC）

2010年04月07日

CNNIC 可信网络服务中心证书业务规则版本控制表

| 版本号   | 主要修改说明   | 完成时间             |
|-------|--|------------------|
| V1.00 | 初次审核通过   | 2007 年 5 月 15 日  |
| V2.00 | 进行年审修改后, 延长 CPS 有效期一年  | 2008 年 4 月 8 日   |
| V2.01 | 提供 http 协议的 CRL 下载   | 2008 年 11 月 5 日  |
| V2.02 | 1、域名证书密钥对要求 2048 位<br>2、赔付金额进行修改<br>3、联络方式中的邮编修改<br>4、年审完成, 延长 CPS 有效期一年         | 2009 年 3 月 19 日  |
| V2.03 | 1、证书主题中 O 项值修改<br>2、多域名证书主题中 CN 项值修改<br>3、证书申请所提交材料调整<br>4、证书结构中证书项说明调整, 与所发证书一致 | 2009 年 4 月 14 日  |
| V2.04 | 1、参考号、授权码发放方式调整<br>2、CP 改为在储存库中公开发布<br>3、对证书发布情况的说明进行调整                          | 2009 年 6 月 18 日  |
| V2.05 | 1、修改交叉认证描述, 增加 CNNIC 中级根证书和 Entrust 根之间的关系说明                                     | 2009 年 11 月 09 日 |
| V2.06 | 1、增加对根签发的证书废止列表的说明, 相应对其他相关部分文字进行调整  | 2010 年 2 月 2 日   |
| V2.07 | 1、延长有效期  | 2010 年 4 月 8 日   |

## 目录

|          |                                    |          |
|----------|------------------------------------|----------|
| <b>1</b> | <b>引言</b>                          | <b>1</b> |
| 1.1      | 概述                                 | 1        |
| 1.2      | 角色与责任                              | 1        |
| 1.2.1    | 安全管理委员会                            | 1        |
| 1.2.2    | 首席安全管理员                            | 1        |
| 1.3      | 适用性                                | 2        |
| 1.3.1    | CNNIC 可信网络服务中心                     | 2        |
| 1.3.2    | 最终实体                               | 3        |
| 1.3.3    | 证书持有者分类                            | 4        |
| 1.3.4    | 证书分类                               | 4        |
| 1.3.5    | 证书有效期                              | 4        |
| 1.3.6    | 从 CNNIC 可信网络服务中心申请证书               | 4        |
| 1.4      | 联络方式                               | 4        |
| 1.5      | 处理投诉程序                             | 5        |
| <b>2</b> | <b>总则</b>                          | <b>5</b> |
| 2.1      | 义务                                 | 5        |
| 2.1.1    | CNNIC 可信网络服务中心认证中心 (CA) 义务         | 5        |
| 2.1.2    | CNNIC 可信网络服务中心注册中心 (RA) 义务         | 6        |
| 2.1.3    | 储存库义务                              | 6        |
| 2.1.4    | 证书持有者义务                            | 6        |
| 2.1.5    | 信赖方义务                              | 7        |
| 2.2      | 其它                                 | 8        |
| 2.2.1    | 合理技术及免责条款                          | 8        |
| 2.2.2    | 责任限制                               | 8        |
| 2.2.3    | CNNIC 可信网络服务中心对已获接受但有缺陷的数字证书所承担的责任 | 11       |
| 2.2.4    | 证书持有者的转让                           | 11       |
| 2.2.5    | 陈述权限                               | 11       |
| 2.2.6    | 更改                                 | 11       |
| 2.2.7    | 保留所有权                              | 12       |
| 2.2.8    | 条款冲突                               | 12       |
| 2.2.9    | 受信关系                               | 12       |
| 2.2.10   | 交叉认证                               | 12       |
| 2.3      | 解释及执行 (管辖法律)                       | 12       |
| 2.3.1    | 管辖法律                               | 12       |
| 2.3.2    | 条款可中止性、修改                          | 13       |
| 2.3.3    | 争议解决程序                             | 13       |
| 2.4      | 证书费用                               | 13       |
| 2.4.1    | 高级证书                               | 13       |

|          |                              |           |
|----------|------------------------------|-----------|
| 2.4.2    | 查询.....                      | 13        |
| 2.4.3    | 废止.....                      | 13        |
| 2.4.4    | 退款策略.....                    | 14        |
| 2.4.5    | 其他费用.....                    | 14        |
| 2.5      | 公布资料及储存库 .....               | 14        |
| 2.5.1    | 证书储存库控制.....                 | 14        |
| 2.5.2    | 证书储存库进入要求.....               | 15        |
| 2.5.3    | 证书储存库更新周期.....               | 15        |
| 2.6      | 遵从规定的评估 .....                | 15        |
| 2.7      | 机密性 .....                    | 15        |
| <b>3</b> | <b>鉴别及认证.....</b>            | <b>16</b> |
| 3.1      | 命名 .....                     | 16        |
| 3.1.1    | 名称类型.....                    | 16        |
| 3.1.2    | 名称要求.....                    | 17        |
| 3.1.3    | 申请者的匿名或伪名.....               | 17        |
| 3.1.4    | 理解不同名称形式的规则.....             | 17        |
| 3.1.5    | 名称唯一性.....                   | 18        |
| 3.1.6    | 商标的识别、鉴证和角色.....             | 18        |
| 3.1.7    | 名称争端解决.....                  | 18        |
| 3.2      | 高级证书首次注册 .....               | 18        |
| 3.2.1    | 单域名, 通配域名证书.....             | 18        |
| 3.2.2    | 多域名证书.....                   | 20        |
| 3.3      | 证明拥有私钥的方法 .....              | 21        |
| <b>4</b> | <b>操作规范.....</b>             | <b>22</b> |
| 4.1      | 高级证书申请、签发、接受及发布.....         | 22        |
| 4.1.1    | 证书申请.....                    | 22        |
| 4.1.2    | 签发、接受证书.....                 | 22        |
| 4.1.3    | 证书发布.....                    | 23        |
| 4.2      | 高级证书补发 .....                 | 23        |
| 4.2.1    | 单域名, 通配域名证书补发.....           | 23        |
| 4.2.2    | 多域名证书补发.....                 | 24        |
| 4.3      | 高级证书续费 .....                 | 25        |
| 4.3.1    | 单域名, 通配域名证书续费.....           | 26        |
| 4.3.2    | 多域名证书续费.....                 | 27        |
| 4.4      | 多域名证书域名修改 .....              | 29        |
| 4.5      | 证书废止 .....                   | 31        |
| 4.5.1    | 废止的情形.....                   | 31        |
| 4.5.2    | 废止程序.....                    | 31        |
| 4.5.3    | 废止效力.....                    | 33        |
| 4.5.4    | 请求证书废止的实体.....               | 33        |
| 4.5.5    | 废止请求的流程.....                 | 33        |
| 4.5.6    | 废止请求提出时限.....                | 33        |
| 4.5.7    | CNNIC 可信网络服务中心处理废止请求的时限..... | 33        |

|          |                          |           |
|----------|--------------------------|-----------|
| 4.5.8    | 信赖方检查证书废止的要求.....        | 34        |
| 4.5.9    | CRL 发布频率.....            | 34        |
| 4.5.10   | CRL 发布的最大滞后时间.....       | 34        |
| 4.5.11   | 在线状态查询的可用性.....          | 34        |
| 4.5.12   | 在线状态查询要求.....            | 34        |
| 4.5.13   | 废止信息的其他发布形式.....         | 34        |
| 4.5.14   | 密钥损害的特别要求.....           | 35        |
| 4.6      | 证书冻结.....                | 35        |
| 4.7      | 证书更新.....                | 35        |
| 4.8      | 证书发布.....                | 35        |
| 4.9      | 计算机安全审计程序.....           | 35        |
| 4.9.1    | 记录事件类型.....              | 35        |
| 4.9.2    | 处理记录的次数.....             | 36        |
| 4.9.3    | 审计追踪记录保存期限.....          | 36        |
| 4.9.4    | 审计追踪记录保护.....            | 36        |
| 4.9.5    | 审计追踪记录备份.....            | 36        |
| 4.9.6    | 审计追踪记录收集系统.....          | 36        |
| 4.9.7    | 安全事件通知.....              | 36        |
| 4.9.8    | 脆弱性评估.....               | 37        |
| 4.10     | 记录归档.....                | 37        |
| 4.10.1   | 归档记录类型.....              | 37        |
| 4.10.2   | 归档保存期限.....              | 37        |
| 4.10.3   | 归档保护.....                | 37        |
| 4.10.4   | 归档备份程序.....              | 38        |
| 4.10.5   | 时间戳.....                 | 38        |
| 4.11     | 密钥变更.....                | 38        |
| 4.12     | CNNIC 可信网络服务中心服务终止.....  | 38        |
| 4.13     | 灾难恢复及密钥泄漏计划.....         | 38        |
| 4.13.1   | 灾难恢复计划.....              | 38        |
| 4.13.2   | 密钥泄漏应对计划.....            | 39        |
| 4.13.3   | 密钥的转换.....               | 39        |
| <b>5</b> | <b>实体、程序及人员安全控制.....</b> | <b>40</b> |
| 5.1      | 实体安全.....                | 40        |
| 5.1.1    | 选址及建造.....               | 40        |
| 5.1.2    | 进入控制.....                | 40        |
| 5.1.3    | 电力及空调.....               | 40        |
| 5.1.4    | 自然灾害.....                | 40        |
| 5.1.5    | 防火及保护.....               | 40        |
| 5.1.6    | 媒体介质存储.....              | 41        |
| 5.1.7    | 场外备份.....                | 41        |
| 5.1.8    | 保管印刷文件.....              | 41        |
| 5.1.9    | 废料处理.....                | 41        |
| 5.2      | 过程控制.....                | 41        |
| 5.2.1    | 可信职责.....                | 41        |

