中国互联网络信息中心（CNNIC）
可信网络服务中心
证书策略

版本号：3.05

有效期：2015-04-26至　2016-04-26

中国互联网络信息中心（CNNIC）

CNNIC 可信网络服务中心证书策略版本控制表

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 CP 有效期一年	2008 年 4 月 8 日
V2.01	1、域名证书密钥对要求 2048 位 2、赔付金额进行修改 3、联络方式中的邮编修改 4、年审完成，延长 CP 有效期一年	2009 年 3 月 19 日
V2.02	1、证书主题中 O 项值修改 2、多域名证书主题中 CN 项值修改 3、证书申请所提交材料调整 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
V2.03	1、对 CP 进行检查,修改文字和格式问题，以使 CP 便于对外发布 2、CP 改为在储存库中公开发布	2009 年 6 月 18 日
V2.04	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
V3.0	1、根据 EV CA 和 DQ CA 上线后的实际情况对本 CP 进行修改，以符合 EV CA 和 DQ CA 的实际情况 2、修改安全管理委员会会议或文件会签频率	2010 年 5 月 20 日
V3.01	1、对高级证书与 EV 证书的名字进行调整	2012 年 4 月 05 日
V3.02	1、 人员控制中增加说明工作人员包括外包人员 2、 对国防类域名的申请做特殊说明 3、 根据实际情况调整参考号/授权码的发送方式	2013 年 5 月 14 日
V3.03	1、在灾难恢复计划中加入了 CA 服务在灾难情况下系统停机时间，恢复时间内容。	2013 年 6 月 24 日
V3.04	1. 停止提供多域名证书域名修改服务。 2. CNNIC 将定期检查 CABForum 的 SSL Baseline Requirement 要求并承诺证书管理及签发符合该要求。 3. CNNIC CA 加入 24*7 的应急处理机制。	2014 年 4 月 25 日
V3.05	1. 在第 5 章第 2 节中添加 CNNIC 可信网络中心重要调整控制流程； 2. 由于证书和 CRL 结构已在 CPS 中有详细说明，故删除第 7 章及附录中证书和 CRL 结构相关内容。 3. 附录中加入二级根签发记录表。	2015.04.26

目录

1 引言

1.1 概述

本证书策略（Certificate Policy，CP，“策略”）详细说明了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”）签发和管理证书的规则和需求，并将用来验证 CNNIC 可信网络服务中心公开密钥基础设施（PKI）的数字签名策略。

本证书策略说明了有关 CNNIC 可信网络服务中心的下列信息:

- 对本策略中定义和管理的认证中心、注册中心、证书持有者和信赖方进行授权;
- 由本策略对各方的主要职责进行管理;
- 按照证书发行和管理的最基本要求，确保为用于校验数字签名或保证通信的机密性而提到的适当申请与本策略中的适应性相一致。

为了下面提到的目的和应用，要求证书对本策略提供支持，每个信赖方都已确定通过该证书对特定交易的发起人进行认证是合适的并可充分信任。

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 CPS 进行审核，以确保 CPS 与 CP 文件一致。

安全管理委员会应保证每年至少召开 1 次会议或进行 1 次文件会签，以对 CNNIC CA 中心相关制度规定进行检查修改和批准续期，并对 CNNIC CA 中心运行状况进行通报。此外，在有其他重要变更时，安全管理委员会应根据实际情况及时通过会议或文件会签的方式对重要事项进行讨论和审批。安全管理委员

会成员由来自于 CNNIC 的领导层、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，由 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，对全 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以下三个关键领域：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；
- 增加和减免其他安全管理员，管理员及 CNNIC 可信网络服务中心工作人员；
- 对于敏感操作的授权，诸如增加和减免安全管理员及管理员；
- 管理交叉认证，发布 CNNIC 可信网络服务中心交叉认证协议，更新及撤消交叉认证；
- 处理审计日志。

1.3 适应性

随着 CNNIC 可信网络服务中心业务的进展，本策略文档将进行修订以反映其新的和扩大的责任。

在 CNNIC 可信网络服务中心现阶段的授权实体为 PKI 服务提供者和最终实体:

PKI 服务提供者：

- 认证中心（Certification Authority，CA）；
- 注册中心（Registration Authority，RA）
- 本地受理点（Local RA，LRA）

最终实体：

- 证书申请者或证书持有者（“证书申请者”在获取证书后变为“证书持有者”）
- 信赖方。

本策略受 CNNIC 可信网络服务中心制约，CNNIC 可信网络服务中心依据本策略监督与 CNNIC 可信网络服务中心签发证书有关的所有部门的行为。证书申请者和信赖方使用符合本策略签发的证书应参照相关的 CPS，以获得进一步的细节,即 CNNIC 可信网络服务中心是如何实施该项策略的。

1.3.1CNNIC 可信网络服务中心认证中心

CNNIC 可信网络服务中心认证中心为两层 CA 结构。第一层 CA 叫做根 CA，制定 CNNIC 可信网络服务中心的整体策略，并可用于同其它 CA 进行交叉认证，CNNIC 可信网络服务中心当前包括 CNNIC ROOT 和 China Internet Network Information Center EV Certificates Root（以下简称 CNNIC EV ROOT）两个根 CA；第二层叫做中级根 CA，也就是实际签发用户证书的 CA，用于 CNNIC 可信网络服务中心证书业务的日常运营,CNNIC 可信网络服务中心当前包括 CNNIC SSL、CNNIC DQ SSL、CNNIC EV SSL 三个中级根 CA，其中 CNNIC SSL 和 CNNIC DQ SSL 由 CNNIC ROOT 签发，CNNIC EV SSL 由 CNNIC EV ROOT 签发 。

