中国互联网络信息中心（CNNIC）
可信网络服务中心
EV 高级证书业务规则

版本号：2.03

生效期：2013-07-1

中国互联网络信息中心（CNNIC）

CNNIC 可信网络服务中心 EV 高级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	2010 年 8 月 31 日
V2.00	经过年审修改：将“每年举行 4 次会议或进行文件会签”更改“保证每年至少召开 1 次会议或进行 1 次文件会签”	2011 年 8 月 31 日
V2.01	将“EV 证书”更名为“EV 高级证书”； 延长 EV CPS 有效期一年	2012 年 4 月 7 日
V2.02	1、修改 EV 证书申请提交资料 2、在申请者中增加一个“申请代表人”的新角色 3、增加电磁防护相关内容	2012 年 9 月 20 日
V2.03	1、在核实私人组织或业务实体公司申请人的法律性和身份调查时，也要关注其母公司、子公司或附属公司。 2、加入针对高风险申请人（如金融类）的预防措施内容。）	2013 年 6 月 24 日

目录

专有名词及术语

CA：Certification Authority 认证中心

CP：Certificate Policy

CPS：Certification Practice Statement 证书业务规则

CRL：Certificate Revocation List 证书废止列表

CSR：

CVC：

EPKI：

EV 高级证书：

HTTP：Hypertext Transfer Protocol 超文本传输协议

ITU：International Telecommunications Union 国际电信联盟

ITU-T：

MDC：

OCSP

OID：

PKI：Public Key Infrastructure 公钥基础设施

PKIX：Public Key Infrastructure X.509 公钥基础设施 X.509

PKCS：

RA：Registration Authority 注册机构

SGC：

SSL：Secure Sockets Layer 安全套接字层

TLS：

URL：Uniform Resource Locator 统一资源定位符

X.509：

公钥：

私钥：

依赖方：

根证书：

主题：

证书持有者：

1 综述

中国互联网络信息中心（以下简称“CNNIC”）可信网络服务中心（以下简称“CNNIC 可信网络服务中心”）为组织机构、政府、以及企业根据此业务规则提供域名增强型可信服务器证书安全服务（也称“EV 高级证书”服务），因此根据 CA/Browser 论坛提供的《EV 指导准则》编写了 CNNIC 可信网络服务中心的 EV 高级证书业务规则（以下简称“EV CPS”），作为 CNNIC 可信网络服务中心的 EV 高级证书相关业务和系统的运行规范。本文为提供证书服务的 CNNIC 员工提供了法律、商业和技术上的原则和业务规则，包括但不限于 EV 高级证书的批准、颁发、使用以及管理，并依据 CNNIC 证书策略（CP）中的 PKI 体系生成的 X.509 证书。

1.1 CNNIC 可信网络服务中心

根据本 EV CPS，CNNIC 可信网络服务中心履行 EV 高级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 EV CPS 授权发出 EV 高级证书的证书认证机构。做为一个证书颁发机构，CNNIC 可信网络服务中心根据 PKI 体系来运营，包括接受请求、颁发、撤销及更新一个数字证书，并维护并发布证书撤销列表（CRLs）。CNNIC 可信网络服务中心在整个的 PKI 服务中遵循了国际标准，包括 CA/Browser 论坛提供的《EV 指导准则》及其他的相关法律和法规。

CNNIC 可信网络服务中心向遵守本 EV CPS 第 5.6 节和其它有关条款的依赖方表明，CNNIC 可信网络服务中心根据本 EV CPS 向证书持有者颁发 EV 高级证书。经 CNNIC 可信网络服务中心签发的 EV 高级证书一经发出并由证书持有者接受，EV 高级证书立即生效。

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）及 EV 高级证书策略（EV CP）；对证书业务 guise（CPS）及 EV 高级证书业务规则（EV CPS）进行审核。

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 可信网络服务中心相关制度规定进行检查修改和批准续期，并对 CNNIC CA 可信网络服务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 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，更新及撤消交叉认证；
- 处理审计报告。

1.3 CNNIC 可信网络服务中心注册中心（RA）

CNNIC 可信网络服务中心仅有一个注册中心，设在 CNNIC。注册中心系统负责证书申请者 EV 高级证书的申请和审批及 EV 高级证书管理，并将 EV 高级证书

申请信息保存在认证中心。

1.4 CNNIC 可信网络服务中心本地受理点（LRA）

CNNIC 可信网络服务中心可把履行本 EV 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 EV 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 认证的可信服务器证书及可信 EV 服务器证书的注册服务机构。

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。

1.5 证书申请者

CNNIC 可信网络服务中心的 EV 高级证书申请者为商业、非商业、政府、私营类机构，根据中国的国情一概以企业、组织机构或其他单位代表。证书申请者持有私钥，并且身份信息会在 EV 高级证书中体现。。EV 高级证书申请者需要先向 CNNIC 可信网络服务中心提出证书服务的申请，然后进行其身份的核实，并向其颁发 EV 高级证书。

证书持有者的责任和义务参见下文 5.3 节。

1.6 证书持有者及依赖方

根据本 EV 高级证书业务规则，存在两类最终实体，包括 EV 高级证书持有者及信赖方。

证书持有者可以是证书持有机构，为 EV 高级证书持有和使用方。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。

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。

1.7 CNNIC 可信网络服务中心 EV CPS

CNNIC 可信网络服务中心增强型证书业务规则是公开的业务标准。CNNIC 可信网络服务中心在自己的证书链下颁发、撤销及更新 EV 高级证书。本 EV 高级证书业务规则主要包含如下几个部分：技术部分、组织架构部分、业务部分和法律部分。

CNNIC 可信网络服务中心证书策略颁发机构负责维护此 EV 高级证书业务规则、相关的协议以及本文档中相关的证书的策略。CNNIC 可信网络服务中心证书策略颁发机构联系方式：

中国互联网路信息中心 可信网络服务中心

地址：北京市海淀区中关村南四街四号，中科院软件园

邮编：100190

电话：58813075

本 EV 高级证书业务规则、证书策略及相关的规范都可以在 CNNIC 网站上查看到，地址： http://tns.cnnic.cn。

1.8 EV CPS 的适用性、修改及发布

CNNIC 可信网络服务中心证书策略颁发机构负责本 EV 高级证书业务规则中描述的证书策略的适用性。同时，颁发机构也要负责 EV 高级证书业务规则在下一版本发布之前所修改部分的适用性。

当证书策略颁发机构认定 EV 高级证书业务规则的变化部分对证书使用者有重大影响的时候，更新版本必须在 7 天之内在网站上予以发布，并详细说明变更版本号及变化部分。

如果证书策略颁发机构认定 EV 高级证书业务规则的变化部分对用户及依赖方的影响很小或没有影响，那么这种修改就不需要向用户通知，也不需要修改 EV 高级证书业务规则的版本号。

在 CNNIC 可信网络服务中心的 EV 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。

具体流程如下：

批准流程是：

（1）EV CPS 编写组编写或修订 EV CPS。

（2）EV 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 EV 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，EV CPS 正式对外发布。