|          |  |           |
|----------|--|-----------|
| 5.2.2    | CNNIC 可信网络服务中心与本地受理点(LRA)之间的文件及资料传递..... | 42        |
| 5.2.3    | 年度评估.....                                | 42        |
| 5.3      | 人员控制.....                                | 42        |
| 5.3.1    | 背景及资格.....                               | 42        |
| 5.3.2    | 背景调查.....                                | 42        |
| 5.3.3    | 培训要求.....                                | 43        |
| 5.3.4    | 向人员提供的文件.....                            | 43        |
| <b>6</b> | <b>技术安全控制.....</b>                       | <b>43</b> |
| 6.1      | 密钥的生成及安装.....                            | 43        |
| 6.1.1    | 密钥对的生成.....                              | 43        |
| 6.1.2    | 公钥传送给证书签发机构.....                         | 44        |
| 6.1.3    | CNNIC 可信网络服务中心公钥发布.....                  | 44        |
| 6.1.4    | 密钥的长度.....                               | 44        |
| 6.1.5    | 密码模块标准.....                              | 44        |
| 6.1.6    | 密钥用途.....                                | 44        |
| 6.1.7    | 密钥销毁.....                                | 44        |
| 6.2      | 私钥保护和密码模块工程控制.....                       | 45        |
| 6.2.1    | 密码模块标准.....                              | 45        |
| 6.2.2    | 私钥多人控制.....                              | 45        |
| 6.2.3    | 私钥托管.....                                | 45        |
| 6.2.4    | CNNIC 可信网络服务中心私钥备份.....                  | 45        |
| 6.3      | 密钥对管理的其它方面.....                          | 46        |
| 6.3.1    | 公钥归档.....                                | 46        |
| 6.3.2    | 私钥归档.....                                | 46        |
| 6.3.3    | 证书操作期和密钥对使用期限.....                       | 46        |
| 6.4      | 计算机安全控制.....                             | 46        |
| 6.5      | 生命周期技术安全控制.....                          | 47        |
| 6.6      | 网络安全控制.....                              | 47        |
| 6.7      | 密码模块工程控制.....                            | 47        |
| <b>7</b> | <b>证书及证书废止列表（CRL）结构.....</b>             | <b>47</b> |
| 7.1      | 证书结构.....                                | 47        |
| 7.1.1    | 版本号.....                                 | 47        |
| 7.1.2    | 证书项说明.....                               | 48        |
| 7.1.3    | 算法对象标识符.....                             | 49        |
| 7.1.4    | 名称形式.....                                | 49        |
| 7.1.5    | 名称限制.....                                | 49        |
| 7.1.6    | 证书策略对象标识符.....                           | 50        |
| 7.1.7    | 策略限制扩展项的用法.....                          | 50        |
| 7.1.8    | 策略限定符的语法和语义.....                         | 50        |
| 7.1.9    | 关键证书策略扩展项的处理规则.....                      | 51        |
| 7.2      | 证书废止列表（CRL）结构.....                       | 51        |
| 7.2.1    | 版本号.....                                 | 51        |
| 7.2.2    | CRL 项.....                               | 51        |

|          |                    |           |
|----------|--------------------|-----------|
| 7.3      | OCSP .....         | 51        |
| 7.3.1    | 版本号.....           | 52        |
| 7.3.2    | OCSP 扩展项.....      | 52        |
| 7.3.3    | OCSP 请求.....       | 52        |
| 7.3.4    | OCSP 响应.....       | 53        |
| <b>8</b> | <b>CPS 管理.....</b> | <b>53</b> |
| 8.1      | 变更流程 .....         | 53        |
| 8.2      | 公告与通知 .....        | 53        |
| 8.3      | CPS 批准程序 .....     | 53        |
| 8.4      | 解释 .....           | 54        |

---

# 1 引言

## 1.1 概述

中国互联网络信息中心（CNNIC）可信网络服务中心（以下简称“CNNIC 可信网络服务中心”）为域名提供域名证书安全服务（也称“网址卫士”服务），因此根据 IETF 组织关于证书业务规则(CPS)的编写规范 RFC3647 编写了 CNNIC 可信网络服务中心的 CPS，作为 CNNIC 可信网络服务中心的证书相关业务和系统的运行规范。

## 1.2 角色与责任

### 1.2.1 安全管理委员会

CNNIC 可信网络服务中心安全管理委员会负责安全策略、规范和决策制定，是 CNNIC 可信网络服务中心安全管理的决策机构。安全管理委员会的职责包括：收集与协调安全管理方面的问题和建议，达成一致意见；制定并维护 CNNIC 可信网络服务中心的证书策略文件（CP）；对本 CPS 进行审核，以确保 CPS 与 CP 文件一致。

安全管理委员会根据需要每年举行 4 次会议或进行文件会签。安全管理委员会成员由来自于 CNNIC 领导、人力资源、财务、法律事务、安全管理等方面的代表组成。

### 1.2.2 首席安全管理员

首席安全管理员将全面负责 CNNIC 可信网络服务中心日常的各项安全事务，受 CNNIC 可信网络服务中心安全管理委员会授权，首席安全管理员可以执行变更 CNNIC 可信网络服务中心的安全策略，对 CNNIC 可信网络服务中心的安全管理进行定期的检查和评估，保持 CNNIC 可信网络服务中心的安全管理始终处

在一个较先进的水平，具有较高的安全性和可信度。随时追踪有关安全管理的最新动态，确保安全体系的先进性。为保障 CNNIC 可信网络服务中心的安全、可靠运营，CNNIC 可信网络服务中心首席安全管理员重点关注下面三个关键领域：开发安全策略，并协助程序开发和执行；维护安全策略和程序，使之保持完备性；审计安全策略及其实际执行情况的一致性。

CNNIC 可信网络服务中心首席安全管理员拥有以下职责：

- ◆ 经授权后建立和变更 CNNIC 可信网络服务中心安全策略和规范；
- ◆ 管理交叉认证，发布 CNNIC 可信网络服务中心交叉认证协议，更新及撤销交叉认证；
- ◆ 处理审计报告。

## 1.3 适用性

### 1.3.1 CNNIC可信网络服务中心

根据本 CPS，CNNIC 可信网络服务中心履行证书认证机构的职能并承担其义务。CNNIC 可信网络服务中心是唯一根据本 CPS 授权发出证书的证书认证机构（见第 2.1.1 节）。

#### 1.3.1.1 CNNIC可信网络服务中心所作的陈述

CNNIC 可信网络服务中心向遵守本 CPS 第 2.1.5 节和其它有关条款的信赖方表明，CNNIC 可信网络服务中心根据本 CPS 向证书持有者颁发证书。

#### 1.3.1.2 生效

经 CNNIC 可信网络服务中心签发的证书一经发出并由证书持有者接受，证书立即生效。

#### 1.3.1.3 CNNIC可信网络服务中心对本地受理点（LRA）授权的权利

CNNIC 可信网络服务中心可把履行本 CPS 及证书持有者协议的部分或全部

工作的职责授权给本地受理点(LRA)执行。无论有关职责是否由本地受理点(LRA)执行，CNNIC 可信网络服务中心仍会负责履行本 CPS 及证书持有者协议。

本业务规则中的本地受理点（LRA）是指 CNNIC 认证的网址卫士注册服务机构。

### 1.3.2 最终实体

根据本证书业务规则，存在两类最终实体，包括证书持有者及信赖方。证书持有者可以是 " 证书持有者个人 " 或 " 证书持有者机构 "。信赖方信任 CNNIC 可信网络服务中心发出的任何类别或种类证书（包括但不限于域名证书）。特此澄清，信赖方信任的不是可信网络服务注册中心(以下简称“注册中心”或 RA)或本地受理点(LRA)等证书注册机构，而是 CNNIC 可信网络服务中心。CNNIC 可信网络服务中心通过注册中心发出数字证书，而注册中心对信赖方并无任何职务职责，也不需对信赖方就发出数字证书而负责（见第 2.1.2 节）。

#### 1.3.2.1 证书持有者的保证及陈述

申请人须签署或确定接受一份协议（按本 CPS 规定的条款），其中载有一条款。申请人据此条款同意，申请人一经接受根据本 CPS 发出的证书，即表示其向 CNNIC 可信网络服务中心保证（承诺）并向所有其它有关人士（尤其是信赖方）做出陈述，在证书的有效期内，以下事实属实并将保持真实：

- ◆ 除域名证书持有者及其授权者外，并无其它人士曾取用证书持有者的私人密钥。
- ◆ 使用与证书持有者域名证书所包含的公开密钥相关的证书持有者私人密钥所产生的每一数字签名实属证书持有者的数字签名。
- ◆ 证书所包含的所有资料及由证书持有者做出的陈述均属真实。
- ◆ 证书将只会用于符合本 CPS 认可并合法的用途。
- ◆ 在证书申请过程中所提供的所有资料，均不侵犯任何第三方的商标、服务标记、商号、公司名称或任何知识产权。

### 1.3.3 证书持有者分类

CNNIC 可信网络服务中心的证书持有者就是域名持有者，可以是法人或自然人，但 CNNIC 可信网络服务中心并不区分他们。

### 1.3.4 证书分类

CNNIC 可信网络服务中心根据本 CPS 提供域名证书服务（也称“网址卫士”服务），目前所颁发的域名证书品牌为“高级证书”，高级证书存在不同的类型：

- ◆ 单域名证书：CN 是一个固定域名
- ◆ 通配域名证书：CN 是一个形式为“\*.xxx.xxx”形式的域名
- ◆ 多域名证书：CN 是多个域名的并列，例如“CN=a. xxx.xxx，CN=b. xxx.xxx，CN=c. xxx.xxx”，SAN 扩展中包含这多个域名

CNNIC 可信网络服务中心颁发的高级证书仅限于域名证书，不能用于其他用途。

### 1.3.5 证书有效期

根据本证书业务规则发出的新申请人的证书，其有效期为一年。

根据本证书业务规则的证书续费程序而发出的证书有效期可超过上述的有效期。数字证书内会注明其有效期。

### 1.3.6 从CNNIC可信网络服务中心申请证书

所有首次申请及证书废止或到期后的申请，申请人须依据本 CPS 规定的程序递交申请。

## 1.4 联络方式

邮寄地址：北京 349 信箱 6 分箱 CNNIC

邮政编码：100190

电话：86-10-58813000

传真：86-10-58812666

电子邮件地址：service@cnnic.cn

网址：http://www.cnnic.cn

中文域名：http://中国互联网络信息中心.CN

通用网址：中国互联网络信息中心:CNNIC

## 1.5 处理投诉程序

CNNIC 可信网络服务中心工作人员会尽快处理所有以书面及口头形式发起的投诉，并在五个工作日内给予详细的答复。若五个工作日内不能给予详细的答复，会向投诉人做出简要回复。在可行范围内，CNNIC 可信网络服务中心人员会在收到投诉后尽快以电话、电子邮件或信件与投诉人联络确认收到有关投诉并做出回复。

## 2 总则

### 2.1 义务

CNNIC 可信网络服务中心对证书持有者的义务由本 CPS 及与证书持有者达成的证书持有者协议进行约定。对于非证书持有者的证书信赖方，CNNIC 可信网络服务中心仅承诺采取合理技术避免根据本 CPS 签发、废止证书时对证书信赖方造成若干类型的损失及损害，并就责任做出限定。

#### 2.1.1 CNNIC可信网络服务中心认证中心（CA）义务

根据条例，CNNIC 可信网络服务中心为受认可的证书认证机构，负责使用稳定系统签发、废止证书及利用公开储存库发布证书撤销列表等信息。根据本 CPS，CNNIC 可信网络服务中心所属认证中心有下述义务：

- a) 接收注册中心的请求及时签发证书
- b) 废止证书并及时发布证书废止列表（CRL）（见第 4.5 节）

## 2.1.2 CNNIC可信网络服务中心注册中心（RA）义务

注册中心系统负责证书申请者证书的申请和审批及证书管理，并将证书申请信息传递到认证中心。注册中心有下述义务：

- a) 根据本 CPS 第 3、4 章规定，验证申请人所提交信息的准确性和真实性，并使验证通过的证书申请生效，将其安全传递给认证中心（CA），证书申请包括证书注册、补发、续费、废止、多域名修改等类型申请
- b) 通知申请人有关已批准或被拒绝的证书申请（见第 4.1、4.2、4.3 及 4.4 节）
- c) 通知证书持有者有关已废止的证书（见第 4.5.1、4.5.2 及 4.5.3 节）