CNNIC 可信网络服务中心 CA 执行的职能有：创建证书并对它们进行签名、将证书分发至证书申请者、废止证书及分发证书废止列表(CRL)。CNNIC 可信网络服务中心 CA 对公钥证书和 CRL 的储存库进行维护并以安全的方式加以使用。CNNIC 可信网络服务中心的证书业务规则（“CPS”）文件副本也应在 CNNIC 可信网络服务中心的网站中公开。

本策略受 CNNIC 可信网络服务中心制约，并监督与 CNNIC 可信网络服务中心签发证书有关的所有部门的行为。

如 CNNIC 可信网络服务中心认为证书申请符合证书业务规则所包含的操作程

序，则 CNNIC 可信网络服务中心可签发证书。

1.3.2最终实体

CNNIC 可信网络服务中心体系中的最终实体包括两部分：证书持有者和信赖方。

1.3.2.1证书持有者

CNNIC 可信网络服务中心的证书持有者除了 CNNIC 可信网络服务中心的系统用户以外，主要是拥有因特网域名的用户，这些用户可以是法人或自然人，同时希望获得为该机构所拥有的域名发出的证书。

1.3.2.2信赖方

指信任 CNNIC 可信网络服务中心签发证书的最终实体，包括：最终用户、服务器等。

1.3.3证书期限

CNNIC 可信网络服务中心的数字证书根证书有效期为 20 年，中级根证书有效期为 10 年。

CNNIC 可信网络服务中心域名证书有效期最长为 3 年。在接近过期日时有一段时间可以进行更新，证书内会注明其有效期。

1.4 证书策略管理

1.4.1安全管理架构

CNNIC 可信网络服务中心的安全管理构架分为两层，其一为安全管理委员会，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，其二为安全管理人员，负责执行安全管理委员会的决定，并对 CNNIC 可

信网络服务中心的安全工作进行日常管理，CNNIC 可信网络服务中心的日常安全管理工作由首席安全管理员负责。

1.4.1.1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。

安全管理委员会授权首席安全管理员及其团队实施其决定。

1.4.1.2首席安全管理员

首席安全管理员全面负责 CNNIC 可信网络服务中心日常的各项安全事务。由 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，对全 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以下三个关键领域：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。

1.4.1.2.1 维护、执行安全策略和程序

CNNIC 可信网络服务中心首席安全管理员负责所有安全策略和程序的日常维持和执行工作。通过使用抽样调查、对问题做出反应，以及采取事先主动的检查行为和程序等方式做好此项工作。

1.4.1.2.2 审计一致性

CNNIC 可信网络服务中心首席安全管理员是所有外部审计要求的联系人和协调者，同时还要确定内部安全策略和程序，并且提供外部审计使用的资料。

1.4.2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

1.4.3证书策略变更流程

在 CNNIC 可信网络服务中心的 CP 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有关法律上的意见后，安全管理委员会形成决议并签署同意。

CNNIC 可信网络服务中心形成决议后，根据变动的具体情况，决定是否将此决议通知用户。如果变动不会影响用户的使用，则不会通知用户，如果 CNNIC 可信网络服务中心安全管理委员会认为这些变动会影响到用户使用，则会通过 CNNIC 可信网络服务中心的网站通知用户此次策略变更。

CNNIC 可信网络服务中心将对 CP 进行严格的版本控制。

1.4.4证书策略审批流程

批准流程是：

- CP 编写组编写或修订 CP。
- CP 编写或修订完成后提交给 CNNIC 可信网络服务中心首席安全管理员组织相关人员审议,并给出与 CPS 的一致性报告。
- 审议通过后的 CP 和一致性报告一同递交 CNNIC 可信网络服务中心安全管理委员会审议。
- CNNIC 可信网络服务中心安全管理委员会最终确定 CP 与 CPS 的一致性。

- CNNIC 可信网络服务中心安全管理委员会审议通过后，CP 的正式版本由 CNNIC 可信网络服务中心安全管理委员会签署。

1.4.5证书策略发布

CNNIC 可信网络服务中心证书策略经批准后会及时对外进行发布。用户可以访问以下网址获取最新版本的证书策略（CP）文档：

http://tns.cnnic.cn

1.4.6适应性和变更效力

如果在进行证书策略的变更时 CNNIC 可信网络服务中心安全管理委员会认为会影响用户的使用，而通过 CNNIC 可信网络服务中心的网站通知用户此次策略变更的具体内容，则此次变更在发布 30 天后生效。证书持有者和合格信赖方有责任定期访问网站查看本策略的最新变更通知。

使用或者信任证书的宽限期为 30 天，宽限期后视为接受修订条款。

2 总则

2.1 义务

2.1.1CNNIC 可信网络服务中心认证中心义务

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。根据本策略，CNNIC 可信网络服务中心所属认证中心（CA）有下述义务：

a) 接收注册中心（RA）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

c) 定期查看来自 CABForum 的 SSL Baseline Requirement 基线要求的更新内容，并承诺将根据基线要求的内容进行 CA 系统及业务逻辑内容的升级调整，保证对服务器证书的签发及管理符合最新版本的 SSL Baseline

Requirement 要求

2.1.1.1CNNIC 可信网络服务中心认证中心陈述

通过给一个证书申请者签发一张证书，CNNIC 可信网络服务中心认证中心（CA）向证书申请者保证所有合格的信赖方能够合理地在有效期内根据本策略信任证书中的信息，并且：

