(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109818946 B
(45)授权公告日 2022.07.26

(21)申请号 201910028642.5
(22)申请日 2019.01.11
(65)同一申请的已公布的文献号
申请公布号 CN 109818946 A
(43)申请公布日 2019.05.28
(73)专利权人 网宿科技股份有限公司
地址 200030 上海市徐汇区斜土路2899号光启文化广场A幢5楼
(72)发明人 江武 邓洛
(74)专利代理机构 北京华智则铭知识产权代理有限公司 11573
专利代理师 姜子朋 王昌贵
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)

审查员 肖丽金

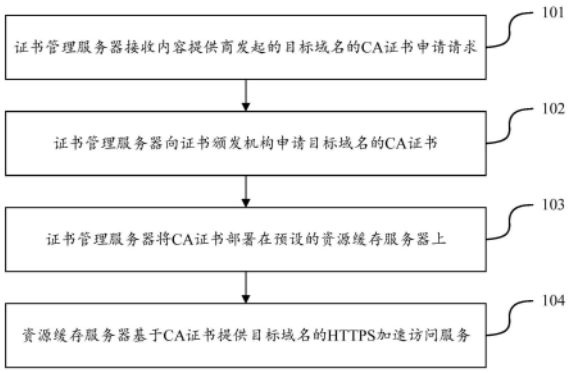
权利要求书3页 说明书8页 附图2页

(54)发明名称

CA证书申请和部署的方法和系统

(57)摘要

本发明公开了一种CA证书申请和部署的方法和系统，属于内容分发网络技术领域。所述方法包括：证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求；所述证书管理服务器向证书颁发机构申请所述目标域名的CA证书；所述证书管理服务器将所述CA证书部署在预设的资源缓存服务器上；所述资源缓存服务器基于所述CA证书提供所述目标域名的HTTPS加速访问服务。本发明可以加快CA证书部署速度，节约时间和人力。



CN 109818946 B

1.一种CA证书申请和部署的方法,其特征在于,包括:

证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求;

所述证书管理服务器向证书颁发机构申请所述目标域名的CA证书,并接收所述证书颁发机构发送的反馈信息和针对所述目标域名的域名验证请求,其中,所述证书管理服务器通过预设的资源缓存服务器上配置的转发设置接收所述目标域名的域名验证请求,所述反馈信息包括验证密 钥,当接收到所述目标域名的域名验证请求时,所述证书管理服务器向所述证书颁发机构发送所述验证密钥,以在验证通过后接收所述CA证书;

所述证书管理服务器将所述CA证书部署在所述资源缓存服务器上;

所述资源缓存服务器基于所述CA证书提供所述目标域名的HTTPS加速访问服务。

2.根据权利要求1所述的方法,其特征在于,所述证书管理服务器向证书颁发机构申请所述目标域名的CA证书,并通过预设的资源缓存服务器上配置的转发设置接收所述目标域名的域名验证请求,将验证密钥发送给所述证书颁发机构,以在验证通过后接收所述CA证书,包括:

所述证书管理服务器将所述目标域名的CA证书申请请求发送给所述证书颁发机构。

3.根据权利要求2所述的方法,其特征在于,在所述证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求之前,所述方法还包括:

所述资源缓存服务器配置所述目标域名的加速访问服务,并在DNS系统中根据所述资源缓存服务器的域名配置所述目标域名的CNAME记录。

4.根据权利要求3所述的方法,其特征在于,所述证书管理服务器通过预设的资源缓存服务器上配置的转发设置接收所述目标域名的域名验证请求,所述反馈信息包括验证密钥;当接收到所述目标域名的域名验证请求时,所述证书管理服务器向所述证书颁发机构发送所述验证密钥,包括:

所述资源缓存服务器接收所述证书颁发机构根据所述目标域名的CNAME记录发送的针对所述目标域名的域名验证请求;

所述资源缓存服务器根据预先配置的转发设置,将所述域名验证请求转发给所述证书管理服务器;

所述证书管理服务器确定所述域名验证请求对应的验证密钥,并将所述验证密钥发送给所述证书颁发机构。

5.根据权利要求2所述的方法,其特征在于,所述CA证书申请请求对应的反馈信息还包括CA证书申请ID,

所述证书管理服务器接收所述证书颁发机构发送的所述目标域名的CA证书,包括:

所述证书管理服务器周期性向所述证书颁发机构发送含有所述CA证书申请ID的CA证书查询请求,以使所述证书颁发机构根据所述CA证书查询请求,将所述目标域名的CA证书发送给所述证书管理服务器;

在接收到所述证书颁发机构发送的所述目标域名的CA证书后,所述证书管理服务器停止向所述证书颁发机构发送所述CA证书查询请求。

6.根据权利要求2所述的方法,其特征在于,所述资源缓存服务器基于所述CA证书提供所述目标域名的HTTPS加速访问服务,包括:

当接收到客户端针对目标域名的HTTPS加速访问请求时,所述资源缓存服务器使用所

述目标域名的CA证书与所述客户端进行CA认证；

在所述CA认证通过后，所述资源缓存服务器根据所述HTTPS加速访问请求，将HTTPS加速响应请求发送给所述客户端；或者，

在所述CA认证通过后，所述资源缓存服务器将所述HTTPS加速访问请求转换成HTTP访问请求后转发给所述目标域名的源站服务器。

7.一种CA证书申请和部署的系统，其特征在于，所述系统包括证书管理服务器和资源缓存服务器：

所述证书管理服务器，用于接收内容提供商发起的目标域名的CA证书申请请求；

所述证书管理服务器，用于向证书颁发机构申请所述目标域名的CA证书，并接收所述证书颁发机构发送的反馈信息和针对所述目标域名的域名验证请求，其中，所述证书管理服务器通过预设的资源缓存服务器上配置的转发设置接收所述目标域名的域名验证请求，所述反馈信息包括验证密 钥，当接收到所述目标域名的域名验证请求时，所述证书管理服务器向所述证书颁发机构发送所述验证密钥，以在验证通过后接收所述CA证书；

所述证书管理服务器，用于将所述CA证书部署在预设的资源缓存服务器上；

所述资源缓存服务器，用于基于所述CA证书提供所述目标域名的HTTPS加速访问服务。

8.根据权利要求7所述的系统，其特征在于，所述证书管理服务器，具体用于：

将所述目标域名的CA证书申请请求发送给所述证书颁发机构。

9.根据权利要求8所述的系统，其特征在于，在所述资源缓存服务器，还用于：

配置所述目标域名的加速访问服务，并在DNS系统中根据所述资源缓存服务器的域名配置所述目标域名的CNAME记录。

10.根据权利要求9所述的系统，其特征在于：

所述资源缓存服务器，具体用于接收所述证书颁发机构根据所述目标域名的CNAME记录发送的针对所述目标域名的域名验证请求；根据预先配置的转发设置，将所述目标域名的域名验证请求转发给所述证书管理服务器；

所述证书管理服务器，具体用于确定所述目标域名的域名验证请求对应的验证密钥，并将所述验证密钥发送给所述证书颁发机构。

11.根据权利要求8所述的系统，其特征在于，所述CA证书申请请求对应的反馈信息还包括CA证书申请ID，

所述证书管理服务器，具体用于：

周期性向所述证书颁发机构发送含有所述CA证书申请ID的CA证书查询请求，以使所述证书颁发机构根据所述CA证书查询请求，将所述目标域名的CA证书发送给所述证书管理服务器；

在接收到所述证书颁发机构发送的所述目标域名的CA证书后，停止向所述证书颁发机构发送所述CA证书查询请求。

12.根据权利要求8所述的系统，其特征在于，所述资源缓存服务器，具体用于：

当接收到客户端针对目标域名的HTTPS加速访问请求时，使用所述目标域名的CA证书与所述客户端进行CA认证；

在所述CA认证通过后，根据所述HTTPS加速访问请求，将HTTPS加速响应请求发送给所述客户端；或者，

在所述CA认证通过后,将所述HTTPS加速访问请求转换成HTTP访问请求后转发给所述目标域名的源站服务器。

CA证书申请和部署的方法和系统

技术领域

[0001] 本发明涉及内容分发网络技术领域，尤其涉及一种CA证书申请和部署的方法和系统。

背景技术

[0002] 超文本传输安全协议(HTTPS，Hyper Text Transfer Protocol over)是在HTTP的基础上再加入安全套接层(SSL，Secure Socket Layer)协议，当客户端基于HTTPS访问某个域名时，通过SSL协议，预先安装了该域名的CA证书的源站服务器可以与客户端进行CA认证，在CA认证通过后，源站服务器就可以向客户端提供对该域名基于HTTPS的访问服务，将客户端对该域名的访问数据进行加密后反馈给客户端。

[0003] 当需要域名提供基于HTTPS的访问服务时，该域名的内容提供商(ICP，Internet Content Provider)首先向证书颁发机构(CA，Certificate Authority)申请该域名的CA证书，然后将CA证书部署到该域名对应的源站服务器上。在此基础上，该域名的内容提供商还可以将该域名的CA证书提供给CDN厂商，由CDN厂商将CA证书部署在CDN系统中为该域名提供加速访问服务的资源缓存服务器上，从而实现通过CDN系统对该域名的HTTPS访问服务进行加速。这样，当客户端通过CDN系统访问该域名时，为该域名提供加速访问服务的资源缓存服务器就可以和客户端进行CA认证，并在CA认证通过之后为客户端提供基于HTTPS的加速访问服务。