CNNIC 可信网络服务中心仅有一个注册中心，设在 CNNIC。

CNNIC 可信网络服务中心确认 LRA 的身份，并授权 LRA 进行证书申请者注册的资料收集工作。LRA 有义务在证书申请者进行证书注册、补发、续费、废止、多域名修改时负责收集相关信息并初步验证这些信息的正确性。

## 2.1.3 储存库义务

CNNIC 可信网络服务中心储存库应根据自己制定的策略，及时公布证书废止列表（CRL）及其他内容。

## 2.1.4 证书持有者义务

证书持有者负责：

- a) 适当完成申请程序并在适当表格内签署或确定接受证书持有者协议；履行该协议规定其应承担的义务并确保在申请证书时所作的陈述准确无误。
- b) 准确地遵守本 CPS 所描述的关于完成证书的程序。
- c) 承诺使用合理预防措施来保护其证书私人密钥的机密性（即对其保密）及完整性以防丢失、泄露或未经授权使用。
- d) 发现其证书的私人密钥丢失或泄漏时，立即向 CNNIC 可信网络服务中心报告丢失或泄漏。
- e) 及时将证书持有者证书资料的任何变动通知给 CNNIC 可信网络服务中

- f) 出现下文 4.5.1 节所规定的废止证书的情形时，立即通知给 CNNIC 可信网络服务中心。
- g) 向 CNNIC 可信网络服务中心保证，并向所有证书信赖方表明，在证书的有效期内，以上第 1.3.2.1 节所描述的事实真实。
- h) 在明知 CNNIC 可信网络服务中心根据本 CPS 可能废止证书的情况下，或证书持有者已提出废止申请，或 CNNIC 可信网络服务中心拟根据本 CPS 废止证书并通知证书持有者后，均不得在交易中使用证书。
- i) 在明知 CNNIC 可信网络服务中心根据本 CPS 可能废止证书的情况下，或证书持有者提出废止申请，或 CNNIC 可信网络服务中心拟根据本 CPS 废止证书并通知证书持有者后，须立即通知从事当时仍有待完成的任何交易的证书信赖方，并明确说明，用于该交易的证书需要废止(由 CNNIC 可信网络服务中心或经证书持有者申请)，证书信赖方不得在交易中信任此证书。
- j) 证书的使用仅限于合法目的，并且符合相关的证书策略和本 CPS（或其他公布的商业事项）。如果注册者有理由相信与证书所用的公钥相对应的私钥有泄密的危险，那么应及时通知 CNNIC 可信网络服务中心废止证书。
- k) 证书持有者承认，如其未能按照上述条款的规定履行其义务，则其应对可能造成的 CNNIC 可信网络服务中心或其信赖方的损失承担赔偿责任。

## 2.1.5 信赖方义务

信任 CNNIC 可信网络服务中心数字证书的证书信赖方负责：

- a) 证书信赖方考虑过所有因素后并确信信任证书实属合理时，方可信任该证书。
- b) 在信任该证书前，确定使用证书是适合本 CPS 规定的用途，即仅信任 CNNIC 可信网络服务中心的证书用作域名证书。
- c) 在信任证书前查核证书废止列表（CRL）上的证书状态。
- d) 执行所有适当证书路径验证程序。
- e) 一旦信任了该证书，即表明同意接受本 CPS 所规定的责任限制的条款。

## 2.2 其它

### 2.2.1 合理技术及免责条款

CNNIC 可信网络服务中心将根据本 CPS 采取合理的技术及管理措施，向各证书持有者和信赖方行使其权利并履行其义务。CNNIC 可信网络服务中心不保证根据本 CPS 提供的服务不中断或无错误。

也就是说，尽管 CNNIC 可信网络服务中心或代表 CNNIC 可信网络服务中心的注册中心根据 CPS 行使应有的权利及义务时采取合理的技术及管理措施，若证书持有者或信赖方遭受出自 CPS 中描述的公开密钥基础设施或与之相关的任何性质的债务、损失或损害，各证书持有者同意 CNNIC 可信网络服务中心及其注册中心无需承担任何责任、损失或损害。

CNNIC 可信网络服务中心或代表 CNNIC 可信网络服务中心的注册中心已采取合理程度的技术及管理措施的前提下，若证书持有者因信任另一证书持有者由 CNNIC 可信网络服务中心所发出的证书支持的虚假或伪造的数字签名而蒙受损失或损害，CNNIC 可信网络服务中心或代表 CNNIC 可信网络服务中心的注册中心概不负责。

在 CNNIC 可信网络服务中心已采取合理的技术或管理手段以避免或减轻无法控制事件后果的前提下，若证书持有者因 CNNIC 可信网络服务中心不能控制的情况遭受不良影响，CNNIC 可信网络服务中心概不负责。CNNIC 可信网络服务中心控制以外的情况包括但不限于互联网或电信或其它基础设施系统的不可用，或天灾、战争、军事行动、国家紧急状态、疫症、火灾、水灾、地震、罢工或暴乱或其它证书持有者或其它第三者的疏忽或蓄意不当行为。

### 2.2.2 责任限制

#### 2.2.2.1 限制的合理性

各证书持有者或信赖方必须同意，CNNIC 可信网络服务中心按证书持有者协议及本 CPS 所列条件限制其法律责任实属合理。

### **2.2.2.2可追讨损失种类的限制**

CNNIC 可信网络服务中心若违反《证书持有者协议》或者出现任何职务职责的情况下，而造成证书持有者或信赖方遭受损失及损害的，CNNIC 可信网络服务中心不负责下述原因造成的损失及损害的赔偿：

- a) 任何直接或间接利润或收入损失、信誉或商誉损失或伤害、任何商机损失、失去项目、或失去或无法使用任何数据、设备或软件；
- b) 任何间接、相应而生或附带引起的损失或损害。

### **2.2.2.3限额**

即使是 CNNIC 可信网络服务中心违反《证书持有者协议》或者负有任何职务职责的情况下，而造成证书持有者或信赖方蒙受损失及损害，对于任何证书持有者、或任何信赖方，CNNIC 可信网络服务中心所负法律责任限于在任何情况下每张域名证书不得超过证书购买价格的 10 倍。

### **2.2.2.4提出赔偿的时限**

证书持有者或信赖方若向 CNNIC 提出赔偿请求，产生该赔偿请求之事由应与证书的签发、废止相关，并须在证书持有者或信赖方自知晓该事由之日起半年内提出；或自应该知晓此事由之日起半年内（若更早）提出。半年期限届满时，该赔偿请求必须放弃且绝对禁止。

### **2.2.2.5故意不当行为的责任**

任何因欺诈或故意不当行为的责任均不在本 CPS、证书持有者协议或 CNNIC 可信网络服务中心签发的证书的任何限制或除外规定范围内。

### **2.2.2.6证书责任限制通知**

CNNIC 可信网络服务中心签发证书已经作出如下责任限制通知：

“CNNIC 可信网络服务中心职员按 CNNIC 可信网络服务中心签署的证书业务规则所载条款，在条件适用于本证书的情况下，根据相关规定作为证书认证机构签发本证书。

因此，任何人士信任本证书前均应阅读适用于域名证书的证书业务规则（可浏览 <http://tns.cnnic.cn>）。中华人民共和国法律适用于本证书，信赖方须承认因信任本证书而引致的任何争议或问题属于中华人民共和国法律管辖。

如果信赖方不接受本证书用来签发的条款及条件，则不应信任本证书。

CNNIC 可信网络服务中心签发本证书，但无须对信赖方承担任何责任或职务职责。

信赖方信任本证书前确保信任行为公平合理无恶意，方可信任本证书；

信任本证书前，确定证书的使用就 CPS 规定的用途而言实属适当；

信任本证书前，根据证书废止列表（CRL）检查本证书的状态，并履行所有适当证书路径验证程序。

尽管 CNNIC 可信网络服务中心已采取合理技术及管理措施，若本证书仍在任何方面存在不准确或误导，则 CNNIC 可信网络服务中心对信赖方的任何损失或损害不承担任何责任。

若本证书在任何方面存在不准确或误导，而这种不准确或误导是因 CNNIC 可信网络服务中心的疏忽所导致，则 CNNIC 可信网络服务中心将可以因合理信任本证书中的这种不准确或误导事项而造成的经证实损失向每名信赖方支付最多为证书购买价格的 10 倍，只有这种损失不属于并且不包括（1）任何直接或间接损失，包括利润或收入损失、信誉或商誉损失或伤害、商机或契机损失、失去项目、失去或无法使用任何数据、设备或软件等；（2）任何间接、相应而生或偶然引起的损失或损害。在该等情况下根据条例适用于本证书的信任额度为证书购买价格的 10 倍。

证书持有者或信赖方若向 CNNIC 提出赔偿请求，产生该赔偿请求之事由应与证书的签发、废止相关，并须在证书持有者或信赖方自知晓该事由之日起半年内提出；或自应该知晓此事由之日起半年内（若更早）提出。半年期限届满时，该赔偿请求必须放弃且绝对禁止。

若本证书包含任何由 CNNIC 可信网络服务中心做出的故意或罔顾后果的失

实陈述，则本证书并不就这类对因合理信任本证书中的失实陈述而遭受损失的信赖方所应承担的法律责任做出任何限制。

本文所描述的法律限制不适用于个人伤害或死亡的（不大可能发生的）情形。”

### **2.2.3 CNNIC可信网络服务中心对已获接受但有缺陷的数字证书所承担的责任**

若证书持有者接受证书后发现，因证书包含的私人密钥或公开密钥出现差错，导致基于公开密钥基础设施的交易无法适当完成或根本无法完成，则证书持有者须将这种情况立即通知 CNNIC 可信网络服务中心，以便废止证书并重新签发。或者在接受证书后三个月内发现这种情况且证书持有者不再需要证书，则在 CNNIC 同意的前提下，可以申请退款。如果证书持有者在接受证书三个月后才将这类差错通知 CNNIC，则将不会退还持有者已缴纳的费用。

### **2.2.4 证书持有者的转让**

证书持有者不可转让证书持有者协议或证书赋予的权利，任何转让行为均属无效。

### **2.2.5 陈述权限**

除非获得 CNNIC 可信网络服务中心授权，CNNIC 可信网络服务中心或注册中心的代理人或工作人员无权代表 CNNIC 可信网络服务中心对本 CPS 的含义或解释作任何陈述。

### **2.2.6 更改**

CNNIC 可信网络服务中心有权更改本 CPS，而无须发出预先通知(见第 2.2.8 节)。证书持有者协议不得做出修改或变更，除非符合本 CPS 中的修改或变更规定，或获得 CNNIC 可信网络服务中心的明确书面同意。

## 2.2.7 保留所有权

根据本 CPS 签发的证书上所有资料的实体权利、版权及知识产权均属 CNNIC 可信网络服务中心所有。

## 2.2.8 条款冲突

若本 CPS 与证书持有者协议或其它规则、指引、协议有冲突，证书持有者、信赖方及 CNNIC 可信网络服务中心须受本 CPS 条款约束，除非该等条款受法律禁止。

## 2.2.9 受信关系

CNNIC 可信网络服务中心或代表 CNNIC 可信网络服务中心的注册中心并非证书持有者或信赖方的代理人或其它代表。证书持有者及信赖方无权以协议或其它方式约束 CNNIC 可信网络服务中心或代表 CNNIC 可信网络服务中心的注册中心承担证书持有者或信赖方的代理人或其它代表的责任。