CNNIC 可信网络服务中心 CA 根据本策略签发证书，在必要时可废止该证书；

CNNIC 可信网络服务中心 CA 在签发证书时已确认证书申请者的身份满足本策略的要求和 CPS 的要求；

在 CNNIC 可信网络服务中心 CA 的证书中没有已知的错误，而且 CNNIC 可信网络服务中心 CA 已经采取合理的做法确保证书中信息的正确性；

在证书申请中由证书申请者提供的信息已被准确应用到证书中；

该证书满足本策略和 CNNIC 可信网络服务中心的 CPS 的所有具体要求；

该证书申请者的公钥和私钥为匹配的密钥对；

在证书中定义的证书申请者拥有与证书中所列公钥相对应的私钥；

CNNIC 可信网络服务中心 CA 已使用一套可信的系统去产生和签发该证书。

2.1.2CNNIC 可信网络服务中心注册中心义务

注册中心 (RA，Registration Authority)系统负责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（CA)。注册中心有下述义务：

a) 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

c) 通知证书持有者有关已废止的证书

CNNIC 可信网络服务中心仅有一个 RA，设在 CNNIC。

CNNIC 可信网络服务中心确认 LRA 的身份，并授权 LRA 进行用户注册的资料收集工作。LRA 有义务在用户进行证书注册、补发、续费、废止时负责收集相

关信息并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被用来发布 CA 证书、CPS、CP 和证书废止信息等内容。

CNNIC 可信网络服务中心支持储存库，并利用定义在 CPS 中的技术实现有效发布。

2.1.4证书持有者义务

证书持有者代表着证书公钥所绑定的唯一实体，拥有与证书公钥唯一对应的私钥的最终控制权。

证书持有者应在本 CP 和 CPS 的范围内使用证书，愿意并能够承担在本 CP 和 CPS 中约定的义务。

2.1.5信赖方义务

要信任或验证一张证书，信赖方必须验证证书的废止信息。信赖方应在经过合理的审核后才能够信任一张证书。

2.2 责任

CNNIC 可信网络服务中心与证书持有者间的责任将在证书持有者协议中约定。

CNNIC 可信网络服务中心与 LRA 间的责任将在相应的 LRA 协议中约定。

2.3 解释与执行

2.3.1管辖法律

本策略受中华人民共和国法律管辖。

2.3.2条款可中止性、修改

若本证书策略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。本证书策略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，可能也需要修改本证书策略。经营活动的改变会与证书策略的修改相一致。

2.3.3争端解决程序

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数字证书（域名证书）费用

证书费用由可信网络服务中心根据市场和管理部门的规定自行决定。

2.5 发布资料和储存库

2.5.1CNNIC 可信网络服务中心信息的发布

CNNIC 可信网络服务中心将在储存库中发布下列信息：

(1)CA 证书；

(2)证书废止信息；

(3)CPS 和 CP 的拷贝

(4)其它相关信息。

2.5.2发布频率

所有需要发布在储存器中的信息都应及时发布。有关证书废止的相关信息将根据第 4.4 节相关规定进行发布。

2.5.3储存库访问控制

储存库在合理的维护下可供 RA、合格信赖方、证书持有者每周 7 天，每天 24 小时使用。

2.6 一致性审计

2.6.1一致性审计

由 CNNIC 可信网络服务中心或法律主管部门指定的审计机构对 CNNIC 可信网络服务中心进行审计。年度审计次数由 CNNIC 可信网络服务中心决定或者由法律指定的监管机构决定。

2.6.2审计员的身份与资质

对 CNNIC 可信网络服务中心实施审计的审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

必须是经许可的、有营业执照的公共会计师或者是经许可的商业评估机构，在业内享有良好的声誉；

了解计算机安全体系、网络通信安全要求、PKI 技术、标准和操作；具备检查系统运行状况的专业技术和工具。

2.6.3审计机构与被审计者的关系

审计机构必须是独立于 CNNIC 可信网络服务中心的实体。

2.6.4审计项目

对 CNNIC 可信网络服务中心规范审计应包括但不限于：

- CNNIC 可信网络服务中心支持的证书操作规程是否完整地在 CPS 中表述，包括 CNNIC 可信网络服务中心的技术、手续和员工的相关管理政策和操作规范；
- CNNIC 可信网络服务中心是否实施了必要的技术、管理、相关政策和操作规范。

2.6.5对审计中不足问题的处理

如果在审计过程中发现执行规范有不足之处，CNNIC 可信网络服务中心将根据审计报告的内容，以最快的速度准备一份解决方案以完善不足之处。

2.6.6结果通报

除非法律明确要求，CNNIC 可信网络服务中心一般不公开审计结果。

2.7 机密性

在执行与 CNNIC 可信网络服务中心签发、废止证书的有关任务时，可取阅任何记录、书刊、记录册、登记册、通讯、信息、文件或其它资料的 CNNIC 可信网络服务中心认证中心（CA）、注册中心（RA）及任何 CNNIC 可信网络服务中心外包商的人员，不得向他人披露该等记录、书刊、记录册、登记册、通讯、信息、文件或资料。CNNIC 可信网络服务中心会确保其 CA、RA 及任何 CNNIC 可信网络服务中心外包商的人员均会遵循此限制事项。