[0004] 在实现本发明的过程中，发明人发现现有技术中至少存在以下问题：

[0005] CDN厂商收到内容提供商发来的CA证书后，还需要对CA证书进行验证，并对验证结果人工审核之后才能够部署到资源缓存服务器，浪费时间与人力。

发明内容

[0006] 为了解决现有技术的问题，本发明实施例提供了一种CA证书申请和部署的方法和系统。所述技术方案如下：

[0007] 第一方面，提供了一种CA证书申请和部署的方法，包括：

[0008] 证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求；

[0009] 所述证书管理服务器向证书颁发机构申请所述目标域名的CA证书；

[0010] 所述证书管理服务器将所述CA证书部署在预设的资源缓存服务器上；

[0011] 所述资源缓存服务器基于所述CA证书提供所述目标域名的HTTPS加速访问服务。

[0012] 进一步的，所述证书管理服务器向证书颁发机构申请所述目标域名的CA证书，包括：

[0013] 所述证书管理服务器将所述目标域名的CA证书申请请求发送给所述证书颁发机构；

[0014] 所述证书管理服务器接收所述证书颁发机构发送的所述CA证书申请请求对应的反馈信息，所述反馈信息包括验证密钥；

[0015] 当接收到所述证书颁发机构发出的针对所述目标域名的域名验证请求时，所述证书管理服务器向所述证书颁发机构发送所述验证密钥；

[0016] 所述证书管理服务器接收所述证书颁发机构发送的所述目标域名的CA证书。

[0017] 进一步的，在所述证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求之前，所述方法还包括：

[0018] 所述资源缓存服务器配置所述目标域名的加速访问服务，并在DNS系统中根据所述资源缓存服务器的域名配置所述目标域名的CNAME记录。

[0019] 进一步的，所述当接收到所述证书颁发机构发出的针对所述目标域名的域名验证请求时，所述证书管理服务器向所述证书颁发机构发送所述验证密钥，包括：

[0020] 所述资源缓存服务器接收所述证书颁发机构根据所述目标域名的CNAME记录发送的针对所述目标域名的域名验证请求；

[0021] 所述资源缓存服务器根据预先配置的转发设置，将所述目标域名的域名验证请求转发给所述证书管理服务器；

[0022] 所述证书管理服务器确定所述目标域名的域名验证请求对应的验证密钥，并将所述验证密钥发送给所述证书颁发机构。

[0023] 进一步的，所述CA证书申请请求对应的反馈信息还包括CA证书申请ID，所述证书管理服务器接收所述证书颁发机构发送的所述目标域名的CA证书，包括：

[0024] 所述证书管理服务器周期性向所述证书颁发机构发送含有所述CA证书申请ID的CA证书查询请求，以使所述证书颁发机构根据所述CA证书查询请求，将所述目标域名的CA证书发送给所述证书管理服务器；

[0025] 在接收到所述证书颁发机构发送的所述目标域名的CA证书后，所述证书管理服务器停止向所述证书颁发机构发送所述CA证书查询请求。

[0026] 进一步的，所述资源缓存服务器基于所述CA证书提供所述目标域名的HTTPS加速访问服务，包括：

[0027] 当接收到客户端针对目标域名的HTTPS加速访问请求时，所述资源缓存服务器使用所述目标域名的CA证书与所述客户端进行CA认证；

[0028] 在所述CA认证通过后，所述资源缓存服务器根据所述HTTPS加速访问请求，将HTTPS加速响应请求发送给所述客户端；或者，

[0029] 在所述CA认证通过后，所述资源缓存服务器将所述HTTPS加速访问请求转换成HTTP访问请求后转发给所述目标域名的源站服务器。

[0030] 第二方面，提供了一种CA证书申请和部署的系统，所述系统包括证书管理服务器和资源缓存服务器：

[0031] 所述证书管理服务器，用于接收内容提供商发起的目标域名的CA证书申请请求；

[0032] 所述证书管理服务器，用于向证书颁发机构申请所述目标域名的CA证书；

[0033] 所述证书管理服务器，用于将所述CA证书部署在预设的资源缓存服务器上；

[0034] 所述资源缓存服务器，用于基于所述CA证书提供所述目标域名的HTTPS加速访问服务。

[0035] 进一步的，所述证书管理服务器，具体用于：

[0036] 将所述目标域名的CA证书申请请求发送给所述证书颁发机构；

[0037] 接收所述证书颁发机构发送的所述CA证书申请请求对应的反馈信息,所述反馈信息包括验证密钥;

[0038] 当接收到所述证书颁发机构发出的针对所述目标域名的域名验证请求时,向所述证书颁发机构发送所述验证密钥;

[0039] 接收所述证书颁发机构发送的所述目标域名的CA证书。

[0040] 进一步的,在所述资源缓存服务器,还用于:

[0041] 配置所述目标域名的加速访问服务,并在DNS系统中根据所述资源缓存服务器的域名配置所述目标域名的CNAME记录。

[0042] 进一步的,所述资源缓存服务器,具体用于接收所述证书颁发机构根据所述目标域名的CNAME记录发送的针对所述目标域名的域名验证请求;根据预先配置的转发设置,将所述目标域名的域名验证请求转发给所述证书管理服务器;

[0043] 所述证书管理服务器,具体用于确定所述目标域名的域名验证请求对应的验证密钥,并将所述验证密钥发送给所述证书颁发机构。

[0044] 进一步的,所述CA证书申请请求对应的反馈信息还包括CA证书申请ID,所述证书管理服务器,具体用于:

[0045] 周期性向所述证书颁发机构发送含有所述CA证书申请ID的CA证书查询请求,以使所述证书颁发机构根据所述CA证书查询请求,将所述目标域名的CA证书发送给所述证书管理服务器;