## 2.2.10 交叉认证

CNNIC 可信网络服务中心在所有情形下均保留与其他证书认证机构定义及确定适当理由进行相互交叉认证的权利。

通过与 Entrust 公司之间的协议，CNNIC 可信网络服务中心中级根证书 CNNIC SSL 同时也被 Entrust 公司的根证书所信任，CNNIC 可信网络服务中心所发出的域名证书可以通过不同的证书路径分别从 CNNIC 根证书和 Entrust 根证书两个信任锚进行认证。

## 2.3 解释及执行（管辖法律）

### 2.3.1 管辖法律

本 CPS 受中华人民共和国法律管辖。

## 2.3.2 条款可中止性、修改

若本 CPS 的任何条款被宣布为非法、不可执行或无效，则应删除其中任何非法的词语，直至该等条款成为合法及可执行为止，同时应保留该等条款的本意。本 CPS 的任何条款的不可执行性将不损害任何其它条款的可执行性。

CNNIC 可信网络服务中心拆分或合并可能导致其经营范围、管理和运营状况的改变。这种情况下，可能也需要修改本 CPS。经营活动的改变会与 CPS 的修改相一致。

## 2.3.3 争议解决程序

若当事人之间的争议无法友好协商解决，应提交中国国际经济贸易仲裁委员会进行仲裁。仲裁的裁决是终局性的，对当事人均有约束力。仲裁的裁决过程采用中文记录，仲裁裁决由有管辖权的法院执行。

## 2.4 证书费用

### 2.4.1 高级证书

高级证书（包括单域名证书、通配域名证书、多域名证书）注册、续费、补发，以及多域名证书域名修改为收费服务，其费用根据市场和管理部门的规定自行决定。

### 2.4.2 查询

CNNIC 可信网络服务中心证书查询现阶段为免费服务。

### 2.4.3 废止

CNNIC 可信网络服务中心证书废止现阶段为免费服务。

## 2.4.4 退款策略

CNNIC 可信网络服务中心证书费用在证书签发后概不退还。

## 2.4.5 其他费用

CNNIC 可信网络服务中心除收取证书注册费、更新费（续费）、补发费、多域名证书域名修改费用外，暂不收取其他费用。

## 2.5 公布资料及储存库

本文为 CNNIC 可信网络服务中心证书业务规则（CPS），在 CNNIC 可信网络服务中心网站发布，CNNIC 可信网络服务中心网址为

<http://tns.cnnic.cn>

CNNIC 可信网络服务中心维持一个储存库，包含最新的根和中级根所签发的证书废止列表（CRL）、CNNIC 可信网络服务中心中级根证书和根证书、本 CPS 以及 CNNIC 可信网络服务中心证书策略（CP）文本一份以及其它相关资料。

除每周最多四小时的定期维修及紧急维修外，储存库保持每天 24 小时、每周 7 天开放。CNNIC 可信网络服务中心储存库可通过下述 URL 访问：

<http://tns.cnnic.cn>

CNNIC 可信网络服务中心也通过 LDAP 目录服务发布中级根签发的最新 CRL，LDAP 访问地址是：

<ldap://tnsldap.cnnic.cn>

公布资料和储存库允许所有互联网用户访问，但仅允许 CNNIC 可信网络服务中心管理员更新。

### 2.5.1 证书储存库控制

储存库所在位置可供在线浏览，并可防止擅自修改。

## 2.5.2 证书储存库进入要求

经授权的 CNNIC 可信网络服务中心工作人员方可进入储存库更新及修改内容。

## 2.5.3 证书储存库更新周期

CNNIC 可信网络服务中心储存库内中级根签发的证书废止列表（CRL）每 12 小时更新一次。

如果没有进行中级根的废止，根签发的证书废止列表（CRL）每 6 个月（182 天）更新一次，在进行中级根的废止后，根签发的证书废止列表（CRL）立即更新。

储存库中其他内容根据变更情况随时更改。

## 2.6 遵从规定的评估

根据中华人民共和国的相关法律的规定，至少每 12 个月进行一次由外部独立的审计机构主持进行的规定遵从情况的评估，查清 CNNIC 可信网络服务中心签发、废止证书及公布证书废止列表（CRL）的系统是否严格遵守本 CPS 和 CNNIC 可信网络服务中心相关的控制措施。

审计内容包括：

- a) 公布的商业事项
- b) 服务的完整性（包括对密钥和证书生命周期管理的控制）
- c) 环境控制

审计结果应通报给 CNNIC 可信网络服务中心安全管理委员会。由其安排 CNNIC 可信网络服务中心将根据具体的审计意见确定改进方案，采取改进行动。

## 2.7 机密性

保密信息包括：

- a) 证书持有者的签名私钥是保密的，不向 CNNIC 可信网络服务中心提供

- b) CNNIC 可信网络服务中心的经营和控制专用的信息，都由 CNNIC 可信网络服务中心秘密保管；除非法律另有规定，否则不能对外泄漏。
- c) 除在证书、CRL、证书政策、CPS 中公开发布的信息之外的有关证书持有者的信息，是保密信息；除非有证书政策要求，或法律另行规定，否则一律不能对外公开。
- d) 一般来说，每年的审计结果应该保密，除非 CNNIC 可信网络服务中心安全管理委员会认为有必要公布审计结果。

非保密信息包括：

- a) 由 CNNIC 可信网络服务中心签发的证书以及 CRL 中所包括的信息是非保密信息。
- b) CNNIC 可信网络服务中心公布的 CPS 中的信息（或其他公布的商业事项）是非保密信息。
- c) 当 CNNIC 可信网络服务中心废止某一证书时，CRL 中列出了证书的废止理由。该废止理由的代码是非保密信息，所有其他证书持有者和证书信赖方都可以分享该信息。但是，有关废止的其他细节一般不公布。

CNNIC 可信网络服务中心将根据法律规定，应执法人员的执法要求公开信息。

CNNIC 可信网络服务中心将根据信息持有人要求向其他方公布有关信息持有人的信息。

## 3 鉴别及认证

### 3.1 命名

#### 3.1.1 名称类型

根据证书对应实体的类型不同，CNNIC 可信网络服务中心签发的证书的实体名字可以是单个域名或多个域名，命名符合 X.500 甄别名规定。

CNNIC 可信网络服务中心所发证书的签发者和主题域中包含 X.500 甄别名。

CNNIC 可信网络服务中心所发证书的主题甄别名由下面的内容组成：

CNNIC 可信网络服务中心根证书主题甄别名

- 国家(C) = CN
- 机构(O) = CNNIC
- 通用名(CN) = CNNIC ROOT

CNNIC 可信网络服务中心中级根证书主题甄别名

- 国家(C) = CN
- 机构(O) = CNNIC SSL
- 通用名(CN) = CNNIC SSL

域名证书的主题域中包含一个 X.500 甄别名，它由如下的内容组成：

- 国家(C) = CN
- 机构(O) = 证书持有者名称
- 组织单元(OU)=SingleDomain（单域名证书或通配域名证书）或 MultiDomain（多域名证书）
- 通用名(CN) = 这个属性包括  
    单个域名（单域名证书或通配域名证书）或多域名的并列（多域名证书）

### 3.1.2 名称要求

CNNIC 可信网络服务中心签发的证书包含的命名应由域名、证书持有者名称与 CNNIC 可信网络服务中心证书固定的内容构成。

### 3.1.3 申请者的匿名或伪名

申请者不能使用匿名或伪名申请证书，证书中也不能使用匿名或伪名。

### 3.1.4 理解不同名称形式的规则

依 X.500 甄别名命名规则解释。

### 3.1.5 名称唯一性

CNNIC 可信网络服务中心签发给某个实体的证书, 其主题甄别名, 在 CNNIC 可信网络服务中心信任域内是唯一的。

### 3.1.6 商标的识别、鉴证和角色

CNNIC 可信网络服务中心签发的证书的主题甄别名只与域名、证书持有者名称相关, 而与商标无关。

### 3.1.7 名称争端解决

名称争端由 CNNIC 可信网络服务中心根据具体情况进行最终裁决。

## 3.2 高级证书首次注册

### 3.2.1 单域名, 通配域名证书

#### 1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员:

对于独立服务器 (安装证书的服务器是由证书申请者自行管理的, 下同), 申请资料包括以下文档:

- 证书申请者身份证明:
  - 企业提供: 组织机构代码证复印件或企业法人营业执照复印件 (每页加盖公章);
  - 政府机关提供: 组织机构代码证复印件或机关法人证书复印件 (每页加盖公章);
  - 事业单位提供: 组织机构代码证复印件或事业单位法人证书复印件 (每页加盖公章);
  - 社团组织提供: 组织机构代码证复印件或社会团体法人登记证书复印件 (每页加盖公章)。
  - 自然人提供: 有效个人身份证明复印件。
- 证书注册申请书原件。
- 证书申请者为企业/政府机关/事业单位/社团组织时, 还需提交主管人和

对于托管服务器（安装证书的服务器是由证书申请者委托其他机构代为管理的，下同），证书申请由受托机构代为办理，申请资料包括以下文档：

- 受托机构的企业法人营业执照或组织机构代码证复印件，每页均加盖受托机构公章。
  - 证书申请者身份证明。
    - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
    - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
    - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
    - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
    - 自然人提供：有效个人身份证明复印件。
  - 证书注册申请书原件。
  - 受托机构经办人身份证明复印件。
  - 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人身份证明复印件。
2. 本地受理点录入员进行初步审核。通过域名注册信息查询(whois)功能，得到所申请域名证书的域名注册者资料，查看域名注册者是否和域名证书申请者一致，初步审核确定域名证书申请者确实拥有此域名。
  3. 本地受理点录入员初步审核通过后，通过 RA 系统将上述资料录入，提交申请，并将全部纸质申请资料通过安全方式递交给 CNNIC 注册中心的 RA 审核员。初步审核不通过，则要求域名证书申请者修改域名注册者资料后再前来申请证书。
  4. RA 审核员检验合法的域名持有者是否与证书申请者相符合（同样使用 whois 功能），审核资料是否真实，并与 RA 系统中的申请信息对比。通过电话分别与主管人、经办人进行确认。
  5. 如果确认通过，RA 审核员登录 RA 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，

### 3.2.2 多域名证书

#### 1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员:

对于独立服务器，申请资料包括以下文档：

- 证书申请者身份证明：
  - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
  - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
  - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
  - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
  - 自然人提供：有效个人身份证明复印件。
- 证书注册申请书原件。
- 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人和经办人的身份证明复印件。

对于托管服务器，申请资料包括以下文档：

- 受托机构的企业法人营业执照或组织机构代码证复印件，每页均加盖受托机构公章。
- 所有证书申请者身份证明。
  - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
  - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
  - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
  - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。