1.9 EV CPS 解释权

CNNIC 可信网络服务中心对本 CPS 拥有最终解释权。

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 EV CPS 的含义或解释作任何陈述。

1.10 与应用标准的一致性

本篇 EV 高级证书业务规则中的条款符合业界标准，包括 AICPA/CICA 的 WebTrust 审计标准、CA/Browser Forum 的 EV 高级证书规则，以及其他相关的 CA 业务标准。

CNNIC 可信网络服务中心每年会由独立的外部审计机构来进行 AICPA/CICA 的 WebTrust 审计。每年的审计主题覆盖但不限于：

- CA 业务的披露
- 服务完整性
- CA 环境控制

CNNIC 可信网络服务中心根据 CA/Browser Forum 在网站 http://www.cabforum.org 上发布的《EV 指导准则》来颁发和管理 EV 高级证书。如果准则中的条款和本文档中的条款有不一致的地方，以准则中的内容为准。

1.11 数字证书策略概述

数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。数字证书允许持有者在信息交互中向对方表示自己的身份。数字证书在交易环境中充当着一个数字身份识别卡的角色。

扩展验证证书（EV 高级证书）包含着在 EV 指导中指定的信息，且这些信息依据 EV 指导中的标准被核实过。

1.12 CNNIC 可信网络服务中心 PKI 架构

CNNIC可信网络服务中心应用China Internet Network Information Center EV Certificates Root作为根证书来签发EV高级证书。EV高级证书架构为：China Internet Network Information Center EV Certificates Root（指纹：4f 99 aa 93 fb 2b d1 37 26 a1 99 4a ce 7f f0 05 f2 93 5d 1e，有效期至2030年8月31日），其证书可以通过http://www.cnnic.cn/download/cert/CNNICEVROOT.cer访问，并查询证书的指纹和有效期。

其子 CA CNNIC EV SSL 证书可以通过

http://www.cnnic.cn/download/cert/CNNICEVSSL.cer，查询该证书的指纹和有效期。

1.13 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 技术

本章节是对 CNNIC 可信网络服务中心构架及 PKI 服务体系的技术部分的说明。

2.1 CNNIC 可信网络服务中心构架

CNNIC 可信网络服务中心架构采用了可信赖的体系来提供证书服务。该体系包括计算机硬件、软件及程序，及用来防护安全风险的措施，并提高可用性、可依赖性和操作的正确性，以达到一个合理的安全水平。

2.1.1 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。

2.1.2 密钥的保护

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。该加密机用来生成、存储和使用根密钥对的。CNNIC 可信网络服务中心的根密钥对长度为 2048 位。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。

CNNIC 可信网络服务中心的根证书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。

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。

2.1.3 密钥的恢复

恢复加密机时也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。

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，然后签发新证书来代替

2.1.4 密钥的生成过程

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 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。

2.1.5 密钥的归档

根证书密钥对到期后，这些密钥对将归档保存至少 10 年。归档密钥对保存在符合国家标准的硬件密码模块中，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 EV CPS 第 2.1.8 节规定对其进行销毁。

2.1.6 密钥的备份

备份加密机时也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。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。

2.1.7 密钥的改变流程

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。

2.1.8 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。

认证证书的申请者私钥存在于证书申请者端，其证书过期后，应由认证证书使用者自行立即销毁私钥。 。

2.1.9 发放给证书使用者的 CA 根的公钥

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。

由管理员操作 CNNIC 可信网络服务中心证书和公钥的归档。

2.1.10 CNNIC 可信网络服务中心物理操作

2.1.10.1 物理地址

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。

2.1.10.2 访问控制

可进入关键区域，控制密码或其它操作程序并可能会对 EV 高级证书的签发、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

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。

CNNIC 可信网络服务中心确保在 EV 高级证书生成前，在对 EV 高级证书请求的处理和审批过程中至少是有两名人员的。

2.1.10.3 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。

2.1.10.4 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。

2.1.10.5 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。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。

2.1.10.6 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。

2.1.10.7 媒体介质存储

媒体介质存储及处置程序已经准备妥当。

2.1.10.8 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。

2.1.10.9 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。

2.1.10.10 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。

2.1.10.11 电磁防护

为防止内部信息通过电磁辐射泄漏，以及屏蔽外界的电磁干扰，CNNIC 可信网络服务中心专门建设了电磁屏蔽室，并通过了军 C 级认证。

CNNIC 可信网络服务中心的所有 CA 服务器、CA 加密机设备均部署在电磁屏蔽室中。

2.1.10.12 其他安全程序

CNNIC 可信网络服务中心执行了一套完整、合理的的安全程序，用来：

1、 保护 EV 请求、证书审批、颁发过程中所涉及的一切数据、软件、密钥及流程等；

2、 防止在 EV 数据的完整性、机密性和可用性中的可预见的威胁；

3、 防止对任何 EV 数据的未授权或非法的访问、使用、泄露、修改或破坏；

4、 防止对 EV 数据或 EV 流程的一些灾难性的破坏或损坏；

5、 遵守 CNNIC 可信网络服务中心的其他符合法律的安全需求

CNNIC 可信网络服务中心的安全程序包括常规的风险评估：

6、 鉴别可预见的内部和外部的威胁，例如未授权的访问、披露、

误用、修改或破坏任何的 EV 相关数据；

7、 评估这些潜在的威胁所引起的后果；

8、 评估 CNNIC 可信网络服务中心对这些威胁所采取的措施、政策是否充分；

基于风险评估，CNNIC 可信网络服务中心有相应的实施方案来保证 EV 高级证书业务的连续性和有效性。

2.1.11 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。

2.2 数字证书的管理

CNNIC 可信网络服务中心的证书管理包括但不限于以下部分：

- 对于证书申请者身份的验证
- 颁发证书
- 撤销证书
- 分发证书
- 发布证书
- 证书备份
- 根据特殊的使用用途的证书检索
- 对申请证书的域名的验证
- 对颁发的 EV 高级证书实体是否被授权的验证

2.3 CNNIC 可信网络服务中心储存库

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、EV CPS、EV CP 文本以及其它相关资料。

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

储存库中其他内容根据变更情况随时更改。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。

2.4 CNNIC 可信网络服务中心证书类型

CNNIC 可信网络服务中心随着业务的发展可能会扩展产品线，包括颁发的证书类型。每发布一款新的证书产品，CNNIC 可信网络服务中心将至少在提供新的证书业务之前的 7 天内，发布新的 CPS。

目前所颁发的域名证书品牌为：

“EV 高级服务器证书”，存在以下不同的类型：

- 单域名证书：CN 是一个固定域名
- 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 EV 高级服务器证书仅限于域名证书，不能用于其他用途。