[0046] 在接收到所述证书颁发机构发送的所述目标域名的CA证书后,停止向所述证书颁发机构发送所述CA证书查询请求。

[0047] 进一步的,所述资源缓存服务器,具体用于:

[0048] 当接收到客户端针对目标域名的HTTPS加速访问请求时,使用所述目标域名的CA证书与所述客户端进行CA认证;

[0049] 在所述CA认证通过后,根据所述HTTPS加速访问请求,将HTTPS加速响应请求发送给所述客户端;或者,

[0050] 在所述CA认证通过后,将所述HTTPS加速访问请求转换成HTTP访问请求后转发给所述目标域名的源站服务器。

[0051] 本发明实施例提供的技术方案带来的有益效果是:

[0052] 本发明实施例中,证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求;证书管理服务器向证书颁发机构申请目标域名的CA证书;证书管理服务器将CA证书部署在预设的资源缓存服务器上;资源缓存服务器基于CA证书提供目标域名的HTTPS加速访问服务。这样,内容提供商直接通过CDN系统中的证书管理服务器向证书颁发机构申请CA证书,证书颁发机构可以将生成的CA证书直接发送给证书管理服务器,证书管理服务器不需要再对CA证书进行验证就可以直接将CA证书部署在资源缓存服务器上,避免了验证结果的人工审核,加快了CA证书部署速度,节约时间和人力。

附图说明

[0053] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于

本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0054] 图1是本发明实施例提供的一种CA证书申请和部署方法的流程图；

[0055] 图2是本发明实施例提供的一种CA证书申请和部署系统的结构示意图。

具体实施方式

[0056] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0057] 本发明实施例提供了一种CA证书申请和部署的方法，该方法可以适用于CDN系统中，CDN系统可以包括资源缓存服务器和证书管理服务器，资源缓存服务器可以是一个或者多个，并分别与证书管理服务器连接，资源缓存服务器可以为目标域名提供加速访问服务，证书管理服务器可以存储并管理目标域名的CA证书。本实施例的应用场景可以是：当目标域名的内容提供商向CDN系统申请目标域名的加速访问服务时，可以同时在CDN系统提交CA证书申请请求，然后由CDN系统中的证书管理服务器向证书颁发机构申请目标域名的CA证书，并在目标域名的CA证书申请成功之后，由证书管理服务器直接从证书颁发机构获取目标域名的CA证书，证书管理服务器再将获取到的目标域名的CA证书部署在之前设置的为目标域名提供加速访问服务的资源缓存服务器上。这样，当客户端基于HTTPS访问目标域名时，部署了目标域名的CA证书的资源缓存服务器就可以与客户端进行CA认证，并在CA认证通过后，为目标域名提供HTTPS加速访问服务。

[0058] 下面将结合具体实施方式，对图1所示的一种CA证书申请和部署的流程进行详细的说明，内容可以如下：

[0059] 步骤101：证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求。

[0060] 在实施中，当在CDN系统申请配置目标域名的加速访问服务时，内容提供商还可以在CDN系统中的证书管理服务器上同时申请目标域名的CA证书，这样，当客户端通过CDN系统访问目标域名时，CDN系统就可以为客户端提供目标域名的HTTPS加速访问服务，提高客户端访问过程中的数据安全性。内容提供商在证书管理服务器上申请目标域名的CA证书时，只需要在证书管理服务器上相关的CA证书一键申请页面中提交想要申请CA证书的目标域名即可，证书管理服务器接收到内容提供商发起的目标域名的CA证书申请请求后，可以自动完成后续申请过程，简化了CA证书申请操作。

[0061] 步骤102：证书管理服务器向证书颁发机构申请目标域名的CA证书。

[0062] 在实施中，证书管理服务器在接收到目标域名的CA证书申请请求后，将目标域名的CA证书申请请求发送给证书颁发机构，向证书颁发机构申请目标域名的CA证书。

[0063] 可选的，在申请CA证书的过程中，证书颁发机构会对申请CA证书的目标域名进行验证，相应的，步骤102的处理具体可以如下：证书管理服务器将目标域名的CA证书申请请求发送给证书颁发机构；证书管理服务器接收证书颁发机构发送的CA证书申请请求对应的反馈信息，反馈信息包括验证密钥；当接收到证书颁发机构发出的针对目标域名的域名验证请求时，证书管理服务器向证书颁发机构发送验证密钥；证书管理服务器接收证书颁发机构发送的目标域名的CA证书。