作为根据本 CP 申请数字证书的组成部分而提交的证书持有者资料，只会用于收集资料的目的并以机密方式保存，CNNIC 可信网络服务中心需根据本 CP 履

行其责任的情况除外。除非经法庭发出的传票或命令，或中华人民共和国法律法规另有规定，未经证书持有者事先同意，不得将这些资料对外发布。

2.7.1机密信息类型

各最终实体的签名私钥是该用户的机密信息,CNNIC 可信网络服务中心 CA 和 RA 不得访问此类私钥。

对 CNNIC 可信网络服务中心的审计信息，考虑到其安全性，除法律要求外，不得对外公开。

由 CNNIC 可信网络服务中心 CA 和 RA 保存的个人和公司信息，除了被明确需要发布在证书、CRL、证书策略或 CPS 中的部分外，除非由法律要求，不得公开。

2.7.2非机密信息类型

包含在证书和 CRL 中,由 CNNIC 可信网络服务中心发布的信息不是机密信息。CPS 和 CP 中公布的信息不是机密信息,但策略要求它只可用于本 PKI 体系内的用户。CPS 的部分内容可在更广泛的范围内使用。

2.7.3证书废止信息批露

当证书由 CNNIC 可信网络服务中心废止时，在 CRL 条目中包含被废止证书的废止原因代码。这个废止原因代码不是机密信息，可与所有其它证书持有者和信赖方分享。其它关于废止的细节不被透露。废止代码列表和一个简短的描述将发布在储存库。

2.7.4披露给执法官员

和 CNNIC 的其它服务一样，根据策略，CNNIC 可信网络服务中心将遵照法律规定披露信息给执法官员。

2.8 知识产权

CNNIC 可信网络服务中心享有并保留对证书及 CNNIC 可信网络服务中心提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。

2.8.1证书和废止信息的拥有权

所有 CNNIC 可信网络服务中心颁发的证书、证书废止信息和 CNNIC 可信网络服务中心提供的软件中使用、体现的一切版权、商标和其他知识产权均属于 CNNIC 可信网络服务中心，这些知识产权包括所有相关的文件和使用手册。

2.8.2证书策略的拥有权

CNNIC 可信网络服务中心拥有本策略的所有知识产权。

2.8.3名称拥有权

在没有 CNNIC 可信网络服务中心预先书面同意的情况下，使用者不得在证书到期、废止之后，使用任何 CNNIC 可信网络服务中心使用的名称、商标或可能与之相混淆的名称、商标。

2.8.4密钥和密钥设备拥有权

由最终用户自己保管的密钥对的知识产权，属于用户自己。

CNNIC 可信网络服务中心的 CA 公钥和 CA 私钥，包括所有 CNNIC 可信网络服务中心所使用的公钥和证书都是 CNNIC 可信网络服务中心的资产。CNNIC 可信网络服务中心准许软件和硬件制造商在生产时将根证书安装在可信的硬件设备或软件中。

3 鉴别与认证

3.1 首次申请

域名证书的申请，证书申请者或其经办人必须亲自到 CNNIC 可信网络服务中心指定的机构地点，并出示第 3.1.7 节所述身份证明。

证书申请者须向 CNNIC 可信网络服务中心本地受理点递交一份填好的申请表。对于单位申请者，域名证书的申请须由申请单位的经办人和主管人填好并签名，并加盖申请单位公章,其中,国防类域名单位还必须提交标准服务器证书证明函,并由申请单位和本地受理点同时加盖公章；对于自然人申请者，域名证书的申请须由本人填好并签名。申请批准后，CNNIC 可信网络服务中心即准备好证书并发布给证书申请者，而证书申请者也将成为证书持有者。

3.1.1 名称类型

通过证书上的主题名称（于附录 B 内指明）可识别证书持有者的身份，该名称包括证书持有者机构所拥有服务器（包括网络域名）的名称。

3.1.2 名称含义

所采用名称的语义必须为一般人所能理解，方便辨识证书持有者身分。证书 DN 中的 Common Name 或者 SubjectAltName 为实际申请 Web 服务器的域名。

3.1.3 各个名称的解释规则

CNNIC 可信网络服务中心数字证书会包含的证书持有者名称(主题名称)类型见第 3.1.1 节。有关 CNNIC 可信网络服务中心数字证书主题名称的诠释，请参照附录 B。

3.1.4 名称唯一性

对证书持有者而言，主题名称 （于附录 B 内指明）应无歧义而且具有唯一

性。

3.1.5名称争端解决程序

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。

3.1.6不侵权承诺

证书申请者或证书持有者向 CNNIC 可信网络服务中心保证并向证书信赖方声明：申请证书过程提供的资料没有以侵犯第三者的商标权、商号或其他知识产权。

3.1.7证书申请者身份认证

证书申请者应依据《CNNIC 可信网络服务中心证书业务规则》（CPS）相关规定，在进行证书申请时提交身份证明材料，CNNIC 可信网络服务中心应履行对证书申请者进行身份认证的职责。

3.1.8证书申请渠道

CNNIC 可信网络服务中心的证书申请一律通过本地受理点（LRA）进行，CNNIC 可信网络服务中心不直接受理申请。

3.1.9密钥对确认

CNNIC 可信网络服务中心在获取到证书申请者的签发证书请求（CSR）后，将验证证书请求的签名和其他相关信息，以确认证书申请者拥有相应的密钥对。

4 操作规范

4.1 证书申请

4.1.1域名证书

4.1.1.1处理申请

域名证书的申请者必须到 CNNIC 可信网络服务中心指定的受理点递交申请。

4.1.1.2身份审核

对于证书申请者，用以证明其身份所需的文件，在本策略第 3.1.7 节中说明。完成核对身份手续后，数字证书会以安全方式送递申请者。

4.2 证书签发

在核对身份手续后，CNNIC 可信网络服务中心会以电子邮件和电话通知证书申请者其申请已被接纳,并发送证书“参考号/授权码”。发出数字证书的过程如下：

证书申请者在其设备上自行产生私人密钥及公开密钥。

证书申请者在其设备上自行产生包含其公开密钥的“签发证书请求”（Certificate Signing Request，CSR），并将“签发证书请求”经由指定的 CNNIC 可信网络服务中心网页传送给 CNNIC 可信网络服务中心。