2.5 EV 高级证书有效期

根据本 EV 高级证书业务规则发出的新申请人的 EV 高级证书，其有效期为一至二年。

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

2.6 扩展和命名

2.6.1 数字证书的扩展

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。

2.7 证书申请者私钥的生成和证书请求过程

2.7.1 私钥的生成

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。CNNIC 可信网络服务中心不提供私钥的生成、备份及恢复服务。在申请过程中，证书申请者将提交包括公钥以及企业详细信息的 CSR。

2.7.2 文档要求

在颁发 EV 高级证书前，证书申请者必须向 CNNIC 可信网络服务中心提交以下文档：

- EV 高级证书申请表
- 用户协议
- 及 CNNIC 可信网络服务中心根据 EV 指导准则要求的其他文档

2.7.3 申请者角色要求

EV 高级证书申请单位需要如下的角色，具体情况可进行调整：

- 证书申请者
- 证书申请批准者
- 协议签署者：EV 高级证书申请的协议必须是由被授权的人来签署。
- 申请代表人：当证书申请者和 CNNIC 可信网络服务中心有附属关系时，申请 EV 证书的使用条款必须由申请代表人确认和同意。该申请代表人为自然人，可以是申请单位的职员或者被授

权的代理人，并且已获得申请单位的授权可以承认和同意使用条款.

证书申请者可授权一个人来完成所有的角色，也可以分别让四个人来完成。EV 高级证书的申请者必须是被授权的自然人。申请者必须是申请单位的职员或被授权的代理人（需要有申请单位授权书或第三方的证明材料）。

2.7.4 EV 高级证书申请请求

- 总述：申请 EV 高级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。
- 请求内容：EV 高级证书请求必须包含经由申请人本人或其授权代表签字确认的申请书。同时还需要提交由申请人或其授权代表签署的协议，包含对提供 EV 高级证书所包含信息的准确无误的确认。
- 信息要求：EV 高级证书的请求可以包括证书中所显示的申请单位的全部实际信息，以及 CNNIC 可信网络服务中心根据《EV 指导准则》所需要的申请者的其他信息。为防止 EV 高级证书请求未能够包含必要的信息，CNNIC 可信网络服务中心会从证书申请者和协议签署者处获得其他的信息。

  申请者信息应该包括单不限于本《EV 指导准则》部分的要求。

2.8 证书申请者私钥的保护和备份

证书申请者的私钥在客户端产生，具有严密且安全的控制措施。CNNIC 可信网络服务中心不提供私钥的生成、备份及恢复服务。

CNNIC 可信网络服务中心强烈建议申请者使用密码、智能 IC 卡、其它硬件加密设备或加密软件来防止非法访问或使用私钥。

2.9 证书申请者公钥的传输

证书申请者使用服务器端的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。该请求（CSR）使用附带数字签名的 PKCS#10 格式，并可通过 CNNIC 网站上进行提交

（https://rawhois.cnnic.cn/pages/CertDownloadStart.ftl）。

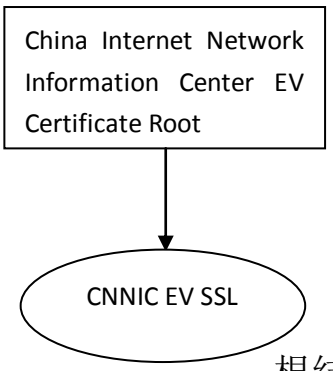
2.10 颁发证书的传输

CNNIC 可信网络服务中心批准该证书申请后，会将参考号、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

2.11 CNNIC 可信网络服务中心 EV 高级证书构架

CNNIC 可信网络服务中心 EV 高级证书构架如下：

2.11.1 EV 高级证书的根证书结构



根结构示意图

2.11.2 EV 根 CA 证书的相关说明

根CA证书没有包含 certificatePolicies 或 extendedKeyUsage extensions字段。
应用软件销售商或任何的证书依赖方均可以通过存储与根CA证书相关的EV数据标识符，来确认被批准签发EV高级证书的根CA。
其关键的扩展项，CA 域的部分已经设”TRUE”’,同时，pathLenConstraint 在其中没有体现.

2.11.3 EV 高级证书的内容及主题

根据《EV 指导准则》,对于 EV 高级证书内容的最基本要求：

主题机构信息

(a) 机构名称

证书域主题：OrganizationName（OID:）

必选/可选：必选

内容：此部分包含经 CNNIC 可信网络服务中心通过官方机构备案或文档核实后的证书持有者的名称。名称必须是法定单位的全称，且名称的长度最长不能超过 64 个字符。如果超过了 64 个字符，可以采用名称的缩写或忽略掉没有重大影响的词。

(b) 域名

证书域主题：CommonName

必选/可选：必选

内容：CN 在 EV 多域名证书时是多个域名的并列，单域名证书是单个域名。EV 高级证书不提供通配符证书类型。

(c) 业务类别

证书域主题：businessCategory

必选/可选：必选

内容：CNNIC 可信网络服务中心 EV 高级证书的业务类别字段包含了私营组织（V1.0,Cause 5.(b)）、政府实体 V1.0,Cause 5.(c)、商业实体 V1.0,Cause 5.(d)、非商业实体 V1.0,Cause 5.(e)

私营组织的定义：个体工商、个人独资企业

政府实体的定义：政府机关、事业单位

商业实体的定义：企业法人

非商业实体的定义：社团、其他

(d) 成立或注册区域

证书域：成立/注册所在地（国家、省、市），用于确定主体是国家级、省级、市级单位 必选/可选：必选

内容：不能包括不相关信息，如国家级单位就不可填写省、市字段；省级单位不可填写市字段。省、市、国家地区不能输入中文，

只能输入英文字母。国家地区默认为 CN。其他位置的城市及省市输入中文。

(e) 注册号

证书域主题：serialNumber

必选/可选：必选

内容：

对于私营组织，包含其成立或注册的机关分配给他的注册号。如无注册号，则填写其成立或注册日期。

对于政府实体，输入相应的话语指明该主体为政府实体。

对于商业实体，写入经过政府批准后获得的注册号。如没有注册号，则写入成立的日期。

(f) 营业及业务地址

证书域主题：包括国家、州或省、城市或乡镇、街道号码、邮编

必选/可选：国家、州或省、城市或乡镇是必选项；街道号码和邮编是可选项。

内容：主体营业地的物理地址。

2.11.4 密钥用法扩展项

CNNIC 可信网络服务中心采用的证书格式为 X509 第三版本。EV 高级证书中的密钥扩展项用来指定证书的用途以及技术上的要求。

CNNIC 可信网络服务中心的 EV 高级证书扩展项如下：

根 CA 证书

- 基本限制 (Basic constraints)：此扩展项必须为关键扩展则此扩展必须为关键扩展。CA字段必须置为真。pathLenConstraint字段不能出现