[0064] 在实施中，证书管理服务器在接收到目标域名的CA证书申请请求后，将该CA证书

申请请求发送给证书颁发机构。证书颁发机构根据目标域名的CA证书申请请求，直接向证书管理服务器发送反馈信息，反馈信息中至少包含有验证密钥(authKey)，还可以包含有目标域名或其他信息。证书管理服务器在接收到反馈信息后，将反馈信息存储在证书管理服务器本地对应的位置，例如，对于目标域名domian，可以在证书管理机构的硬盘中建立domian/.well-known/pki-validation文件夹，并将包括验证密钥authKey在内的目标域名domian的反馈信息存储在该文件夹中。之后，证书颁发机构会向目标域名发送域名验证请求，并最终被证书管理服务器接收到。证书管理服务器从上述文件夹中获取本地存储的验证密钥，然后将验证密钥直接发送给证书颁发机构。证书颁发机构接收到验证密钥后，判断之前发送的反馈信息中包含的验证密钥与当前接收到的验证密钥是否一致，如果一致，则对目标域名的验证通过，证书颁发机构就可以生成目标域名的CA证书，进而，证书管理服务器就可以接收到证书颁发机构发送的目标域名的CA证书。

[0065] 可选的，在CA证书申请过程中，为了使证书管理服务器能够接收到证书颁发机构针对目标域名发送的域名验证请求和CA证书，需要使发送给目标域名的信息被转发到CDN系统，故而，相应的处理可以如下：资源缓存服务器配置目标域名的加速访问服务，并在DNS系统中根据资源缓存服务器的域名配置目标域名的CNAME记录。

[0066] 在实施中，在证书管理服务器向证书颁发机构发送目标域名的CA证书申请请求之前，CDN系统在资源缓存服务器上配置目标域名的加速访问服务，并且在DNS系统中根据资源缓存服务器的域名，配置目标域名的CNAME记录。这样，发送给目标域名的任何信息，在经过DNS系统进行域名解析之后，都可以被发送到CDN系统中为目标域名提供加速访问服务的资源缓存服务器上。

[0067] 可选的，通过DNS系统只能使CDN系统中的资源缓存服务器接收到发送给目标域名的信息，为了使CDN系统中的证书管理服务器可以接收到证书颁发机构发送的域名验证请求，相应的处理可以如下：资源缓存服务器接收证书颁发机构根据目标域名的CNAME记录发送的针对目标域名的域名验证请求；资源缓存服务器根据预先配置的转发设置，将域名验证请求转发给证书管理服务器；证书管理服务器确定域名验证请求对应的验证密钥，并将验证密钥发送给证书颁发机构。

[0068] 在实施中，在向证书管理服务器发送反馈信息后，证书颁发机构进一步向目标域名发送域名验证请求。证书颁发机构向目标域名发送的域名验证请求，根据之前DNS系统中配置的目标域名的CNAME记录，经过DNS系统进行域名解析，最终被发往CDN系统中为目标域名提供加速访问服务的资源缓存服务器。资源缓存服务器上预先配置有域名验证请求的转发设置，在接收到域名验证请求后，资源缓存服务器根据转发设置，将域名验证请求在CDN系统内转发给证书管理服务器。证书管理服务器接收到域名验证请求后，根据域名验证请求，在本地确定域名验证请求对应的验证密钥，然后根据域名验证请求，直接将验证密钥发送给证书颁发机构。

[0069] 例如，可以在资源缓存服务器上配置转发设置：将包含特定URL的请求转发给证书管理服务器，其中特定URL为/.well-known/pki-validation/authKey，当证书颁发机构根据http://domian/.well-known/pki-validation/authKey发送针对目标域名domain的域名验证请求时，经过DNS系统解析，该域名验证请求被资源缓存服务器接收到，由于该域名验证请求包含的URL符合资源缓存服务器配置的转发设置，因此，资源缓存服务器可以将该

域名验证请求转发给证书管理服务器。进一步的，如前文所述，当接收到该域名验证请求后，证书管理服务器就可以查找本地的domian/.well-known/pki-validation文件夹，获得其中存储的验证密钥authKey，并将验证密钥authKey直接发送给证书颁发机构。

[0070] 可选的，证书颁发机构发送的CA证书申请请求对应的反馈信息中，还可以包括CA证书申请ID，这样，证书管理服务器就可以主动向证书颁发机构获取CA证书，相应的处理可以如下：证书管理服务器周期性向证书颁发机构发送含有CA证书申请ID的CA证书查询请求，以使证书颁发机构根据CA证书查询请求，将目标域名的CA证书发送给证书管理服务器；在接收到证书颁发机构发送的目标域名的CA证书后，证书管理服务器停止向证书颁发机构发送CA证书查询请求。

[0071] 在实施中，证书管理服务器接收到的证书颁发机构发来的CA证书申请请求对应的反馈信息中，除了验证密钥和目标域名外，还包括CA证书申请ID。CA证书申请ID是证书颁发机构在接收到目标域名的CA证书申请请求时生成的，可以是申请CA证书的订单编号，能够用于查询CA证书申请进度或其他申请过程中的相关信息。在向证书颁发机构发送验证密钥之后，每隔固定时间间隔(例如15分钟)，证书管理服务器可以向证书颁发机构发送含有CA证书申请ID的CA证书查询请求。这样，证书颁发机构在接收到CA证书查询请求之后，就可以根据其中包含的CA证书申请ID，查询该CA证书申请ID对应的CA证书是否已经生成。如果已经生成，证书颁发机构就可以对该CA证书查询请求进行反馈，将该CA证书直接发送给证书管理服务器。证书管理服务器在收到证书颁发机构根据CA证书查询请求反馈的CA证书后，则停止向证书颁发机构发送该CA证书申请请求，并在前文所述的CA证书一键申请页面中，向内容提供商反馈CA证书申请成功。如果证书管理服务器在预设的时间范围(通常可以设置为24小时)内始终没有接收到证书颁发机构根据CA证书查询请求反馈的CA证书，说明可能是之前发送给证书颁发机构的验证密钥错误、证书颁发机构没有接收到验证密钥等原因导致的CA证书无法生成，或者证书颁发机构没有接收到CA证书查询请求导致CA证书虽然生成，但没有被证书管理服务器接收到，此时，需要管理人员对没有接收到CA证书的原因进行分析，然后再做进一步处理。