- 自然人提供：有效个人身份证明复印件。
  - 证书注册申请书原件。
  - 受托机构经办人身份证明复印件。
  - 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人身份证明复印件。
2. 本地受理点录入员进行初步审核。通过域名注册信息查询(whois)功能，得到多域名证书的所有域名注册者资料，查看这些域名注册者是否分别和域名证书申请者一致，初步审核确定各域名证书申请者确实拥有此域名。
  3. 本地受理点录入员初步审核通过后，通过 RA 系统将上述资料录入，提交申请，并将全部纸质申请资料通过安全方式递交给 CNNIC 注册中心的 RA 审核员。初步审核不通过，即某域名证书申请者与域名注册者不一致，则要求此域名证书申请者修改域名注册者资料，然后受托机构才能再次前来申请多域名证书，或者在此多域名证书内去掉资料不一致的域名。
  4. RA 审核员检验合法的域名持有者是否与证书申请者相符合(同样使用 whois 功能)，审核资料是否真实，并与 RA 系统中的申请信息对比。通过电话分别与主管人、经办人进行确认。
  5. 如果确认通过，RA 审核员登录 RA 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，并制作纸质“高级版网址卫士证书核准证明”。如果未确认通过，则拒绝证书注册申请，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和申请经办人联系交涉，按照拒绝原因进行相应修改，重新进行申请。

### 3.3 证明拥有私钥的方法

CNNIC 可信网络服务中心通过使用附带数字签名的 PKCS#10 格式的证书请求，验证证书申请者拥有与证书公钥对应的私钥。

## 4 操作规范

### 4.1 高级证书申请、签发、接受及发布

#### 4.1.1 证书申请

##### 4.1.1.1 处理申请

申请域名证书的经办人必须到 CNNIC 指定的 CNNIC 可信网络服务中心本地受理点处递交申请。CNNIC 可信网络服务中心（包括注册中心）不直接面对申请者接受申请。

##### 4.1.1.2 身份审核

用以证明证书持有者机构、经办人及经办人身份的文件，在本 CPS 第 3.2 节说明，申请者需要按照本 CPS 第 3.2 节进行申请操作。CNNIC 可信网络服务中心注册中心完成核对身份手续后，将下载证书所必须的参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，同时通过安全邮递方式将纸质“高级版网址卫士证书核准证明”发送给证书申请经办人。

### 4.1.2 签发、接受证书

#### 4.1.2.1 单域名，通配域名证书

单域名及通配域名证书的签发、接受的步骤如下：

1. 证书申请经办人在 Web 服务器中生成证书请求 CSR。
2. 证书申请经办人访问 CNNIC 证书下载页面，提交 CSR，并输入参考号、授权码。
3. CNNIC 可信网络服务中心系统自动检查 CSR 的完整性。
4. CNNIC 可信网络服务中心签发证书，由证书申请经办人下载安装。
5. CNNIC 可信网络服务中心签发证书完成即表明申请者接受 CNNIC 可信

网络服务中心的服务。

#### 4.1.2.2 多域名证书

多域名证书的签发、接受的步骤如下：

1. 证书申请经办人在 Web 服务器中生成证书请求 CSR。
2. 证书申请经办人访问 CNNIC 证书下载页面，提交 CSR，并输入参考号、授权码。
3. CNNIC 可信网络服务中心系统自动检查 CSR 的完整性。
4. CNNIC 可信网络服务中心签发证书，由证书申请经办人下载安装。
5. CNNIC 可信网络服务中心签发证书完成即表明申请者接受 CNNIC 可信网络服务中心的服务。

#### 4.1.3 证书发布

CNNIC 可信网络服务中心所发放的域名证书不在储存库中发布，但可以通过 CNNIC 可信网络服务中心网站查询域名证书注册信息。

### 4.2 高级证书补发

在 CNNIC 可信网络服务中心的证书体系中，证书补发需要重新产生证书请求文件 CSR，同时 CNNIC 可信网络服务中心要求使用与原来密钥对不同的密钥对进行申请，不允许使用旧的证书请求文件。

新证书补发后，原证书立即作废，新证书截至有效期与原证书相同。

#### 4.2.1 单域名，通配域名证书补发

1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员：  
对于独立服务器，申请资料包括以下文档：
  - 证书补发申请书原件。
  - 证书申请者为自然人时，提交有效个人身份证明复印件；申请者为企业/政府机关/事业单位/社团组织时，提交单位主管人、经办人的身份证明复

印件。

对于托管服务器，申请资料包括以下文档：

- 证书补发申请书原件。
- 受托机构经办人身份证明复印件。

2. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
3. 本地受理点录入员将全部申请资料通过安全方式递交给 CNNIC 注册中心的 RA 审核员。
4. RA 审核员审核资料并与 RA 系统中的申请信息和域名证书原注册信息对比。通过电话分别与主管人（如有）、经办人进行确认。
5. 如果确认通过，RA 审核员登录 RA 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，并制作纸质“高级版网址卫士证书核准证明”。如果未确认通过，则拒绝证书补发，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和申请经办人联系交涉，按照拒绝原因进行相应修改，重新申请补发。
6. 纸质“高级版网址卫士证书核准证明”通过安全邮递方式发送给证书申请经办人。
7. 证书申请经办人在 Web 服务器中生成证书请求 CSR。
8. 证书申请经办人访问 CNNIC 证书下载页面，提交 CSR，并输入参考号、授权码。
9. CNNIC 可信网络服务中心签发证书，由证书申请经办人安装。

## 4.2.2 多域名证书补发

1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员：

对于独立服务器，申请资料包括以下文档：

- 证书补发申请书原件。
- 证书申请者为自然人时，提交有效个人身份证明复印件；申请者为企业/政府机关/事业单位/社团组织时，提交单位主管人、经办人的身份证明复印件。

对于托管服务器，申请资料包括以下文档：

- 证书补发申请书原件。
  - 受托机构经办人身份证明复印件。
2. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
  3. 本地受理点录入员将全部申请资料通过安全方式递交给 CNNIC 注册中心的 RA 审核员。
  4. RA 审核员审核资料并与 RA 系统中的申请信息和域名证书原注册信息对比。通过电话与主管人（如有）、经办人进行确认。
  5. 如果确认通过，RA 审核员登录 RA 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，并制作纸质“高级版网址卫士证书核准证明”。如果未确认通过，则拒绝证书补发，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和申请经办人联系交涉，按照拒绝原因进行相应修改，重新申请补发。
  6. 纸质“高级版网址卫士证书核准证明”通过安全邮递方式发送给证书申请经办人。
  7. 证书申请经办人在 Web 服务器中生成证书请求 CSR。
  8. 证书申请经办人访问 CNNIC 证书下载页面，提交 CSR，并输入参考号、授权码。
  9. CNNIC 可信网络服务中心签发证书，由证书申请经办人安装。

### 4.3 高级证书续费

在证书持有者证书到期前，证书持有者需要获得新的证书以保持证书使用的连续性。证书持有者产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，证书持有者希望为一个现存的密钥对申请一个新证书，称作“证书更新”。

在 CNNIC 可信网络服务中心的证书体系中，证书续费需要证书持有者重新产生证书请求文件 CSR，同时 CNNIC 可信网络服务中心要求证书持有者使用与原来密钥对不同的密钥对进行申请，不允许使用旧的证书请求文件 CSR(即必须进行“密钥更新”)。

证书续费期为当前证书失效前 3 个月内，在此之前或之后 CNNIC 可信网络服务中心将拒绝续费申请。

续费之后，新的证书下载后应该立即安装。续费的有效期顺延：新证书失效期 = 当前时间 + 新购证书的时间长度 + 当前证书剩余的时间长度。

### 4.3.1 单域名，通配域名证书续费

#### 1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员：

对于独立服务器，申请资料包括以下文档：

- 证书申请者身份证明：
  - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
  - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
  - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
  - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
  - 自然人提供：有效个人身份证明复印件。
- 证书续费申请书原件。
- 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人和经办人的身份证明复印件。

对于托管服务器，申请资料包括以下文档：

- 受托机构的企业法人营业执照或组织机构代码证复印件，每页均加盖受托机构公章。
- 证书申请者身份证明。
  - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
  - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
  - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；

- 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
  - 自然人提供：有效个人身份证明复印件。
  - 证书续费申请书原件。
  - 受托机构经办人身份证明复印件。
  - 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人身份证明复印件。
2. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
  3. 本地受理点录入员将全部申请资料通过安全方式递交给 CNNIC 注册中心的 RA 审核员。
  4. RA 审核员审核资料并与 RA 系统中的申请信息和域名证书原注册信息对比。通过电话分别与主管人、经办人进行确认。
  5. 如果确认通过，RA 审核员登录 RA 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，并制作纸质“高级版网址卫士证书核准证明”。如果未确认通过，则拒绝证书续费，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和申请经办人联系交涉，按照拒绝原因进行相应修改，重新申请续费。
  6. 纸质“高级版网址卫士证书核准证明”通过安全邮递方式发送给证书申请经办人。
  7. 证书申请经办人在 Web 服务器中生成证书请求 CSR。
  8. 证书申请经办人访问 CNNIC 证书下载页面，提交 CSR，并输入参考号、授权码。
  9. CNNIC 可信网络服务中心签发证书，由证书申请经办人安装。

### 4.3.2 多域名证书续费

1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员：  
对于独立服务器，申请资料包括以下文档：
  - 证书申请者身份证明：
    - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；

- 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
  - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
  - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
  - 自然人提供：有效个人身份证明复印件。
- 证书续费申请书原件。
  - 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人和经办人的身份证明复印件。

对于托管服务器，申请资料包括以下文档：

- 受托机构的企业法人营业执照或组织机构代码证复印件，每页均加盖受托机构公章。
  - 所有证书申请者身份证明。
    - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
    - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
    - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
    - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
    - 自然人提供：有效个人身份证明复印件。
  - 证书续费申请书原件。
  - 受托机构经办人身份证明复印件。
  - 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人身份证明复印件。
2. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
  3. 本地受理点录入员将全部申请资料通过安全方式递交给 CNNIC 注册中心的 RA 审核员。
  4. RA 审核员审核资料并与 RA 系统中的申请信息和域名证书原注册信息对比。通过电话分别与主管人、经办人进行确认。

5. 如果确认通过，RA 审核员登录 RA 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，并制作纸质“高级版网址卫士证书核准证明”。如果未确认通过，则拒绝证书续费，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和申请经办人联系交涉，按照拒绝原因进行相应修改，重新申请续费。
6. 纸质“高级版网址卫士证书核准证明”通过安全邮递方式发送给证书申请经办人。
7. 证书申请经办人在 Web 服务器中生成证书请求 CSR。
8. 证书申请经办人访问 CNNIC 证书下载页面，提交 CSR，并输入参考号、授权码。
9. CNNIC 可信网络服务中心签发证书，由证书申请经办人安装。

## 4.4 多域名证书域名修改

多域名证书提供域名修改服务，可以增加、删除和修改域名：

1. 证书申请经办人提交申请资料给本地受理点(LRA)录入员：  
对于独立服务器，申请资料包括以下文档：
  - 证书申请者身份证明：
    - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
    - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
    - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
    - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
    - 自然人提供：有效个人身份证明复印件。
  - 多域名证书修改申请书原件。
  - 证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人和经办人的身份证明复印件。