- 密钥用法 (Key usage)：“关键”字段。限制证书中密钥的用法。KeyCertSign 和 cRLSing 必须设置。

子 CA 证书

- 证书策略（certificatePolicies）：该扩展箱必须存在，且不得标识为关键扩展。证书策略的 OID 标识和位置。
- 证书废止列表发布点（cRLDistributionPoint）：本扩展项必须存在，且不得标识为关键扩展。发布点名称 = [证书废止列表发布点 HTTP URL]。
- 颁发机构信息访问（authorityInformationAccess）：本扩展项应该存在，且不得标识为关键扩展。需要包括 CNNIC 可信网络服务中心的 OCSP 响应地址（HTTP URL）。
- 基本限制 (Basic constraints)：
  此项设为真，扩展项标识为关键， Subject Type=CA
  Path Length Constraint=None
- 密钥用法 (Key usage)：该项必须存在，且标识为关键。CertSign 和 cRLSign 必须设置，且其他项不得设置。

用户证书

- 证书策略（certificatePolicies）：本扩展项必须存在，且不得标识为关键。

  Certificate Policy:

  Policy Identifier=EV策略OID

  Policy Qualifier Info:

  Policy Qualifier Id=CPS

  Qualifier: http://www.cnnic.cn/cps/

- 证书废止列表发布点（cRLDistributionPoint）：该扩展项存在，且未被标识为关键。包含CNNIC可信网络服务中心证书废止列表（CRL）的发布HTTP地址URL=http://www.cnnic.cn/download/evcrl/crl1.crl。

- 颁发机构信息访问（authorityInformationAccess）：该扩展项存在，且未被标识为关键。
  [1] Authority Info Access
  Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1)
  Alternative Name:
  URL=http://ocspev.cnnic.cn

[2]Authority Info Access
Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2)
Alternative Name:
URL=http://www.cnnic.cn/download/cert/CNNICEVSSL.cer。

- Path Length Constraint=None，Subject Type=End Entity；
- Digital Signature, Key Encipherment (a0)
- 增强型密钥用法（extKeyUsage）：服务器验证 （id-kp-serverAuth）值为 1.3.6.1.5.5.7.3.1 及客户端验证 （id-kp-clientAuth）值为 1.3.6.1.5.5.7.3.2。

2.11.5 EV 高级证书策略

证书策略详细说明了 CNNIC 可信网络服务中心签发和管理证书的规则和需求。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。

- EV 用户证书

  每一个 CNNIC 可信网络服务中心签发的 EV 高级证书都包含一个被 CNNIC 可信网络服务中心定义的 OID。此 OID 在证书中的证书策略（certificatePolicies）扩展项中，用来

  （1）表明该证书所对应的 CA 策略种类，

  （2）声明 CNNIC 可信网络服务中心遵守 EV 指导准则，

  （3）通过与软件应用销售商的先前协议，将证书标识为 EV 高级证书。

- EV 子 CA 证书

  CNNIC 可信网络服务中心暂无给从属认证机构签发证书的服务。

- 根 CA 证书

  CNNIC 可信网络服务中心不包含证书策略（certificatePolicies）或扩展终端密钥用法的扩展字段。

2.11.6 加密算法和密钥长度

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。

CNNIC 可信网络服务中心 EV 高级证书格式如下：

CNNICEV 高级服务器证书		
签名算法	Sha1RSA	
颁发者	CN	CNNIC EV SSL
	O	China Internet Network Information Center
	C	CN
有效期	1 年、2 年	
主题	CN	域名
	OU	部门名称
	O	单位名称
	L	城市
	S	州或省
	C	国家
	序列号	注册号码
颁发机构密钥标识符	KeyID	
密钥用法（非关键）	Digital Signature, Key Encipherment (a0)	
增强型密钥用法	服务器验证 (1.3.6.1.5.5.7.3.1)	
基本限制	Subject Type=End Entity Path Length Constraint=None	
证书策略	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.29836.1.10	

	[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cnnic.cn/cps/
CRL 分发策略	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN= crl*（*这个序号是根据证书序列号计算出来的） OU=crl O= China Internet Network Information Center C=cn C=cn [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.cnnic.cn/download/evcrl/crl*（*这个序号是根据证书序列号计算出来的）.crl
指纹算法	sha1RSA

2.12 CNNIC 可信网络服务中心 EV CRL 及其构架

2.12.1 EV CRL 发布

CNNIC可信网络服务中心也通过CRL列表对外发布中级根签发的最新CRL， 访问地址是：http://www.cnnic.cn/download/evcrl/crl*.crl*这个序号是根据证书序列号计算出来的）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。

由于没有进行中级根的废止，根签发的证书废止列表（CRL）,地址为：URL=http://www.cnnic.cn/download/evrootcrl/crl1.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 中保存所有的证书条目，保存期 5 年，已注销的证书的条目在 5 年内也不会删除 。

2.12.2 EV CRL 构架

CNNIC 可信网络服务中心 CRL 构架如下：

版本（Version）	显示 CRL 的版本号	X.509 第二版本
颁发机构名称（Signature）	签发 CRL 的 CA 的签名	CN = CNNIC EV SSL O = China Internet Network Information Center C = CN
算法标识（algorithmIdentifier）	定义签发 CRL 所使用的算法	
CRL 的签发者（Issuer）	签发 CRL 的 CA 的甄别名	
本次更新（thisUpdate）	CRL 发布时间	
下次更新 (next update)	预计下一个 CRL 更新时间	
注销证书目录 (revoked certificates)	CRL 入口	
	证书序列号	
	注销日期	

2.13 在线状态查询（OCSP）

2.13.1 OCSP 发布

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。

CNNIC 可信网络服务中心提供基于 HTTP 的证书状态在线查询服务（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。证书在线查询服务在用户点击获得证书状态响应的同时，将会看到该证书状态下次更新的具体时间（根据证书和根的不同，证书一般为不超过 12 小时更新一次，根证书为 120 天一更新）OCSP 中保存所有的证书条目。。

2.13.2 OCSP 结构

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。签发者公钥的 SHA1 数据摘要值和证书甄别名。
产生时间	OCSP 响应的产生时间。
下次更新时间	OCSP状态下次更新时间（根据证书和根的不同，证书一般为不超过12小时一更新，根证书为120天一更新）
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。

2.13.3 OCSP 请求

OCSP 请求可以支持 GET 和 POST 两种方式。如果请求内容小于 255 字节，可以使用 GET 方式。如果请求内容超过 255 字节，请求应该用 POST 方式

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

过期时间提醒： OSCP 所反馈的信息最长过期时间为 10 天，请所有通过此信息确认证书有效性的用户，注意此过期时间。

2.13.4 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

2.14 安全控制

2.14.1 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：

1, 系统安全配置，关闭不必要的服务与端口。

2, 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。

3, 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。

4, 日志和操作记录的审计制度。

5, 数据备份和恢复机制。

2.14.2 生命周期技术安全控制

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。

2.14.3 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。

3 组织架构

CNNIC 可信网络服务中心的证书业务均是在安全的环境下进行的。本章节主要是对安全策略、物理和逻辑访问控制的机制、服务级别及员工策略等的概述，来提供可信赖的证书业务。