[0072] 需要说明的是，证书管理服务器还可以通过证书颁发机构通知回调的方式获取目标域名的CA证书，如果采用该方式获取目标域名的CA证书，需要在步骤102向证书颁发机构申请目标域名的CA证书时，同时向证书颁发机构发送回调URL，并在资源管理服务器配置回调URL转发设置，这样，在生成目标域名的CA证书之后，证书颁发机构根据目标域名和回调URL，发送目标域名的CA证书，并被资源缓存服务器接收到，资源缓存服务器就可以根据配置的回调URL转发设置，将目标域名的CA证书转发给证书管理服务器。

[0073] 例如，可以预先设置回调URL为/.well-known/callback，目标域名为domian，在步骤102时，证书管理服务器将/.well-known/callback加入目标域名的CA证书申请请求，发送给证书颁发机构，然后在资源管理服务器配置转发设置：将包含回调URL的请求转发给证书管理服务器，其中，回调URL为/.well-known/callback。这样，当证书颁发机构生成目标域名的CA证书之后，证书颁发机构根据http://domian/.well-known/callback发送目标域名domian的CA证书。通过DNS系统解析后，资源管理服务器接收到该CA证书，然后根据资源管理接配置的转发设置，将该CA证书转发给证书管理服务器。

[0074] 步骤103：证书管理服务器将CA证书部署在预设的资源缓存服务器上。

[0075] 在实施中，证书管理服务器在接收到证书颁发机构发来的目标域名的CA证书后，根据CDN系统为目标域名配置的加速访问服务，将CA证书部署在为目标域名提供加速访问服务的资源缓存服务器上。

[0076] 步骤104：资源缓存服务器基于CA证书提供目标域名的HTTPS加速访问服务。

[0077] 在实施中，证书管理服务器在预设的资源缓存服务器上部署好目标域名的CA证书之后，资源缓存服务器就可以根据该CA证书，提供目标域名的HTTPS加速访问服务。

[0078] 可选的，在部署了目标域名的CA证书之后，资源缓存服务器在为目标域名提供加速访问服务的时候，就可以使用该CA证书进行CA验证，实现基于HTTPS的加速访问服务，相应的处理可以如下：当接收到客户端针对目标域名的HTTPS加速访问请求时，资源缓存服务器使用目标域名的CA证书与客户端进行CA认证；在CA认证通过后，资源缓存服务器根据HTTPS加速访问请求，将HTTPS加速响应请求发送给客户端；或者，在CA认证通过后，资源缓存服务器将HTTPS加速访问请求转换成HTTP访问请求后转发给目标域名的源站服务器。

[0079] 在实施中，资源缓存服务器上部署好目标域名的CA证书之后，当客户端对目标域名发起HTTPS访问请求时，经过DNS系统对目标域名进行解析，资源缓存服务器可以接收到该HTTPS访问请求，然后，资源缓存服务器使用部署的目标域名的CA证书与客户端进行CA认证，在CA认证通过之后，资源缓存服务器就可以将该HTTPS访问请求对应的数据通过HTTPS加速响应请求反馈给客户端；如果资源缓存服务器上没有该HTTPS加速访问请求对应的数据，资源缓存服务器可以将该HTTPS访问请求转换成HTTP访问请求后转发给目标域名的源站服务器，以获得对应的数据。

[0080] 本发明实施例中，证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求；证书管理服务器向证书颁发机构申请目标域名的CA证书；证书管理服务器将CA证书部署在预设的资源缓存服务器上；资源缓存服务器基于CA证书提供目标域名的HTTPS加速访问服务。这样，内容提供商直接通过CDN系统中的证书管理服务器向证书颁发机构申请CA证书，证书颁发机构可以将生成的CA证书直接发送给证书管理服务器，证书管理服务器不需要再对CA证书进行验证就可以直接将CA证书部署在资源缓存服务器上，避免了验证结果的人工审核，加快了CA证书部署速度，节约时间和人力。