对于托管服务器，申请资料包括以下文档：

- 新增的域名证书申请者身份证明。
    - 企业提供：组织机构代码证复印件或企业法人营业执照复印件（每页加盖公章）；
    - 政府机关提供：组织机构代码证复印件或机关法人证书复印件（每页加盖公章）；
    - 事业单位提供：组织机构代码证复印件或事业单位法人证书复印件（每页加盖公章）；
    - 社团组织提供：组织机构代码证复印件或社会团体法人登记证书复印件（每页加盖公章）。
    - 自然人提供：有效个人身份证明复印件。
  - 多域名证书修改申请书原件。
  - 受托机构经办人身份证明复印件。
  - 新增的域名证书申请者为企业/政府机关/事业单位/社团组织时，还需提交主管人身份证明复印件。
2. 本地受理点录入员通过 **RA** 系统将上述资料录入，提交申请。
  3. 本地受理点录入员将全部申请资料通过安全方式递交给 CNNIC 注册中心的 **RA** 审核员。
  4. **RA** 审核员检验合法的域名持有者是否与证书申请者相符合，审核资料是否真实，并与 **RA** 系统中的申请信息对比。通过电话分别与主管人、经办人进行确认。
  5. 如果确认通过，**RA** 审核员登录 **RA** 系统，批准该证书申请，将参考号、授权码的前 13 位通过电子邮件、后 3 位通过手机分别发送给证书申请经办人，并制作纸质“高级版网址卫士证书核准证明”。如果未确认通过，则拒绝域名修改申请，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和申请经办人联系交涉，按照拒绝原因进行相应修改，重新申请域名修改。
  6. 纸质“高级版网址卫士证书核准证明”通过安全邮递方式发送给证书申请经办人。
  7. 证书申请经办人在 **Web** 服务器中生成证书请求 **CSR**。
  8. 证书申请经办人访问 CNNIC 证书下载页面，提交 **CSR**，并输入参考号、授权码。
  9. CNNIC 可信网络服务中心签发证书，由证书申请经办人安装。

\*注：域名变更后，原证书马上作废，新的证书下载后必须马上安装，证书有效期与原证书相同。

## 4.5 证书废止

### 4.5.1 废止的情形

如果出现下列情况，CNNIC 可信网络服务中心有权废止所签发的域名证书：

1. 事后检查发现证书持有者申请域名证书时提供的资料存在虚假信息；
2. 证书持有者未履行证书持有者协议所约定的义务；
3. 证书持有者要求废止域名证书；
4. 证书持有者主体消亡；
5. 证书持有者变更域名证书的用途；
6. 法律或法规要求的其他情况。

### 4.5.2 废止程序

如出现本文第 4.5.1 节规定的除第 3 条外的情况，CNNIC 可信网络服务中心将主动废止域名证书并通知证书持有者。

证书持有者也有权自行申请废止证书，申请废止的流程如下：

#### 4.5.2.1 单域名，通配域名证书废止

1. 证书持有者提交纸质证书废止申请资料给本地受理点(LRA)录入员。  
对于独立服务器，申请资料包括：
  - 证书废止申请书原件。
  - 申请者为自然人时，提交有效个人身份证明复印件；申请者为企业/政府机关/事业单位/社团组织时，提交单位主管人、经办人的身份证明复印件。对于托管服务器，申请资料包括：
  - 证书废止申请书原件。

- 受托机构经办人身份证明复印件。
- 2. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
- 3. 本地受理点录入员将全部申请资料通过安全方式交给 CNNIC 注册中心的 RA 审核员。
- 4. RA 审核员审核资料并与 RA 系统中的申请信息和域名证书原注册信息对比。通过电话分别与主管人（如有）、经办人进行确认。
- 5. 如果审核通过，RA 审核员直接废止此域名证书。如果审核不通过，则拒绝证书废止，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和经办人者联系交涉，按照拒绝原因进行相应修改，重新申请废止。

#### 4.5.2.2 多域名证书废止

1. 证书持有者提交纸质证书废止申请资料给本地受理点(LRA)录入员。  
对于独立服务器，申请资料包括：
  - 证书废止申请书原件。
  - 申请者为自然人时，提交有效个人身份证明复印件；申请者为企业/政府机关/事业单位/社团组织时，提交单位主管人、经办人的身份证明复印件。对于托管服务器，申请资料包括：
  - 证书废止申请书原件。
  - 受托机构经办人身份证明复印件。
2. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
3. 本地受理点录入员将全部申请资料通过安全方式交给 CNNIC 注册中心的 RA 审核员。
4. RA 审核员审核资料并与 RA 系统中的申请信息和域名证书原注册信息对比。通过电话与主管人（如有）、经办人进行确认。
5. 如果审核通过，RA 审核员直接废止此域名证书。如果审核不通过，则拒绝证书废止，发回所有资料给本地受理点，并附加拒绝的理由。由本地受理点和证书申请者联系交涉，按照拒绝原因进行相应修改，重新申

请废止。

### 4.5.3 废止效力

CNNIC 可信网络服务中心把废止状态发布到证书废止列表（CRL）中，即终止某一证书的使用效力。

### 4.5.4 请求证书废止的实体

CNNIC 可信网络服务中心或证书持有者可以在 CPS 第 4.5.1 节所述情形下要求废止一个证书。

### 4.5.5 废止请求的流程

当 CNNIC 可信网络服务中心有充分的理由相信需要废止证书时，CNNIC 可信网络服务中心认证中心或注册中心的有关人员可以通过内部确定的流程提交废止证书的请求。在证书废止后，CNNIC 可信网络服务中心将通过适当的方式，包括邮件、传真等，通知证书持有者证书已被废止及被废止的理由。

证书持有者也可以通过废止程序自行要求废止自己的证书。在证书持有者提交废止请求时，需同时提供证书申请时提供的资料作为身份鉴别的信息。

### 4.5.6 废止请求提出时限

当发现出现 CPS 第 4.5.1 节中的情况时，从发现需要废止证书到提出废止请求的时间间隔，不应超过 24 小时。

### 4.5.7 CNNIC可信网络服务中心处理废止请求的时限

CNNIC 可信网络服务中心注册中心(RA)从接到废止请求（包括纸质资料）到完成处理请求的时间，不能超过两个工作日。CNNIC 可信网络服务中心工作日不包括周末和国家法定假日。

## 4.5.8 信赖方检查证书废止的要求

信赖方是否检查证书废止完全取决于信赖方的安全要求。

## 4.5.9 CRL发布频率

CNNIC 可信网络服务中心中级根每隔 12 个小时签发一次证书废止列表 (CRL)。

## 4.5.10 如果没有进行中级根的废止，根签发的证书废止列表 (CRL) 每 6 个月 (182 天) 更新一次，在进行中级根的废止后，根签发的证书废止列表 (CRL) 立即更新。CRL发布的最大滞后时间

一个域名证书从它被废止到它被发布到 CRL 上的滞后时间不超过 12 小时。如果中级根被废止，根签发的 CRL 则立即发布。

## 4.5.11 在线状态查询的可用性

CNNIC 可信网络服务中心提供证书状态的在线查询服务 (OCSP)，每周除最多四小时的定期维修及紧急维修外，该服务 7×24 小时可用。

## 4.5.12 在线状态查询要求

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查询系统检查该证书的状态。

## 4.5.13 废止信息的其他发布形式

CNNIC 可信网络服务中心目前只提供 OCSP 查询，以及通过 LDAP 目录服务和 HTTP 服务提供 CRL 查询。

## 4.5.14 密钥损害的特别要求

无论是证书持有者还是 CNNIC 可信网络服务中心，发现证书密钥受到安全损害时应立即废止证书。

## 4.6 证书冻结

不适用。CNNIC 可信网络服务中心不支持证书冻结。

## 4.7 证书更新

不适用。CNNIC 可信网络服务中心不支持密钥不更换的情况下的证书更新。

## 4.8 证书发布

CNNIC 可信网络服务中心所发放的域名证书不在储存库中发布，但可以通过 CNNIC 可信网络服务中心网站查询域名证书注册信息。

## 4.9 计算机安全审计程序

### 4.9.1 记录事件类型

CNNIC 可信网络服务中心的重要安全事件，均以人工或自动记录在受保护的审计追踪记录内。这类事件包括但不限于以下内容：

- ◆ 可疑网络活动
- ◆ 多次试图进入而不能访问
- ◆ 与安装设备或软件、修改及配置 CNNIC 可信网络服务中心系统的有关事件
- ◆ 相关人员访问 CNNIC 可信网络服务中心各组成部分的过程

定期管理证书的操作同样也包括在审计追踪记录中，这些操作包括但不限于以下内容：

- ◆ 处理废止证书的请求

- ◆ 实际发出（包括证书注册、续费、补发等）、废止证书
- ◆ 更新储存库资料
- ◆ 汇编证书废止列表（CRL）并刊登新数据
- ◆ 证书认证中心密钥转换
- ◆ 档案备份
- ◆ 紧急密钥恢复

## 4.9.2 处理记录的次数

CNNIC 可信网络服务中心每周均会处理审计追踪记录，用以审计追踪有关 CNNIC 可信网络服务中心行动、交易及程序。

## 4.9.3 审计追踪记录保存期限

存盘审计追踪记录文件的保存期为 10 年。

## 4.9.4 审计追踪记录保护

CNNIC 可信网络服务中心处理审计追踪记录时实施多人式控制，可提供足够保护，避免有关记录意外受损或被人蓄意修改。

## 4.9.5 审计追踪记录备份

CNNIC 可信网络服务中心每周均会按照预定程序为审计追踪记录作适当备份。备份会另行离机储存，并获足够保护，以免被盗用、损毁及媒体衰变。

## 4.9.6 审计追踪记录收集系统

无

## 4.9.7 安全事件通知

CNNIC 可信网络服务中心拥有自动监控系统，可向 CNNIC 可信网络服务中

心适当人士或系统报告重要安全事件。

## 4.9.8 脆弱性评估

脆弱性评估是 CNNIC 可信网络服务中心风险评估的一部份：根据审计记录，CNNIC 可信网络服务中心定期进行技术安全、管理安全方面的脆弱性评估，并根据评估报告采取加固措施。

## 4.10 记录归档

### 4.10.1 归档记录类型

CNNIC 可信网络服务中心须确保归档记录包括足够资料，从而确定证书是否有效以及以往是否运行妥当。CNNIC 可信网络服务中心应保存有以下数据：

- ◆ 系统设备结构档案
- ◆ 评估结果及设备合格复查记录
- ◆ 证书业务规则所有版本
- ◆ 对 CNNIC 可信网络服务中心具约束力的协议
- ◆ 所有发出的证书及证书废止列表（CRL）
- ◆ 定期事件记录
- ◆ 其它用以核实归档内容的工作日志

### 4.10.2 归档保存期限

上述归档记录至少妥善保存 10 年。审计跟踪文档以 CNNIC 可信网络服务中心视为适当的方式存放。

### 4.10.3 归档保护

CNNIC 可信网络服务中心保存的归档介质受各种实体或加密措施保护，可避免未经授权进入。保护措施用以保护归档介质免受温度、湿度及磁场等环境侵害。

#### 4.10.4 归档备份程序

制作并保存归档的副本。

#### 4.10.5 时间戳

归档资料均注明归档项目的开始时间及日期。CNNIC 可信网络服务中心利用控制措施防止擅自调校系统时钟。

### 4.11 密钥变更

由 CNNIC 可信网络服务中心认证中心产生，并用以证明根据本 CPS 发出的证书的认证中心根密钥及证书寿命为期不超过二十年。CNNIC 可信网络服务中心证书认证机构密钥及证书在期满前至少三个月会进行更新。更新为新根密钥后，相关的根证书也会公布供大众取用。原先的根密钥则保留至第 4.10.2 节指定的最短的时限，以供核对用原根密钥签名的证书。