3.1 对 EV 高级证书业务规则的遵从

CNNIC 可信网络服务中心安全依照该《CNNIC EV 高级证书业务规则》提供业务、运营及服务。

3.2 证书颁发机构业务的终止

一旦 CNNIC 可信网络服务中心由于任何原因需要终止证书业务，CNNIC 可信网络服务中心都将及时发布通知，并提供后续的服务包括对证书持有者的责任、记录的保留及恢复等。在证书业务终止前，CNNIC 可信网络服务中

心将进行以下操作：

- 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）

3.3 记录存档的格式

CNNIC 可信网络服务中心将以电子版或纸质版的形式来进行资料及记录的存档，同时也将制作并保存归档的副本。

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。

3.4 记录存档保留期

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。根据《EV 指导准则》的要求，CA 必须保留与 EV 高级证书请求及验证相关的一切文件及 EV 高级证书。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 EV 高级证书、注销的 EV 高级证书及证书废止列表（CRL）
- 定期事件记录
- EV 高级证书请求及验证过程中的所有文档
- 其它用以核实归档内容的工作日志。

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。所有的记录将存档在安全的地点。

3.5 核心功能日志

根据《EV 指导准则》的要求，CNNIC 可信网络服务中心将保留所有的日志记录，包括 EV 高级证书请求、处理、颁发过程中的所有日志。日志中需要记录时间、日期和人员的操作记录。所有的日志需要备份在一个放在安全地点的可移动介质中。

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。当可移动的存储介质即将结束生命周期时，将使用第三方的安全数据破坏仪器来清除这些数据。

存档记录包括但不限于以下事件：

- CNNIC可信网络服务中心密钥生命周期管理，包括：
  - 密钥的产生、备份、存储、修复、存档及销毁；
  - 密码设备声明周期管理事件。
- CNNIC可信网络服务中心及用户的EV高级证书声明周期管理事件，包括：
  - EV高级证书请求、续签及密钥重新申请及撤销；
  - 本指导准则规定的所有验证活动；
  - 验证电话的数据、时间、使用的电话号码、通话对象及最终结果；
  - EV高级证书请求的接收与拒绝；
  - EV高级证书的签发；及
  - EV高级证书撤销列表（CRLs）及OCSP条目
- 安全事件，包括：
  - 成功及失败的PKI系统访问尝试；
  - 实施的PKI及安全系统活动；
  - 安全策略的变更；
  - 系统崩溃、硬件故障及其他异常现象；
  - 防火墙及路由器活动；
  - CA设备的条目及从中退出。

- 登录条目必须包含下列元素：
  - 条目的数据和时间；
  - 制作日志的人员身份；及
  - 对条目的描述。

3.6 业务连续性计划和灾难恢复

为了保证服务的完整性，CNNIC 可信网络服务中心将实施、记录并阶段性测试业务的连续性和灾难恢复计划。此类计划需要至少每年更新或修改一次。

CNNIC 可信网络服务中心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。

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。

3.7 注销数据的可用性

CNNIC 可信网络服务中心发布 EV 高级证书撤销列表（EV CRL）供依赖方验证 CNNIC 可信网络服务中心签发的 EV 数字证书的有效性。EV CRL 包含注销 EV 高级证书的访问入口，并 24 小时均可进行访问的。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）。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。被废止

的 CRL 列表需要存档，并保存 10 年。

3.8 关键信息的发布

CNNIC 可信网络服务中心将在官方网站上发布《EV 高级证书业务规则》、与用户的协议等规定。所有的更新、修改都按照本 EV 高级证书业务规则中的流程严格执行。

3.9 机密信息

CNNIC 可信网络服务中心会依照本 EV 高级证书业务规则中的规定确保用户信息或机密信息的安全性和机密性。

3.9.1 机密信息的类型

CNNIC 可信网络服务中心将以下类型的信息列为机密的，并采用了合理的措施保证机密信息不被泄露：

a) 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。
b) 除在 EV 高级证书、EV CRL、EV 高级证书政策、EV 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。
c) 证书申请者提交的文档及资料包括证书申请者签署的协议、身份证明及其他需要提交的文件和材料（无论是通过审核和未通过审核的）。
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。
e) 业务连续性计划及灾难恢复计划
f) CNNIC 可信网络服务中心架构、证书管理、注册服务及数据的操作记录。

3.9.2 非机密信息

a) 由 CNNIC 可信网络服务中心签发的 EV 高级证书以及 EV 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 EV 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 EV 高级证书时，EV 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 EV 高级证书持有者和 EV 高级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。

3.9.3 机密信息的访问

只有被授权的人才能访问机密信息。CNNIC 可信网络服务中心的员工需要遵循相关的条款。

3.10 计算机安全审计程序

3.10.1 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 EV 高级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 EV 高级证书的请求
- 实际发出（包括证书注册、续费、补发等）、废止 EV 高级证书
- 更新储存库资料
- 汇编 EV 高级证书废止列表（EV 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

3.10.2 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。

3.10.3 保存期限

存盘审计追踪记录文件的保存期为 10 年。

3.10.4 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。

3.10.5 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。

3.10.6 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。

3.10.7 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加固措施。

3.11 员工的管理和规则

CNNIC 可信网络服务中心采取如下规则和管理流程来保证员工的可信性及是否可以满足相应的职责：

3.11.1 员工身份验证

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的背景、资历、经验等情况进行调查（其聘用前及其后有需要时定期进行）。以根据本 EV 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。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 EV CPS 履行职责。

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。调

查包括教育及工作经历，该信息将由人力资源进行相应的核实和确认。

3.11.2 培训及技能

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。培训内容包括但不限于：公钥基础设施（PKI）知识、验证的方式及步骤、业务流程、常见威胁及应对措施等相关的问题。

同时，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 EV 高级证书的注册、续费、补发及废止程序及与其职责有关的其它软件功能。

3.11.3 职责分离

CNNIC 可信网络服务中心有严格的管理措施，保证员工权限的独立性。EV 高级证书申请信息与证书的审核和签发分别由两个角色操作。

3.12 EV 审计

根据相关规定，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 EV 高级证书及公布 EV 高级证书废止列表（EV CRL）的系统是否严格遵守《EV 指导准则》、本 EV 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。

3.13 信息的发布

CNNIC 可信网络服务中心储存库，包括 EV 高级证书业务规则、EV 高级证书策略等，将在 CNNIC 官网(www.cnnic.cn)进行发布。储存库所在位置可供在线浏览，并可防止擅自修改。

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。

4 业务规则

本章主要是对需要提交的申请资料等证书申请过程的描述。其中特别强调，对于所有的 EV 高级证书申请、续费、补办两码或修改操作中，如果用户提交材料中使用其他语言（如英文）时，RA 需要将该语言明确表述。CA 将依赖 RA 的工作来执行交互相关和尽职调查。CA 的审核人员将核查 RA 的工作来验证其确实符合申请者的自身要求。