[0081] 基于相同的技术构思，本发明实施例还提供了一种CA证书申请和部署的系统，所述系统包括证书管理服务器和资源缓存服务器：

[0082] 所述证书管理服务器，用于接收内容提供商发起的目标域名的CA证书申请请求；

[0083] 所述证书管理服务器，用于向证书颁发机构申请所述目标域名的CA证书；

[0084] 所述证书管理服务器，用于将所述CA证书部署在预设的资源缓存服务器上；

[0085] 所述资源缓存服务器，用于基于所述CA证书提供所述目标域名的HTTPS加速访问服务。

[0086] 可选的，所述证书管理服务器，具体用于：

[0087] 将所述目标域名的CA证书申请请求发送给所述证书颁发机构；

[0088] 接收所述证书颁发机构发送的所述CA证书申请请求对应的反馈信息，所述反馈信息包括验证密钥；

[0089] 当接收到所述证书颁发机构发出的针对所述目标域名的域名验证请求时，向所述证书颁发机构发送所述验证密钥；

[0090] 接收所述证书颁发机构发送的所述目标域名的CA证书。

[0091] 可选的，在所述资源缓存服务器，还用于：

[0092] 配置所述目标域名的加速访问服务，并在DNS系统中根据所述资源缓存服务器的域名配置所述目标域名的CNAME记录。

[0093] 可选的，

[0094] 所述资源缓存服务器，具体用于接收所述证书颁发机构根据所述目标域名的CNAME记录发送的针对所述目标域名的域名验证请求；根据预先配置的转发设置，将所述目标域名的域名验证请求转发给所述证书管理服务器；

[0095] 所述证书管理服务器，具体用于确定所述目标域名的域名验证请求对应的验证密钥，并将所述验证密钥发送给所述证书颁发机构。

[0096] 可选的，所述CA证书申请请求对应的反馈信息还包括CA证书申请ID，

[0097] 所述证书管理服务器，具体用于：

[0098] 周期性向所述证书颁发机构发送含有所述CA证书申请ID的CA证书查询请求，以使所述证书颁发机构根据所述CA证书查询请求，将所述目标域名的CA证书发送给所述证书管理服务器；

[0099] 在接收到所述证书颁发机构发送的所述目标域名的CA证书后，停止向所述证书颁发机构发送所述CA证书查询请求。

[0100] 可选的，所述资源缓存服务器，具体用于：

[0101] 当接收到客户端针对目标域名的HTTPS加速访问请求时，使用所述目标域名的CA证书与所述客户端进行CA认证；

[0102] 在所述CA认证通过后，根据所述HTTPS加速访问请求，将HTTPS加速响应请求发送给所述客户端；或者，

[0103] 在所述CA认证通过后，将所述HTTPS加速访问请求转换成HTTP访问请求后转发给所述目标域名的源站服务器。

[0104] 需要说明的是：上述实施例提供的CA证书申请和部署系统与CA证书申请和部署方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0105] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务端，或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0106] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

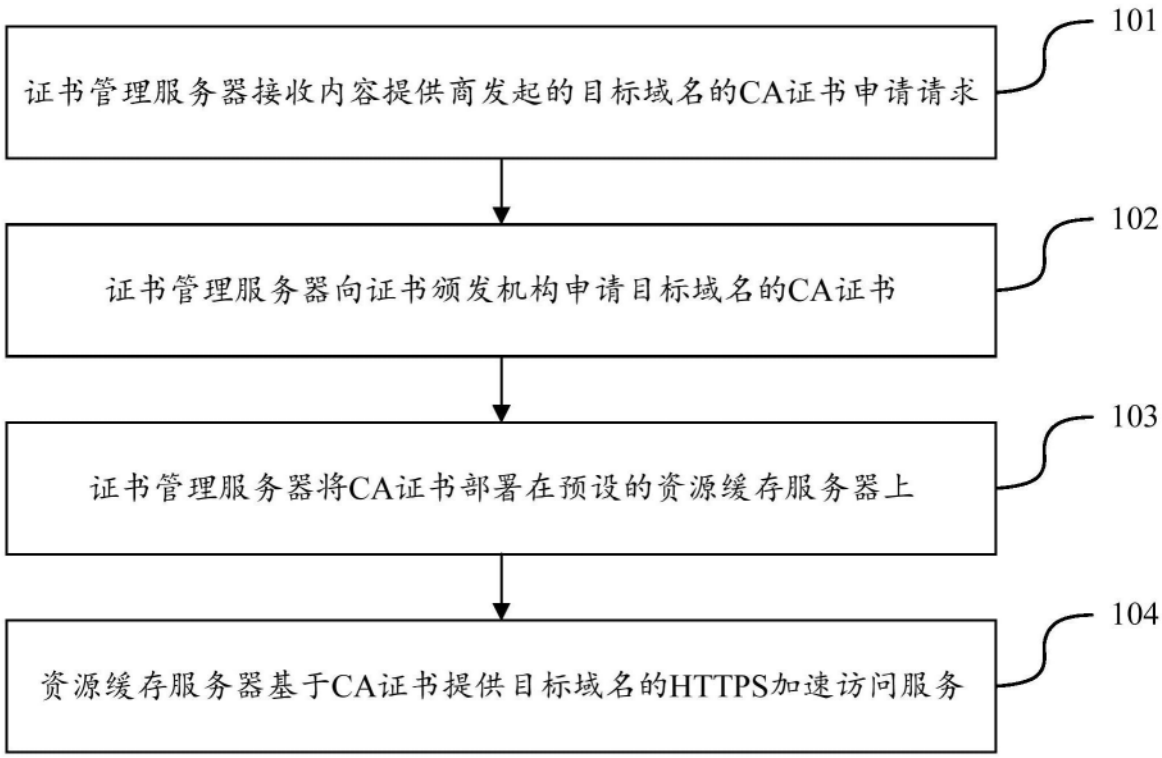

101
证书管理服务器接收内容提供商发起的目标域名的CA证书申请请求
102
证书管理服务器向证书颁发机构申请目标域名的CA证书
103
证书管理服务器将CA证书部署在预设的资源缓存服务器上
104
资源缓存服务器基于CA证书提供目标域名的HTTPS加速访问服务