在收到“签发证书请求”后，CNNIC 可信网络服务中心系统会自动查证包含公开密钥资料的“签发证书请求”上的数字签名，以核对证书申请者是持有配对的私人密钥。CNNIC 可信网络服务中心并不会持有证书申请者的私钥。

在核对证书申请者是持有配对的私钥后，CNNIC 可信网络服务中心会产生载有证书申请者公开密钥的数字证书。

证书申请者可在指定的 CNNIC 可信网络服务中心网页核对数字证书的内容及确认接受该数字证书。

4.3 证书接受

下载证书即构成证书持有者的证书接受。

4.4 证书废止

4.4.1废止情况

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。

4.4.2废止程序

如出现本文第 4.4.1 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通过本地受理点提出废止证书要求，废止申请具体流程请参考 CPS。CNNIC 可信网络服务中心的注册中心（RA）收到申请，并和申请者确认废止证书后，该证书即会废止且永久失效。废止证书申请表格可从 CNNIC 可信网络服务中心网页 http://tns.cnnic.cn 下载。

所有废止证书的有关资料（包括表明废止证书的原因代码）将包含在废止证书列表（CRL）内。（见第 7.2 节）

CNNIC 可信网络服务中心处理废止证书请求的时间为每工作日上午九时至下午五时。

4.4.3废止请求处理时限

在 CNNIC 可信网络服务中心所发布的操作时段内，废止请求应在 CNNIC 可信网络服务中心接收到正式申请资料后两个工作日内处理完成。

4.4.4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中，即终止某一证书的使用效力。

4.4.5服务承诺

CNNIC 可信网络服务中心将做出合理努力，确保在 (1) CNNIC 可信网络服务中心从证书持有者处收到废止申请或 (2) 在无此申请之情况下，CNNIC 可信网络服务中心决定废止证书，两个工作日内，将该废止证书数据在证书废止列表发布。然而，证书废止列表并不会在各证书废止后随即在公众目录中发布。只有在下一张证书废止列表更新时一并发布，证书废止列表届时才会显示该证书已废止的状态。

CNNIC SSL 中级根（签发标准服务器证书）以及 CNNIC EV SSL 中级根（签发 EV 高级服务器证书）签发的证书废止列表每 12 小时发布一次，CNNIC DQ SSL 中级根（签发快速证书）签发的证书废止列表每 7 天（168 小时）发布一次；如果没有进行中级根的废止，CNNIC ROOT 及 CNNIC EV ROOT 根签发的证书废止列表（CRL）每 6 个月（182 天）更新一次，如果进行中级根的废止，根签发的证书废止列表（CRL）会立即更新。

CNNIC 可信网络服务中心在处理证书废止时，会以合理的方式与证书持有者保持联系（例如电话），进行确认。

在证书持有者明知 CNNIC 可信网络服务中心根据 CPS 条款可能据以废止证书的任何事项的情况下，或证书持有者已做出废止申请，或经 CNNIC 可信网络服务中心通知拟根据本 CP 条款废止证书后，证书持有者均须立刻停止在交易中使用证书。倘若证书持有者无视本条所述的规定，仍在交易中使用证书，则 CNNIC 可信网络服务中心毋须就任何此类交易向证书持有者或证书信赖方承担

责任。

此外，在证书持有者明知 CNNIC 可信网络服务中心根据 CP 条款可能据以废止证书的任何事项的情况下，或证书持有者已做出废止申请，或经 CNNIC 可信网络服务中心通知拟根据 CP 条款废止证书后，均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，用于该交易的证书须予废止（由 CNNIC 可信网络服务中心或经证书持有者申请），并明确说明，故证书信赖方不得在交易中继续信任该证书。若证书持有者未能通知证书信赖方，则 CNNIC 可信网络服务中心无须就此类交易向证书持有者承担责任，并无须向虽已收到通知但仍完成交易的证书信赖方承担责任。

除非 CNNIC 可信网络服务中心未能行使合理技术且证书持有者未能按此等规定的要求通知证书信赖方，否则，CNNIC 可信网络服务中心无须就 CNNIC 可信网络服务中心做出废止证书(根据申请或其它原因)的决定与此信息出现在证书废止列表之间的时间内进行的交易承担责任。任何这类责任均仅限于本 CP 其它部分规定的范畴内。在任何情况下，注册中心自身无须对证书信赖方承担独立责任。因此，即使出现疏忽，注册中心也无须对证书信赖方负责。

数字证书的证书废止列表会依据在附录 C 内指明的格式更新。

有关 CNNIC 可信网络服务中心对于证书信赖方暂时未能获取已废止的证书资料时的政策，已列于本 CP 第 2.1.5 节(证书信赖方的义务)中。

4.4.6 CRL 更新频率

CNNIC 可信网络服务中心应以尽可能快的速度签发一个最新的 CRL 并在储存库中发布:CNNIC SSL 中级根（签发标准服务器证书）以及 CNNIC EV SSL 中级根（签发 EV 高级服务器证书）签发的证书废止列表每 12 小时发布一次，即标准服务器证书和 EV 高级服务器证书的 CRL 不晚于正确的域名证书废止请求被处理完成后 12 小时后发布；CNNIC DQ SSL 中级根（签发快速证书）签发的证书废止列表每 7 天（168 小时）发布一次 ，即快速证书的 CRL 不晚于正确的域名证书废止请求被处理完成后 168 小时后发布。。