4.1 EV 高级证书申请

在 CNNIC 可信网络服务中心 EV 高级证书的申请中特别强调，所有用户在填写可信服务器证书申请表时，请注意如果某些项目为可选项如不填，则必须为空，不能填写任何其他内容，具体 EV 高级证书的申请流程，EV 高级证书的有效期为 1 年期和 2 年期证书，如果为 2 年期证书，在证书已经使用 9 个月——12 个月期间需要进行年检操作，该操需要提交相应的审核资料。如下：

4.1.1 单域名 EV 高级证书

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：
   - EV 高级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（每页加盖公章）；
     - 事业单位提供：组织机构代码证复印件（每页加盖公章）；

- 社团组织提供：组织机构代码证复印件（每页加盖公章）。

➢ EV 高级证书注册申请书原件。

➢ EV 高级证书申请者为企业/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。

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 EV 高级证书的域名注册者资料，查看域名注册者是否 EV 高级证书申请者一致，初步审核确定 EV 高级证书申请者确实拥有此域名。

(备注：在核实私人组织或业务实体公司申请人的法律性和身份调查时,也要关注其母公司,子公司或附属公司。)

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 EV 高级证书申请者修改域名注册者资料后再前来申请 EV 高级证书。

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。

（备注：针对高风险申请人(如金融类)，由 CA 中心标记为高风险或可疑的证书申请，需要进行额外的预防措施方法，包括检查组织名称，有针对性的查看是否存在钓鱼和其他欺诈行为。）

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“可信 EV 服务器证书核准证明”。如果未确认通过，则拒绝 EV 高级证书注册申请，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。

6. 申请书提交给可信网络服务中心委托的合法受理机构时，必须有该机构人员当面验签的证明书，该验签人员必须在该证明书亲笔签名。

4.1.2 多域名 EV 高级证书

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：
   - 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（每页加盖公章）；
     - 事业单位提供：组织机构代码证复印件（每页加盖公章）；
     - 社团组织提供：组织机构代码证复印件（每页加盖公章）。
   - EV 高级证书注册申请书原件。
   - EV 高级证书申请者为企业/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。
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 EV 高级证书申请者一致，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 EV 高级证书申请者与域名注册者不一致，则要求此 EV 高级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。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。
6. 申请书提交给可信网络服务中心委托的合法受理机构时，必须有该机构人员当面验签的证明书，该验签人员必须在该证明书亲笔签名。

4.1.3 申请方法

申请 EV 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。

EV 高级证书申请者可直接到 CNNIC 官网下载申请书及用户协议。证书请求（CSR）需要从网上直接提交。

4.2 EV 高级证书的续费

在 EV 高级证书持有者证书到期前，证书持有者需要获得新的 EV 高级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，EV 高级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”)。

EV 高级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 EV 高级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 EV 高级证书的时间长度＋当前 EV 高级证书剩余的时间长度。

4.2.1 单域名 EV 高级证书续费

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：

- EV 高级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（每页加盖公章）；
- 事业单位提供：组织机构代码证复印件（每页加盖公章）；
- 社团组织提供：组织机构代码证复印件（每页加盖公章）。
- 自然人提供：有效个人身份证明复印件。

➢ EV 高级证书续费申请书原件。

➢ EV 高级证书申请者为企业/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。

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。

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。如果未确认通过，则拒绝 EV 高级证书续费，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． EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。

5． EV 高级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。

6．CNNIC 可信网络服务中心签发 EV 高级证书，由 EV 高级证书申请经办人安装。

4.2.2 多域名 EV 高级证书续费

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：

➢ 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（每页加盖公章）；
- 事业单位提供：组织机构代码证复印件（每页加盖公章）；
- 社团组织提供：组织机构代码证复印件（每页加盖公章）。
- 自然人提供：有效个人身份证明复印件。

- EV 高级证书续费申请书原件。
- EV 高级证书申请者为企业/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。

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，。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。EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。
6. EV 高级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。
7. CNNIC 可信网络服务中心签发 EV 高级证书，由证书申请经办人安装。

4.3 EV 高级证书的补发

在 CNNIC 可信网络服务中心的 EV 高级证书体系中，EV 高级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 EV 高级证书补发后，原 EV 高级证书立即作废，新 EV 高级证书截至有效期与原 EV 高级证书相同

4.3.1 单域名证书补发

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：

   申请资料包括以下文档：

   - EV 高级证书补发申请书原件。
   - EV 高级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。

1. 本地受理点录入员通过 RA 系统将上述资料录入，提交申请。
2. 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。
3. 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。
4. 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。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。
5. EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。
6. EV 高级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。
7. CNNIC 可信网络服务中心签发 EV 高级证书，由证书申请经办人安装。

4.3.2 多域名证书补发

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：

   申请资料包括以下文档：

   - EV 高级证书补发申请书原件。
   - EV 高级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。

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。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. EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。
7. EV 高级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。
8. CNNIC 可信网络服务中心签发 EV 高级证书，由证书申请经办人安装。

4.4 EV 高级证书的变更

4.4.1 多域名 EV 高级证书域名变更

多域名 EV 高级证书提供域名修改服务，可以增加、删除和修改域名：

1. EV 高级证书申请经办人提交申请资料给本地受理点(LRA)录入员：

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（每页加盖公章）；
  - 事业单位提供：组织机构代码证复印件（每页加盖公章）；
  - 社团组织提供：组织机构代码证复印件（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 EV 高级证书修改申请书原件。
- EV 高级证书申请者为企业/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。

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。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. EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。
7. EV 高级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。
8. CNNIC 可信网络服务中心签发证书，由 EV 高级证书申请经办人安装。

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

4.5 EV 高级证书的年检

对于用户申请的 EV 高级证书超过 1 年以上的，其每年需要进行年检操作，具体操作同于其申请时所提交资料。

4.6 EV 高级证书验证过程

CNNIC 可信网络服务中心完全遵循《EV 指导准则》，在颁发 EV 高级证书前对证书所包含的信息做严格的验证。主要验证过程及措施如下：

4.6.1 申请者依法存在及身份的验证

1） 验证要求

EV 高级证书不面向个人，必须是企业、事业单位、组织社团等实体。

- 必须保证其依法存在
- 实体名称与 EV 高级证书申请者的名称一致
- 成立或注册管辖区域所分配的注册编号，如未指定则获取成立日期
- 注册机构的身份和地址

2） 验证方法

- 申请单位实体的验证：

  申请者需要提交如下材料

  企业法人：组织机构代码证复印件 或 营业执照复印件

  事业单位：组织机构代码证复印件

  政府机关：组织机构代码证复印件

  社团组织：组织机构代码证复印件

CNNIC 可信网络服务中心审核员将申请者提供的身份证明文件所包含的基本信息（包括单位名称、组成形式、注册编号、法人、注册资本、成立日基本信息（包括单位名称、组成形式、注册编号、法人、注册资本、成立日期、年检时间等等）与第三方提供的申请者基本信息进行比对，以确认该申请者的身份证明文件是否真实。