图1

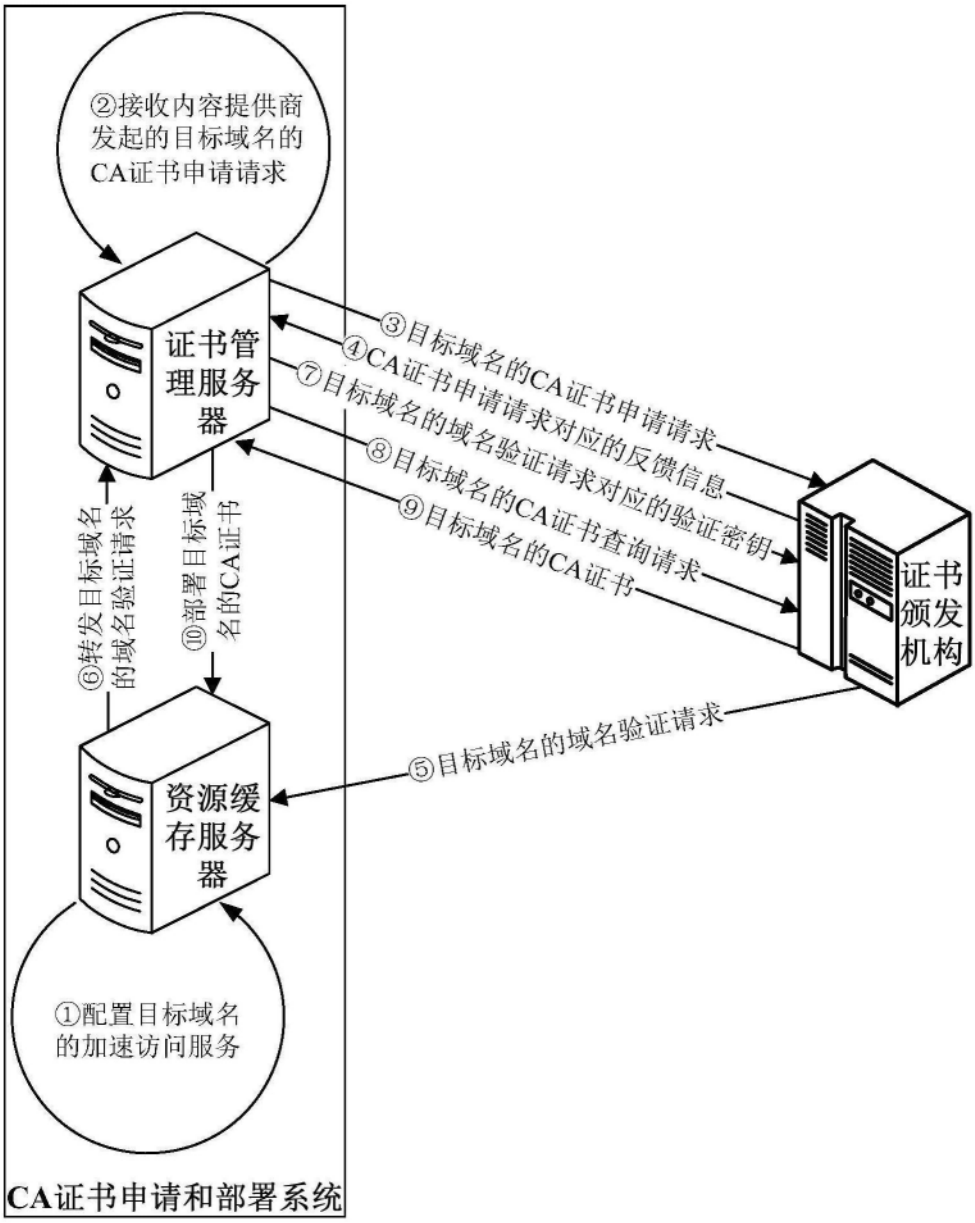

②接收内容提供商发起的目标域名的CA证书申请请求
证书管理服务器
③目标域名的CA证书申请请求
④CA证书申请请求对应的反馈信息
⑦目标域名的域名验证请求对应的验证密钥
⑧目标域名的CA证书查询请求
⑨目标域名的CA证书
证书颁发机构
⑥转发目标域名的域名验证请求
⑩部署目标域名的CA证书
⑤目标域名的域名验证请求
资源缓存服务器
①配置目标域名的加速访问服务
CA证书申请和部署系统

图2