如果没有进行中级根的废止，CNNIC ROOT 及 CNNIC EV ROOT 根签发的证书废止列表（CRL）每 6 个月（182 天）更新一次，如果进行中级根的废止，根签发

的证书废止列表（CRL）则立即更新。

4.4.7证书续费

CNNIC 可信网络服务中心会于证书的有效期届满前，以电子邮件或信件等方式向域名证书的证书持有者发出续费通知。证书持有者可依据 CNNIC 可信网络服务中心的流程从本地受理点处更新证书。

4.5 密钥变更

由 CNNIC 可信网络服务中心认证中心产生，并用以签发、认证本中心所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一定的时限，以供核对用原根密钥签名的证书。

4.6 密钥泄漏及灾难恢复程序

4.6.1灾难恢复计划

CNNIC 可信网络服务中心应有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。

每年需要对业务连续性计划进行复查，并严格执行。

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

为保证 CNNIC CA 中心在市场上的竞争力，并保证在所确定的系统中断时间内，CA 中心可能遭受的损失相对较低，风险相对较小，同时建设成本和管理成本也比较适合，CNNIC CA 中心最终确认：

1. 对于证书注册服务，在一般灾难情况下 CNNIC CA 中心会使用合理的商业手段在 24 小时内予以恢复，并在 48 小时内完全恢复全面注册服务功能。如不可抗力灾难（例如战争、地震、洪水、火灾等）造成 CNNIC CA 中心出现大面积硬件、设备、人员损失，可以在向公众通告具体情况，保证信息公开的基础上，延长注册服务系统中断时间。
2. 对于包括 CRL 下载服务在内的储存库服务，在灾难情况（包括不可抗力灾难）下，CNNIC CA 中心会使用合理的商业手段在 4 小时内予以恢复，并在 8 小时内完全恢复储存库服务。

4.6.2密钥泄漏恢复计划

业务连续性计划应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 可信网络服务中心应及时进行公布。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 可信网络服务中心应及时废止由此私钥签发的证书，然后签发新证书取代。

4.7 CNNIC 可信网络服务中心终止服务

如 CNNIC 可信网络服务中心停止担任证书认证机构的职能，即按 CNNIC 可信网络服务中心终止服务计划所定程序通知政府部门并做出公布。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适当地存盘 10 年（由终止服务日起计）；这类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）。

4.8 RA 终止服务

如注册中心（RA）根据注册中心协议或因注册中心终止服务停止担任注册中心的职能，且其代表 CNNIC 可信网络服务中心行使的授权已予以收回，由此注册中心申请的证书仍会按其条款和有效期继续有效。

4.9 CNNIC 可信网络服务中心 CA 私钥归档

当 CNNIC 可信网络服务中心的 CA 密钥对到期后，这些 CA 密钥对将归档保存至少 10 年。归档 CA 密钥对保存在 CPS 所述的硬件密码模块中，并且 CNNIC 可信网络服务中心的密钥管理策略和流程阻止归档 CA 密钥对返回到生产系统中。对归档私钥到了归档保存期，CNNIC 可信网络服务中心将按 CPS 所述进行销毁。

CNNIC 可信网络服务中心 CA 私钥归档的具体步骤如下：

1. 加密机管理员到业务内审员处领申请表单
2. 业务内审员签字
3. 首席安全管理员签字
4. 通知 CA 系统管理员等相关人员
5. 进入相应加密机区域进行密钥复制到归档密钥空间
6. 操作结束填写维护表单
7. 参与操作相关人员签字确认（加密机管理员、业务内审员和 CA 系统管理员）
8. 首席安全管理员签字
9. 业务内审员归档

4.10 CNNIC 可信网络服务中心应急机制

CNNIC 可信网络服务中心将提供 24*7 的应急机制，在如下所述的情况下，可以通过 010-58813000 联系 CNNIC 可信网络服务中心，进行紧急事件的处理：

1. CNNIC CA 中心将在 24 小时之内完成证书废止的申请，在如下情况：

- 当签发的证书在技术内容和格式上存在不可接受的风险时；
- 当证书申请者不是有效的授权者，或授权已过期；
- 当 CNNIC CA 中心确认证书申请者的使用有危害的密钥申请了证书时；
- 当 CNNIC CA 中心发现申请者使用的不再是一个有效的全域名时；
- 当申请人违反了申请协议或应组遵守的义务时；

当证书出现问题的时候（技术问题，外界因素等），CNNIC CA 中心可以及时处理并在 24 小时之内对高优先级的证书问题发起调查。

5 实体、程序和人员的安全控制

5.1 实体安全

CNNIC 可信网络服务中心应通过有效的物理控制来确保实体安全，具体措施可参考 CPS。

5.2 过程控制

CNNIC 可信网络服务中心应建设、维护和执行完备的管理制度和流程来对人员以及人员操作进行控制，从而确保 CNNIC 可信网络服务中心的安全。

CNNIC 可信网络服务中心对重要调整按照如下流程进行控制，重要调整指业务及 IT 环境的重大变更，包括可能导致秘钥泄漏的操作、可能导致关键业务中断的非常规操作、建立或开展新的 CA 业务,以及对业务流程、审批环节和 IT 环境现有安全控制进行变更等。