- 主要个人的验证

1）当面验证：包括用户协议的《CNNIC EV 高级证书申请书》的填写及签署必须由 CNNIC 可信网络服务中心注册服务机构的人员进行当面的验证。此外，CNNIC 可信网络服务中心注册服务机构的人员还需进行资料的搜集，包括主管人和经办人的身份证明、两份书面证明及根据要求需要的其他申请材料。

2）两份书面证明必须有一份是出自金融机构的，可以是：

- 有效的信用卡
- 有效的借记卡

- ◆ 提供金融机构的不少于 6 个月的银行结单
- ◆ 出自公认借贷人的不少于 6 个月的抵押声明

其他文件可包括：

- ◆ 固定电话账单
- ◆ 出生证明
- ◆ 当年的地方机构税单

3）申请者提供的主管人和经办人的身份证名证件，CNNIC 可信网络服务中心审核员将通过公安部门的身份证查询平台进行验证。

4.6.2 申请者匿名或假名

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。

4.6.3 申请者物理运营地址及联系电话的验证

为验证申请单位的物理存在，CNNIC 可信网络服务中心必须保证申请者提供的物理地址为申请单位或其子公司或母公司的业务地址。且申请者提供的电话号码是其营业地点的电话号码。

CNNIC 可信网络服务中心审核员将通过电信运营网站或电话、邮件等方式，进行物理运营地址及电话的验证：

4.6.4 申请者营运存在的验证

如申请单位成立时间不超过三年，CNNIC 可信网络服务中心必须确认其是否有经商能力。

- ◆ CNNIC 可信网络服务中心将从金融机构直接获取证明文件，已确认申请人在该机构有活期存款账户。
- ◆ 或申请单位需要提交在金融机构开有活期存款账户的法律意见书或会计书。

4.6.5 申请者域名的验证

为验证申请者对 EV 高级证书中列出的域名有唯一管理权，CNNIC 可信网络服务中心通过 WHOIS 查询核实域名所有者是否与申请单位一致。

若域名持有者的名称与申请者名称不相同，需由申请者提交补充资料：

- 补充域名持有者的授权及域名持有者的身份证明，或加盖授权单位的公章。
- 或补充相应说明资料，并且提供域名的注册合同。

4.6.6 主管人及经办人的名称、职务、权限的验证

CNNIC 可信网络服务中心 EV 高级证书申请有如下角色：

- 经办人：托管服务器的必须是受托机构的工作人员；独立主机的必须是申请单位的员工。
- 主管人：法人单位主管人为法定代表人授权代表；非法人单位主管人为单位负责人或单位负责人授权代表。此人为经办人的直接主管。
- 合同签署人：经办人及主管人。
  - CNNIC 可信网络服务中心审核员将对主管人和经办人的身份证进行官方的核实；
- 此外，CNNIC 可信网络服务中心审核员将通过电话与主管人、经办人及单位的前台（或总机）工作人员或人力资源部人员或其它同事分别进行职位等信息确认工作。申请代表人：当证书申请者和 CNNIC 可信网络服务中心有附属关系时，申请 EV 证书的使用条款必须由申请代表人确认和同意。该申请代表人为自然人，可以是申请单位的职员或者被授权的代理人，并且已获得申请单位的授权可以承认和同意使用条款.

4.6.7 证书请求及用户协议的验证

CNNIC 可信网络服务中心 EV 高级证书请求包括申请书和最终用户协

议两部分，需要主管人和经办人的签署。CNNIC 可信网络服务中心审核员将通过电话与主管人、经办人分别进行确认工作。

4.6.8 其他的验证要求

4.6.8.1 高风险的申请者

CNNIC 可信网络服务中心将定期关注及搜集钓鱼网站的列表，同时也将参考国际反钓鱼工作组（APWG）及中国反钓鱼联盟（APAC）发布的钓鱼网站名单，对于此类网站的申请需要严格、谨慎的把控或拒绝。

4.6.8.2 拒绝签发名单及其他黑名单

对于列在国家或当地政府禁止从事商业活动的组织，CNNIC 可信网络服务中心也将禁止对此部分用户发放 EV 高级证书。

4.7 EV 高级证书的废止

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 EV 域名证书：

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

4.7.1 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 EV 高级证书时，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 EV 高级证书的请求。在 EV 高级证书废止后，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 EV 高级证书持有者 EV 高级证书已被废止及被废止的理由。

EV 高级证书持有者也可以通过废止程序自行要求废止自己的 EV 高级证书。在 EV 高级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。

4.7.2 证书问题报告和相应机制

CNNIC 拥有7*24小时的证书问题报告和受理机制，在接受报告后并可以在24小时内对已经接受报告的证书进行调查和决定是否撤销或采取其他适当的行动的处理机制。其中主要包括对以下信息进行认定的过程：

1. 问题性质的认定；
2. 问题上报次数的调查；
3. 上报人身份认证；
4. 有关法律法规的遵循。

4.7.3 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。

4.7.4 单域名 EV 高级证书的废止

1. EV 高级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：

- EV 高级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 EV 高级证书废止，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。

4.7.5 多域名 EV 高级证书的废止

1. EV 高级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：

- EV 高级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：

- EV 高级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 EV 高级证书。如果审核不通过，则拒绝 EV 高级证书废止，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。

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，即终止该 EV 高级证书的使用效力。

4.8 签发接受 EV 高级证书

4.8.1 单域名 EV 高级证书的签发

1. EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。
2. EV 高级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 EV 高级证书，由证书申请经办人下载安装。
5. CNNIC 可信网络服务中心签发 EV 高级证书完成即表明申请者接受 CNNIC 可信网络服务中心的服务。

4.8.2 多域名 EV 高级证书的签发

1. EV 高级证书申请经办人在 Web 服务器中生成证书请求 CSR。
2. EV 高级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 EV 高级证书，由证书申请经办人下载安装。

5. CNNIC 可信网络服务中心签发 EV 高级证书完成即表明申请者接受 CNNIC 可信网络服务中心的服务。

4.8.3 证书发布

CNNIC 可信网络服务中心所发放的 EV 高级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 EV 高级证书注册信息。

4.8.4 废止信息发布形式

EV 高级证书废止信息除 HTTP 服务提供 CRL 查询外，CNNIC 可信网络服务中心还提供 OCSP 查询。

4.9 审计

CNNIC 可信网络服务中心在完成所有验证及签发 EV 高级证书后，会有审计员对所有步骤进行定期审查,审查结果记录在案，同时每年接受 CICA/AICPA 制定的审计机构定期审计工作。。