### 4.12 CNNIC可信网络服务中心服务终止

在 CNNIC 可信网络服务中心服务终止的情况下，CNNIC 可信网络服务中心将废止所有由 CNNIC 可信网络服务中心发布的证书。并将 CNNIC 可信网络服务中心的归档记录移交给法律法规规定的机构。

在终止服务后，CNNIC 可信网络服务中心会将证书认证机构的记录存盘 10 年（由终止服务日起计）；这些记录包括根证书和中级根证书、已发出的域名证书、证书业务规则及证书废止列表（CRL）。

### 4.13 灾难恢复及密钥泄漏计划

#### 4.13.1 灾难恢复计划

CNNIC 可信网络服务中心已经准备了妥善的业务连续性计划，包括每天备份主要业务信息和认证中心系统数据，并适当地备份认证中心系统的软件，以维持

主要业务持续运营，保障在严重故障或灾难影响下仍可继续提供服务或在最短时间内恢复提供服务。

每年都会对业务连续性计划进行复查，并严格执行。

CNNIC 可信网络服务中心在异地设有一个灾难恢复基地。如发生严重故障或灾难，CNNIC 可信网络服务中心会及时通知政府部门，并公布运营由生产基地转至灾难恢复基地。

在发生灾难后但稳妥可靠的环境尚未重新确立前：

- ◆ 敏感性材料或仪器会安全地锁在设施内；
- ◆ 若不能将敏感性材料或仪器安全地锁在设施内或这些物资或仪器有受损毁的风险，这些材料或仪器会移离设施并锁在其它临时设施内；
- ◆ 设施的出入会实行访问控制，以防范盗窃或被人擅自访问。

### 4.13.2 密钥泄漏应对计划

业务连续性计划包含处理密钥泄漏的应对计划。这些计划每年均会进行复检。

如根据本 CPS 用来签发域名证书的 CNNIC 可信网络服务中心根证书或中级根证书私钥信息泄漏，CNNIC 可信网络服务中心会及时进行公布。CNNIC 可信网络服务中心的根证书或中级根证书私钥信息一旦泄漏，CNNIC 可信网络服务中心会及时废止由此私钥签发的证书，然后签发新证书取代。

### 4.13.3 密钥的转换

在密钥信息泄漏或灾难情况下，CNNIC 可信网络服务中心根据本 CPS 签发域名证书所使用的私钥信息泄漏或遭破坏而无法复原，CNNIC 可信网络服务中心会进行公布。公布内容包括已废止证书的名单、如何为证书持有者提供新的 CNNIC 可信网络服务中心根证书或中级根证书公开密钥及如何向证书持有者重新颁发证书。

## 5 实体、程序及人员安全控制

### 5.1 实体安全

#### 5.1.1 选址及建造

CNNIC 可信网络服务中心运行在具备合理安全条件的地点。在场地建造过程中，CNNIC 可信网络服务中心已采取适当预防措施，为 CNNIC 可信网络服务中心运行做好准备。

#### 5.1.2 进入控制

CNNIC 可信网络服务中心实施合理的安全控制，限制访问 CNNIC 可信网络服务中心所使用的硬件及软件（包括服务器、工作站及任何外部加密硬件模块）。可访问上述硬件及软件的人员只限于本 CPS 第 5.2.1 节所述的履行可信职责的人员。在任何时间都对上述访问进行控制及电子监控，以防发生未经授权入侵。

#### 5.1.3 电力及空调

CNNIC 可信网络服务中心设施可获得的电力和空调资源包括专用的空调系统、不间断电力供应系统（UPS）以及租用的电力公司的发电车，以备城市电力系统发生故障时供应电力。

#### 5.1.4 自然灾害

CNNIC 可信网络服务中心设施在合理可能的限度内可免受自然灾害影响。

#### 5.1.5 防火及保护

CNNIC 可信网络服务中心已为其设施准备妥当防火计划及灭火系统。

## 5.1.6 媒体介质存储

媒体介质存储及处置程序已经准备妥当。

## 5.1.7 场外备份

CNNIC 可信网络服务中心系统数据的适当备份会作场外储存，并获足够保护，以免被盗用、损毁及媒体衰变。

## 5.1.8 保管印刷文件

印刷文件（包括证书持有者的身份确认文件，管理文档等）由 CNNIC 可信网络服务中心妥为保存，只有授权人员可以取阅。

## 5.1.9 废料处理

根据正常的废料处理要求处理废料。加密设备作废前根据设备生产商的指导，对其进行物理上的销毁或清零。

## 5.2 过程控制

### 5.2.1 可信职责

可进入关键区域，控制密码或其它操作程序并可能会对证书的签发、使用、废止带来重大影响的 CNNIC 可信网络服务中心人员，应视作承担可信职责。此类人员包括但不限于系统管理人员、操作员、工程人员及获委派监督 CNNIC 可信网络服务中心运作的行政人员。

CNNIC 可信网络服务中心已为所有涉及 CNNIC 可信网络服务中心域名证书服务而承担可信职责的人员制定了相关管理制度，包括：

- 按角色及责任制定各级实体及系统的操作控制流程
- 详细职责划分规定

## 5.2.2 CNNIC可信网络服务中心与本地受理点(LRA)之间的文件及资料传递

CNNIC 可信网络服务中心及其所属注册中心（RA）与本地受理点(LRA)之间的所有文件及资料的传递，均在受控制及安全的方式下进行。

## 5.2.3 年度评估

CNNIC 可信网络服务中心每年进行一次年度评估，以确保日常运营过程符合安全策略及其他流程控制相关规定。

## 5.3 人员控制

### 5.3.1 背景及资格

CNNIC 可信网络服务中心工作人员的背景、资历、经验等情况都进行核实和审查。具备忠诚、可信赖及工作热情、无影响系统运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

背景：要求政治素质高、业务优秀、有非常强的责任感，原则性强，无犯罪记录和不良记录；

资历：精通本岗位工作，其所受教育、培训及工作经历保证足够胜任其工作；

CNNIC 可信网络服务中心工作人员及管理政策可合理确保 CNNIC 可信网络服务中心或代表 CNNIC 可信网络服务中心的 LRA 人员的可信程度及胜任程度，并确保他们根据本 CPS 履行职责。

### 5.3.2 背景调查

CNNIC 可信网络服务中心（包括注册中心）对担任可信职责的人员进行调查（其聘用前及其后有需要时定期进行），以根据本 CPS 及 CNNIC 可信网络服务中心的人员策略要求核实工作人员的可信程度及胜任程度。未能通过首次及定期调查的人员不得担任或继续担任可信职责。

### 5.3.3 培训要求

CNNIC 可信网络服务中心（包括注册中心）工作人员已接受履行其职责所需要的初步培训。CNNIC 可信网络服务中心会提供持续培训，使人员能掌握所需最新工作技能。

### 5.3.4 向人员提供的文件

CNNIC 可信网络服务中心（包括注册中心）人员会收到指导手册，详细描述证书的注册、续费、补发及废止程序及与其职责有关的其它软件功能。

## 6 技术安全控制

### 6.1 密钥的生成及安装

#### 6.1.1 密钥对的生成

**根 CA：**根 CA 的密钥对由硬件加密设备直接产生，并且直接保存在该硬件加密设备（加密机）中，CNNIC 可信网络服务中心使用的是国家商业密码管理委员会鉴定通过的加密硬件设备。产生密钥的时候，必须由五个密钥管理员中的三个同时登录后由加密硬件设备产生，任何单独的一个人均没有办法执行产生密钥的操作。密钥管理员登录是采用 IC 卡的方式，其他人员无法获取 IC 卡或相应的密码。

**运营 CA：**运营 CA 的密钥对在本地的硬件加密设备上产生（硬件加密设备使用的是国家商业密码管理委员会鉴定通过的加密硬件设备），私钥不能出此加密硬件设备。产生密钥的时候，必须由五个密钥管理员中的三个同时登录后由加密硬件设备产生，任何单独的一个人没有办法执行产生密钥的操作。密钥管理员登录是采用 IC 卡的方式，其他人员无法获取 IC 卡或相应的密码。

**证书申请者：**签名密钥对在证书申请者端产生，具有严密且安全的控制措施。CA 服务器不为证书申请者提供密钥生成服务。CNNIC 可信网络服务中心不为证书申请者提供密钥介质。

## 6.1.2 公钥传送给证书签发机构

证书申请者使用 Web 服务器软件把公钥封装成 PKCS #10 格式的证书请求发给 CNNIC 可信网络服务中心由 CNNIC 可信网络服务中心生成证书。

CNNIC 可信网络服务中心将根据证书申请者提交的证书请求验证证书请求的完整性，CNNIC 可信网络服务中心只处理完整的证书请求。

## 6.1.3 CNNIC可信网络服务中心公钥发布

CNNIC 可信网络服务中心会把自己的公钥发布在网站上，以便最终实体获取。

## 6.1.4 密钥的长度

CNNIC 可信网络服务中心的根证书和中级根证书密钥对为 2048 位 RSA。证书申请者密钥对也要求为 2048 位 RSA。

## 6.1.5 密码模块标准

产生签名密钥、存储及签署操作在硬件密码模块进行。硬件密码模块是由中国国家密码主管机构审查通过的安全产品，符合国家的相关规定。

## 6.1.6 密钥用途

CNNIC 可信网络服务中心域名证书使用的密钥可用于加密通讯。CNNIC 可信网络服务中心的根证书和中级根证书密钥只用于签发证书及证书废止列表（CRL）。

## 6.1.7 密钥销毁

CNNIC 可信网络服务中心的根证书和中级根证书密钥在失效以后归档保留 10 年，然后通过适当方法销毁。归档的密钥在其归档期限结束后，需在多名可

信人员参与的情况下安全销毁。密钥的销毁将确保其私钥从硬件密码模块中彻底删除，不留有任何残余信息。

证书申请者私钥存在于证书申请者端，其证书过期后，应立即销毁私钥。

## 6.2 私钥保护和密码模块工程控制

### 6.2.1 密码模块标准

CNNIC 可信网络服务中心采用的硬件密码模块是由中国国家密码主管机构审查通过的安全产品，符合国家的相关规定。硬件密码模块安置在安全区域，并在有至少三名加密机管理员（密钥管理员）在场的情况下才可以访问存储在加密机中的密钥。