1. 申请人提出申请。
2. 申请人发起风险评估申请，由 CA 各相关角色生成风险评估的结果。
3. 业务内审员对风险评估结果给出评审意见。
4. 首席安全管理员根据风险评估结果给出审核意见，并判断是否有必要提交安全管理委员会进行评审。
5. 如有必要，由安全管理委员会进行审核，给出评审结论。
6. 申请人根据审批结论协调相关 CA 角色进行操作，CA 相关角色记录操作步骤及内容。
7. 操作完成后将事件结果向业务内审员和首席安全管理员汇报。
8. 对于由安全管理委员会审核的事项，由首席安全管理员向安全管理委员会汇报事件处理结果。

5.3 人员控制

CNNIC 可信网络服务中心应对工作人员的背景、资历、经验等情况都进行核实和审查，通过管理制度对其行为进行约束，并对其进行持续的培训，确保其

可信程度及胜任程度，并确保他们履行职责。工作人员包括 CNNIC 正式员工以及外包人员。

5.4 计算机安全审计程序

5.4.1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、补办等）、废止证书
- 更新储存库资料
- 汇编证书废止列表并刊登新数据
- 证书认证中心密钥转换
- 档案备份
- 紧急密钥恢复

5.4.2处理记录的次数

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

5.4.3 审计追踪记录的保护

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。

5.4.4 审计追踪记录备份程序

CNNIC 可信网络服务中心每日均会按照预先界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。

5.4.5 审计资料收集系统

无

5.4.6 安全主体向 CNNIC 可信网络服务中心发出通知

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。

5.4.7 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措施。

5.5 记录归档

5.5.1 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

5.5.2归档保存期限

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

5.5.3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。

5.5.4归档备份程序

制作并保存归档的副本。

5.5.5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。

6 技术安全控制

6.1 密钥的生成和安装

6.1.1密钥对的生成

根 CA：根 CA 的根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，必须由三个加密机管理员（共计五个加密机管理员）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。

子 CA：子 CA 的 CA 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，必须由三个加密机管理员（共计五个加密机管理员）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：签名密钥对在客户端产生，具有严密且安全的控制措施，可采用智能 IC 卡、其它硬件加密设备或加密软件生成。

6.1.2公钥传送给证书签发机构

证书申请者使用安全软件把公钥发给 CNNIC 可信网络服务中心由 CNNIC 可信网络服务中心生成证书。

6.1.3CNNIC 可信网络服务中心 CA 公钥传送给信赖方

CNNIC 可信网络服务中心会把自己的 CA 公钥证书发布在自己的网站上，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 CNNIC ROOT 及 CNNIC EV ROOT 根密钥和 CNNICSSL、CNNIC EV SSL、CNNIC DQ SSL 等中级根密钥对为 2048 位 RSA。证书持有者密钥对也要求为 2048 位 RSA。

6.1.5密码模块标准

产生签名密钥、存储及签名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密钥只用于签发证书及证书废止列表。

6.2 私钥保护和密码模块工程控制

CNNIC 可信网络服务中心应根据本策略条款规定采取相应的步骤保护自己的 CA 私钥。CNNIC 可信网络服务中心 CA 的签名私钥不能泄露。如果证书到期或被废止,或者签名私钥的使用终结,那么,所有私钥的复制都要被安全地毁掉。

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授使用。

CNNIC 可信网络服务中心签发的最终用户签名私钥，在其生命周结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

在 CNNIC 可信网络服务中心的 CA 私钥生命周期结束后，CNNIC 可信网络服务中心应将 CA 私钥继续保存在一个硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从件密码模块中彻底删除，不留有任何残余信息。

具体实施细节参见 CPS 中相关的内容。

6.3 密钥对管理

CNNIC 可信网络服务中心应考虑 CA 证书和域名证书的公私钥有效期和归档问题。

6.4 计算机安全控制

CNNIC 可信网络服务中心需要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需要遵循 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应经过详细测试，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，应考虑将 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必须是经过中国国家密码主管机构审查通过的加密机。

7 其他商业与法律事项

7.1 法律责任

7.1.1法律责任限制

7.1.1.1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 CP 及 CPS 所列条件限制其法律责任实属合理。

7.1.1.2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。

7.1.1.3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 CP 及 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。

7.1.1.4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数字证书的业务规则（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庭管辖。

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概不承担任何责任。

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。

本文所描述的法律责任限制不适用于个人伤害或死亡的（不大可能发生的）情形。”

7.1.2CNNIC 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。

7.1.3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。拟转让的行为均属无效。

7.1.4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雇员无权代表 CNNIC 可信网络服务中心对本 CP 及 CPS 的含义或解释作任何陈述。

7.1.5更改

CNNIC 可信网络服务中心有权更改本证书策略，而无须发出预先通知。证书持有者协议不得做出更改、修改或变更，除非符合本证书策略中的更改或变更规定，或获得 CNNIC 可信网络服务中心的明确书面同意。

7.1.6保留所有权

根据本证书策略签发的证书上所有资料的实质权利、版权及知识产权现属 CNNIC 可信网络服务中心所有。

7.1.7条款冲突

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

7.1.8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。

7.2 财务责任

7.2.1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。

7.2.2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。

8 附录

附录 A 词汇

证书认证中心（CA） Certification Authority

受用户信任,负责创建和分配公钥证书的权威机构。有时，证书认证中心也可为用户创建密钥。

CA 证书 CA-certificate

由其他 CA 为一个 CA 的公钥签发的证书。

证书认证路径 Certification Path

一个有序的证书序列，连同路径中起始对象的公钥，通过处理该序列可获得路径末端对象的公钥。

公钥基础设施（PKI） Public Key Infrastructure (PKI)