5 证书颁发的法律条款

本章主要叙述 CNNIC 可信网络服务中心数字证书的法律相关要求。

5.1 CNNIC 可信网络服务中心的责任和义务

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 EV CPS，CNNIC 可信网络服务中心所属认证中心有下述义务：

b) 遵守本 EV CPS、内部流程及其他的相关条例及流程
c) 遵守当地的法律法规
d) 接收注册中心的请求及时签发 EV 高级证书
e) 保证系统的安全性，包括密钥生成、密钥保护等机制

f) 废止证书并及时发布 EV 高级证书废止列表（EV CRL）

g) 一旦私钥泄露，立即发布通知

h) 严格验证 EV 高级证书申请请求

i) 提供 EV 高级证书续费、年检、更新等操作的服务

5.2 CNNIC 可信网络服务中心责任的豁免

CNNIC 可信网络服务中心将采取合理的技术及管理措施，向各 EV 高级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 EV 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 EV 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 EV 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 EV 高级证书持有者同意 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 EV 高级证书持有者因信任另一 EV 高级证书持有者由 CNNIC 可信网络服务中心所发出的 EV 高级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 EV 高级证书持有者因 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。

5.3 证书持有者的责任和义务

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 EV 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 EV 高级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 EV 高级证书持有者证书资料的任何变动通知给 CNNIC 可信网络服务中心。
f) 如发生本 EV CPS 的 4.5.2 节中的情形时，需要废止 EV 高级证书，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，以下第 5.5 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 EV CPS 可能废止 EV 高级证书的情况下，或 EV 高级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 EV CPS 废止证书并通知 EV 高级证书持有者后，均不得在交易中使用 EV 高级证书。
i) 在明知 CNNIC 可信网络服务中心根据本 EV CPS 可能废止 EV 高级证书的情况下，或 EV 高级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 EV CPS 废止 EV 高级证书并通知 EV 高级证书持有者后，须立即通知从事当时仍有待完成的任何交易的 EV 高级证书信赖方，并明确说明，用于该交易的 EV 高级证书需要废止(由 CNNIC 可信网络服务中心或经 EV 高级证书持有者申请)，EV 高级证书信赖方不得在交易中信任此 EV 高级证书。
j) EV 高级证书的使用仅限于合法目的，并且符合相关的 EV 高级证书策略和本 EV CPS（或其他公布的商业事项）。如果注册者有理由相信与 EV 高级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 EV 高级证书。
k) EV 高级证书持有者承认，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。

5.4 证书持有者的保证

申请人须签署或确定接受一份协议（按本 EV 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 EV 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 EV 高级证书持有者及其授权者外，并无其它人士曾取用 EV 高级证书持有者的私人密钥。
- 使用与证书持有者 EV 高级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。
- EV 高级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。
- EV 高级证书将只会用于符合本 EV CPS 认可并合法的用途。
- 在 EV 高级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。

5.5 CNNIC 可信网络服务中心注册中心（RA）的责任和义务

注册中心系统负责 EV 高级证书申请者的申请和审批及 EV 高级证书管理，并将 EV 高级证书申请信息传递到认证中心。注册中心有下述义务：

- 根据本 EV CPS 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 EV 高级证书申请生效，将其安全传递给认证中心（CA），EV 高级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
- 通知申请人有关已批准或被拒绝的 EV 高级证书申请
- 通知 EV 高级证书持有者有关已废止的 EV 高级证书

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。

5.6 依赖方的责任和义务

信任 CNNIC 可信网络服务中心数字证书的 EV 高级证书信赖方负责：

- EV 高级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。
- 在信任该 EV 高级证书前，确定使用 EV 高级证书是适合本 EV CPS 规定的用途，即仅信任 CNNIC 可信网络服务中心的 EV 高级证书用作域名证书。
- 在信任 EV 高级证书前查核 EV 高级证书废止列表（EV CRL）上的证书状态。
- 执行所有适当 EV 高级证书路径验证程序。
- 一旦信任了该 EV 高级证书，即表明同意接受本 CPS 所规定的责任限制的条款。

5.7 CNNIC 可信网络服务中心储存库的责任和义务

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 EV 高级证书废止列表（EV CRL）、CNNIC 可信网络服务中心中级根证书和根证书、本 EV CPS 以及 CNNIC 可信网络服务中心 EV 高级证书策略（EV CP）文本一份以及其它相关资料。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 可信网络服务中心储存库应根据自己制定的策略，及时公布 EV 高级证书废止列表（EV CRL）及其他内容。

5.8 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 EV 高级证书业务规则所载条款，在条件适用于本 EV 高级证书的情况下，根据相关规定

作为 EV 高级证书认证机构签发本 EV 高级证书。

因此，任何人士信任本 EV 高级证书前均应阅读适用于 EV 高级证书的 EV 高级证书业务规则（可浏览 http://tns.cnnic.cn）。中华人民共和国法律适用于本 EV 高级证书，信赖方须承认因信任本 EV 高级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 EV 高级证书用来签发的条款及条件，则不应信任本 EV 高级证书。

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

信赖方信任本 EV 高级证书前确保信任行为公平合理无恶意，方可信任本 EV 高级证书；

信任本 EV 高级证书前，确定 EV 高级证书的使用就 EV CPS 规定的用途而言实属适当；

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

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 EV 高级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 EV 高级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 EV 高级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 EV 高级证书购买价格的 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 EV 高级证书的信任额度为 EV 高级证书购买价格的 10 倍。

EV 高级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 EV 高级证书包含任何由 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 EV 高级证书并不就这类对因合理信任本 EV 高级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。”

5.9 CNNIC 可信网络中心对有缺陷的 EV 高级证书所承担的责任

若 EV 高级证书持有者接受 EV 高级证书后发现，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 EV 高级证书并重新签发。或者在接受 EV 高级证书后三个月内发现这种情况且证书持有者不再需要 EV 高级证书，则在 CNNIC 同意的前提下，可以申请退款。如果 EV 高级证书持有者在接受 EV 高级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。

5.10 证书废弃列表的发布

CNNIC 可信网络服务中心保留发布证书废弃列表（CRL）的权利。

5.11 信息的发布

重要的信息会逐渐的更新版本。此类更新应该指定版本号，并标明发布的时间。

5.12 信息准确性

CNNIC 可信网络服务中心储存库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。保证其内容的准确和及时。

5.13 保险计划

一旦 CNNIC 可信网络服务中心违反《EV 高级证书持有者协议》或者负有任何职务职责的情况下，而造成 EV 高级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 EV 高级证书不得超过 EV 高级证书购买价格的 10 倍。

EV 高级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 EV 高级证书的签发、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。

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

5.14 条款冲突

若本 EV 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 EV CPS 条款约束，除非该等条款受法律禁止。

5.15 CNNIC 可信网络服务中心所有权

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

5.16 管辖法律

本 EV CPS 受中华人民共和国法律管辖。

5.17 司法机构

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

5.18 分割性

若本 EV 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 EV 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 EV CPS。经营活动的改变会与 EV CPS 的修改相一致。

5.19 费用

EV 高级证书（包括单域名证书和多域名证书）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。

CNNIC 可信网络服务中心证书查询现阶段为免费服务。

CNNIC 可信网络服务中心证书废止现阶段为免费服务。

5.20 退款

CNNIC 可信网络服务中心证书费用在证书签发后概不退还。