备份与恢复加密机时必须同时拥有三张管理员口令卡，才能对加密机进行备份与恢复的操作。

### 6.2.2 私钥多人控制

在所有管理员的大多数同时在场的情况下才可以访问存储在加密机中的密钥。采取中国国家密码主管机构审查通过的保护措施保证加密机内密钥的安全性。

具体地说，CNNIC 可信网络服务中心对根证书和中级根证书私钥的保护采用五人控制，三人必须同时到场的策略。

### 6.2.3 私钥托管

CNNIC 可信网络服务中心的根证书和中级根证书私钥不托管给其他机构，CNNIC 可信网络服务中心也不接受证书申请者的签名私钥托管。

### 6.2.4 CNNIC可信网络服务中心私钥备份

作为灾难恢复的一项措施，需要进行密钥备份。CNNIC 可信网络服务中心采用符合国家规定的硬件密码模块对根证书和中级根证书私钥进行加密和备份，备

份存储在与硬件密码模块系统独立的系统内防止被窃。在备份密钥时，必须由密钥管理员使用口令 IC 卡，启动密钥管理程序，执行密钥备份指令才能完成。

证书申请者私钥存放在证书申请者端，证书申请者宜根据其具体情况采用合适的手段对其私钥进行存储、备份和恢复。

## 6.3 密钥对管理的其它方面

### 6.3.1 公钥归档

由管理员操作 CNNIC 可信网络服务中心证书和公钥的归档。

### 6.3.2 私钥归档

根证书和中级根证书密钥对到期后，这些密钥对将归档保存至少 10 年。归档密钥对保存在 6.2.1 所述的硬件密码模块中，并且 CNNIC 的密钥管理策略和流程阻止归档密钥对返回到生产系统中。归档密钥对超过归档保存期后，CNNIC 可信网络服务中心将按 CPS 第 6.1.7 节规定对其进行销毁。

证书申请者私钥保存在证书申请者端，因此证书申请者私钥归档不适用。

### 6.3.3 证书操作期和密钥对使用期限

CNNIC 可信网络服务中心根证书和中级根证书公钥和私钥的有效期保持一致，根证书密钥对有效期为 20 年，中级根证书密钥对有效期为 10 年。

CNNIC 可信网络服务中心域名证书有效期为 1 年。在接近过期日时有一段时间可以进行更新。

## 6.4 计算机安全控制

CNNIC 可信网络服务中心在安全的环境下运行，并实行分区访问权限控制。核心系统和其它系统隔离，采用防火墙和入侵检测保证安全。并实行：

系统安全配置，关闭不必要的服务与端口。

操作系统必须安装最新的补丁程序，由专人负责最新补丁的安装。

生产系统每台机器均由专人负责，严格上机操作程序，口令逐级管理，逐级授权。各人负责各自权限范围内的操作。

日志和操作记录的审计制度。

数据备份和恢复机制。

## 6.5 生命周期技术安全控制

证书生命周期安全控制遵循 WebTrust 认证规范。

CNNIC 可信网络服务中心所使用的系统在使用前均经过详细测试，并在使用过程中进行不定期检查。

## 6.6 网络安全控制

根据安全要求的不同，将 CNNIC 可信网络服务中心系统划分为不同的网段，部分高安全级系统进行离线操作。并采用层次模型保证网络的安全性以及系统的可靠性。

## 6.7 密码模块工程控制

CNNIC 可信网络服务中心使用的密码模块是经过中国国家密码主管机构审查通过的加密机。

# 7 证书及证书废止列表（CRL）结构

## 7.1 证书结构

本 CPS 提及的证书包含用来确认身份和核实这些信息是否完整的公开密钥。本 CPS 提及的证书一律以 X.509 第三版本的格式发出。

### 7.1.1 版本号

CNNIC 可信网络服务中心域名证书有广泛的通用性。证书格式符合 X.509 V3

标准，可以提供支持证书扩展的能力。

## 7.1.2 证书项说明

| 域          | 值或值的限制  |
|------------|---|
| <b>基本域</b> |   |
| 版本         | V3  |
| 序列号        | CNNIC 可信网络服务中心给所发证书赋予的唯一的值  |
| 签名算法       | 用于签发证书的算法的名称，见本 CPS 7.1.3 节                                       |
| 颁发者        | 证书颁发者的甄别名，域名证书中为 CNNIC 可信网络服务中心中级根证书的主题                           |
| 有效起始日期     | 用来指定证书有效的起始日期，基于国际通用时间(UTC)，和北京时间同步                               |
| 有效终止日期     | 用来指定证书有效的终止日期，基于国际通用时间(UTC)，和北京时间同步                               |
| 主题         | 证书持有者的甄别名，见本 CPS 7.1.4 节  |
| 公钥         | 证书公钥，使用 RSA 算法，密钥长度满足本 CPS 6.1.4 节的要求                             |
| <b>扩展项</b> |   |
| 基本限制       | 域名证书值为：Subject Type=End Entity<br>Path Length Constraint=None     |
| CRL 分发点    | CNNIC 可信网络服务中心签发的证书中包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载 CRL，见本 CPS |
| 密钥用法       | 域名证书值为：Key Encipherment, DigitalSignature                         |
| 主题密钥标识符    | 所颁发域名证书公钥的标识  |
| 颁发机构密钥标识符  | 上级 CA 证书公钥的标识   |
| 证书策略       | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.29836.1.1 |

|         |   |
|---------|---|
|         | [1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br><a href="http://www.cnnic.cn/cps/">http://www.cnnic.cn/cps/</a> |
| 增强型密钥用法 | 域名证书值为：服务器验证  |
| 主题备用名   | 在多域名证书中值为证书所认证的所有域名   |

### 7.1.3 算法对象标识符

CNNIC 可信网络服务中心签发证书所使用的签名算法为 sha1RSA。

### 7.1.4 名称形式

CNNIC 可信网络服务中心签发证书的甄别名符合 X500 关于甄别名的规定。对于证书主题甄别名，C 代表国家，值是 CN；O 代表组织，值是 CNNIC 或 CNNIC SSL 或域名证书持有者名称；CN 在多域名证书时是多个域名的并列，单域名证书、通配域名证书是单个域名。

### 7.1.5 名称限制

在 DN 中，可以使用除专用字符和特殊字符外的所有 ASCII 字符。专用字符为反斜杠 (“\”) 和双引号 (“” )，由于在 DN 中有特殊含义，不能用在 DN 中。另外，如果在 cn 中包含特殊字符 (“,”、“=”、“+”、“#”、“<”、“>”、“;”)，CNNIC 可信网络服务中心的 CA 系统会做特殊处理，即对整个 cn 内容加双引号，这样会导致以后实际处理上的不方便，因此不允许在 cn 中包含这些特殊字符。

由于存在不可见的 ASCII 字符，不便于证书申请者使用，下面给出本证书业务规则中所有可用的 ASCII 字符列表（ASCII 值为十进制数值）：

| ASCII 值 | 字符 |
|---------|----|
| 032     | 空格 |
| 033     | !  |
| 036     | \$ |
| 038     | &  |
| 040     | (  |

|         |     |
|---------|-----|
| 041     | )   |
| 045     | -   |
| 046     | .   |
| 047     | /   |
| 048~057 | 0~9 |
| 058     | :   |
| 065~090 | A~Z |
| 091     | [   |
| 093     | ]   |
| 094     | ^   |
| 095     | —   |
| 096     | `   |
| 097~122 | A~z |
| 123     | {   |
| 125     | }   |
| 126     | ~   |

## 7.1.6 证书策略对象标识符

证书策略由发证机构制定并对外广泛发布，同时向国际标准化组织申请标准的对象标识符（OID），从而保证与其它应用相兼容，对象标识符在通信服务中进行传递，作为该证书机构证书策略的标识，代表该认证机构提供证书服务的相关策略。另一方面，只有证书申请者同意该证书策略，才可以从认证中心去申请和获得数字证书。

## 7.1.7 策略限制扩展项的用法

规定在 CA 体系中的各层 CA 使用相同的 CP 以及是否和其他 CA 体系互相信任。CNNIC 可信网络服务中心域名证书未使用本扩展域。

## 7.1.8 策略限定符的语法和语义

对于本扩展域，X.509V3 标准没有规定格式，可以提供 CPS 在网上的位置说明。CNNIC 可信网络服务中心域名证书未使用本扩展域。

## 7.1.9 关键证书策略扩展项的处理规则

CNNIC 可信网络服务中心域名证书未使用。

## 7.2 证书废止列表（CRL）结构

CNNIC 可信网络服务中心证书废止列表（CRL）的格式为 X.509 第二版本。

### 7.2.1 版本号

V2

### 7.2.2 CRL项

CRL 数据定义

版本（Version）

含义：显示 CRL 的版本号。

签名（Signature）

含义：签发 CRL 的 CA 的签名。

算法标识（algorithmIdentifier）

含义：定义签发 CRL 所使用的算法。

CRL 的签发者（Issuer）

含义：指明签发 CRL 的 CA 的甄别名。

CRL 发布时间（thisUpdate）

预计下一个 CRL 更新时间(next update)

废止证书信息目录(revoked certificates)

## 7.3 OCSP

CNNIC 可信网络服务中心 CA 签发的 OCSP 响应符合 RFC2560 标准。OCSP 响应至少包含如下表所述基本域和内容。

OCSP 结构的基本域

| 域      | 值或值的限制  |
|--------|---|
| 状态     | 响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项           |
| 版本     | V1  |
| 签名算法   | 签发 OCSP 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)算法签名。 |
| 颁发者    | 签发 OCSP 的实体。颁发者公钥的 SHA1 数据摘要值和证书甄别名。                                  |
| 产生时间   | OCSP 响应的产生时间。   |
| 证书状态列表 | 包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书废止信息。                            |
| 证书标识   | 包括数据摘要算法(SHA1, OID: 1.3.14.3.2.26)、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。        |
| 证书状态   | 证书的最新状态，包括有效、废止和未知。   |
| 证书废止信息 | 当返回证书状态为废止时包含废止时间和废止原因。   |

### 7.3.1 版本号

V1

### 7.3.2 OCSP 扩展项

与 RFC2560 一致。

### 7.3.3 OCSP请求

OCSP 请求至少包括：

协议版本

服务请求

目标证书标识

OCSP 服务器需要的扩展项

### 7.3.4 OCSP 响应

正确的 OCSP 响应须包括：

响应协议的版本

OCSP 服务器的名称

对一个请求中的每一个证书的应答（包括目标证书标识、证书状态值、有效应答的时间间隔、可选的扩展项）

可选的扩展项

签名计算方法 OID

用杂凑函数计算出的签名

## 8 CPS 管理

### 8.1 变更流程

在 CNNIC 可信网络服务中心的 CPS 做出任何变动之前，CNNIC 可信网络服务中心将对变动的条款进行研究，做出变更的决定。在征求 CNNIC 可信网络服务中心律师法律意见后，由安全管理委员会形成决议。

CNNIC 可信网络服务中心形成决议后，在 CNNIC 可信网络服务中心网站公布变更后的 CNNIC 可信网络服务中心 CPS。

CNNIC 可信网络服务中心将对 CPS 进行严格的版本控制。

### 8.2 公告与通知

所有公告和通知将在 CNNIC 可信网络服务中心网站上公布 (<http://tns.cnnic.cn>)。

### 8.3 CPS 批准程序

批准流程是：

- (1) CPS 编写组编写或修订 CPS。
- (2) CPS 编写或修订完成后提交 CNNIC 可信网络服务中心各部门审议。
- (3) 审议通过后的 CPS 递交 CNNIC 可信网络服务中心安全管理委员会审议。
- (4) CNNIC 可信网络服务中心安全管理委员会审议通过后，CPS 正式对外发布。

## 8.4 解释

CNNIC 可信网络服务中心对本 CPS 拥有最终解释权。