支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。

激活数据 Activation Data

用于操作密码模块所必需的、并且需要被保护的数据值（例如 PIN、口令、或人工控制的密钥共享部分），而不是密钥。

鉴别 Authentication

确定个人、组织或事物如其所声称的人或事物的过程。在 PKI 上下文中，鉴别指的是确定以某个特定名称申请或试图访问某事物的个人或组织确实为正确的个人或组织的过程。

证书策略（CP） Certificate Policy

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。

证书业务规则（CPS） Certification Practice Statement

关于证书认证机构在签发、管理、废止或更新证书（或更新证书中的密钥）过程中所采纳的业务实践的声明。

CPS 摘要 CPS Summary or CPS Abstract

由一个 CA 公布的、关于其完整 CPS 的一个子集。

身份标识 Identification

建立个人或组织的身份的过程，如指明某个人或组织是特定的个人或组织。在 PKI 上下文中，身份标识指代两个过程：

确定某个人或组织的给定名称与真实世界中该个人或组织的身份相联系；

确定在该名称之下申请或试图访问某事物的个人或组织确实为被命名的个人或组织。寻求标识的人可能是证书申请者，或者是 PKI 中可信职位的申请者，或者是试图访问网络或应用软件的人（如 CA 管理员试图访问 CA 系统）。

签发证书认证中心（签发 CA） Issuing Certification Authority

在特定的 CA 证书上下文中，签发 CA 是签发证书的 CA（参见主体 CA）。

参与者 Participant

在一个给定 PKI 中扮演某一角色的个人或组织，如证书持有者、信赖方、CA、RA、证书制作机构、证书库服务提供者、或类似实体。

PKI 信息公开声明（PDS） PKI Disclosure Statement

关于 CP 或 CPS 的补充手段，用于公开证书策略和 CA/PKI 业务中的关键信息。PDS 是公开和强调信息的载体工具，这些信息通常在相关 CP 或 CPS 中作更详细描述。因此，PDS 并不能替代 CP 或 CPS。

策略限定符 Policy qualifier

依赖于策略的信息，可能与 CP 标识符共同出现在 X.509 证书中。该信息中可能包含指向适用 CPS 或信赖方协议的 URL 指针，也可能包含证书使用条款的文字（或引起文字出现的数字）。

注册中心（RA） Registration Authority

具有下列一项或多项功能的实体：标识和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动废止或挂起证书，处理证书持有者废止或挂起其证书的请求，同意或拒绝证书持有者更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

信赖方 Relying party

证书的接收者，他依赖于该证书和（或）可通过该证书所验证的数字签名。在本证书策略中，术语“证书使用者”与“信赖方”可互换使用。

信赖方协议 Relying party agreement

证书认证机构与信赖方所签署的协议，通常规定了在验证数字签名或其他使用证书的过程中有关方所拥有的权利和义务。

条款集 Set of provisions

关于业务实施和（或）策略声明的集合，覆盖了一定范围的标准主题，用于使用本框架中所描述的方法来表达 CP 或 CPS。

主体证书认证中心（主体 CA） Subject Certification Authority

在特定的 CA 证书上下文中，主体 CA 指的是在证书中其公钥被认证的 CA。（参见签发 CA）

证书持有者 Subscriber

被颁发给一张证书的证书主体。

证书持有者协议 Subscriber Agreement

CA 与证书持有者之间签署的协议，规定了双方在颁发和管理证书的过程中所拥有的权利和义务。

验证 Validation

对证书申请者进行身份标识的过程。验证是身份标识的子集，并且在建立证书申请者身份的过程中指的就是身份标识。

附录 B 缩略语

CA	Certification Authority	认证中心
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	证书业务规则
CRL	Certificate Revocation List	证书废止列表
DAP	Directory Access Protocol	目录访问协议
DES	Data Encryption Standard	数据加密标准
DN	Distinguished Name	甄别名称
DNS	Domain Name Server	域名服务器
DSA/DSS	Digital Signature Algorithm/ Digital Signature Standard	数字签名算法/数字签名标准
HTTP	Hypertext Transfer Protocol	超文本传输协议
IETF	Internet Engineering Task Force	因特网工程任务组
ISO	Information Security Officer	信息安全官员
ITU	International Telecommunications Union	国际电信联盟
LDAP	Lightweight Directory Access Protocol	轻量目录访问协议
RA	Registration Authority	注册机构
OID	Object Identifier	对象标识符
PKI	Public Key Infrastructure	公钥基础设施
PKIX	Public Key Infrastructure X.509	公钥基础设施 X.509
RFC	(IETF)Request For Comments	意见要求
RSA	Rivest-Shamir-Adleman	RSA 算法
SHA-1	Secure Hash Algorithm	安全散列算法
HTTPS	Secure Hypertext Transfer Protocol	安全 Http 协议
SSL	Secure Sockets Layer	安全套接字层
URL	Uniform Resource Locator	统一资源定位符

附录 C 二级根签发记录表

二级根申请人信息			
名称		组织机构代码证（或其他公司标示）	
注册所在地		公司性质	
公司简介			
申请事由简述			
CNNIC 审批信息			
CNNIC 业务经办人		申请日期	
审批资料是否齐全（安委会审批记录）			
CNNIC CA 内审员审批意见			年　月　日
CNNIC 首席安全管理员审批意见			年　月　日
操作记录			
开始时间		结束时间	
操作区域			
操作对象			
CA 管理员			
策略管理员（PA）		其他支持人员	
证书信息			

证书有效起始日期		证书有效终止日期	
证书序列号		证书使用者	
基本限制			
密钥用法			
证书发放公开			
证书接收人	年　月　日		
发放时间			
发放目标			