(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111865992 A
(43)申请公布日 2020.10.30

(21)申请号 202010718560.6

(22)申请日 2020.07.23

(71)申请人 亚数信息科技(上海)有限公司
地址 200233 上海市徐汇区桂平路391号3号楼32层3201A室

(72)发明人 厚建勇 陈启敬

(74)专利代理机构 上海科盛知识产权代理有限公司 31225
代理人 杨宏泰

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 29/12(2006.01)

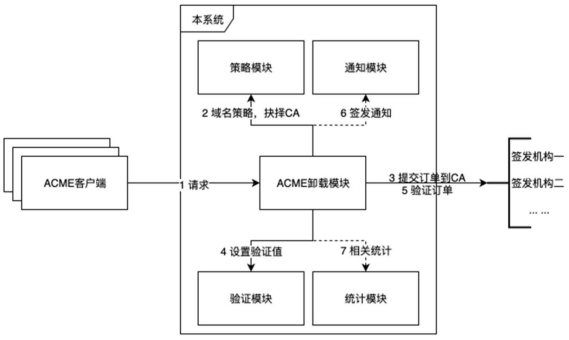
权利要求书3页 说明书6页 附图2页

(54)发明名称

一种ACME集中管理系统及其负载均衡方法

(57)摘要

本发明涉及一种ACME集中管理系统及其负载均衡方法,该系统分别连接ACME客户端以及多个证书颁发机构CA,包括ACME卸载模块以及分别与ACME卸载模块连接的统计模块、策略模块、验证模块和通知模块,所述的ACME卸载模块与ACME客户端通信,并且与多个证书颁发机构CA通信。与现有技术相比,本发明具有避免验证频繁、快速签发证书副本、更高效的证书签发等优点。



CN 111865992 A

1.一种ACME集中管理系统,其特征在于,该系统分别连接ACME客户端以及多个证书颁发机构CA,包括ACME卸载模块以及分别与ACME卸载模块连接的统计模块、策略模块、验证模块和通知模块,所述的ACME卸载模块与ACME客户端通信,并且与多个证书颁发机构CA通信。

2.根据权利要求1所述的一种ACME集中管理系统,其特征在于,该系统的工作流程包括以下步骤:

1)ACME客户端向ACME卸载模块发起证书申请,ACME卸载模块进行数据解析卸载;

2)ACME卸载模块通过策略模块设定的策略选择证书颁发机构CA并提交订单到对应的证书颁发机构CA开始申请证书,

3)ACME卸载模块通过验证模块设置验证值并通过证书颁发机构CA对订单进行验证;

4)验证通过后ACME卸载模块通过通知模块签发申请状态通知,并通过统计模块统计数据。

3.根据权利要求2所述的一种ACME集中管理系统的负载均衡方法,其特征在于,包括以下步骤:

1)用户通过ACME集中管理系统创建ACME目录URL获得URL地址,并且携带与订单绑定的token;

2)ACME客户端通过ACME目录URL获取API列表;

3)ACME客户端通过调用newNonce函数与newAccount API完成账户的注册;

4)ACME客户端通过调用newNonce函数与newOrder API将域名信息带入ACME集中管理系统;

5)ACME集中管理系统通过AMCE客户端请求的ACME目录URL中的token获取到对应的策略;

6)ACME集中管理系统通过ACME客户端请求的ACME目录URL中的token获取到对应的订单信息;

7)ACME集中管理系统创建一个包含域名待提交到证书颁发机构CA且未带有CSR的CA订单;

8)ACME集中管理系统返回携带订单ID以及用以域名所有权验证的ACME Authorization数据,并在此步中欺骗ACME客户端表示ACME客户端的域名已通过验证,并发送已通过验证信息,由此跳过由传统ACME客户端来自动配置完成ACME验证域名验证的过程;

9)ACME客户端生成私钥和CSR,通过调用newNonce函数与finalizeOrder函数提交订单ID与CSR到ACME集中管理系统;

10)ACME集中管理系统将待提交的CA订单与CSR一并提交到证书颁发机构CA获取到域名验证信息,调用验证模块进行域名验证;

11)验证模块收到需要验证的域名和验证值,通过文件代理和DNS CNAME授权设置验证值;

12)ACME集中管理系统调用CA证书获取API,证书颁发机构CA完成域名验证后签发并返回证书内容;

13)ACME集中管理系统按照ACME协议方式将证书内容返回给ACME客户端,完成证书签发过程。

4.根据权利要求3所述的一种ACME集中管理系统的负载均衡方法,其特征在于,所述的步骤7)中,当订单在多个ACME客户端形成竞争关系时,通过对订单加互斥锁避免多个ACME客户端同时请求同一ACME目录URL带来的冲突,并且对后续的同一请求采取挂起的方式。

5.根据权利要求4所述的一种ACME集中管理系统的负载均衡方法,其特征在于,所述的步骤7)中,对于取到互斥锁的ACME客户端,ACME集中管理系统创建一个包含域名待提交到证书颁发机构CA且未带有CSR的CA订单。

6.根据权利要求4所述的一种ACME集中管理系统的负载均衡方法,其特征在于,在按照步骤1)-13)完成具有竞争关系的多个ACME客户端中的ACME客户端A的证书签发过程后,对于具有竞争关系的多个ACME客户端中的ACME客户端B,通过以下步骤完成证书签发过程:

14)ACME集中管理系统释放ACME客户端A的互斥锁后,ACME客户端B获取到互斥锁,ACME客户端B获取ACME客户端A创建的CA订单号;

15)ACME客户端B重复步骤8)-9);

16)ACME集中管理系统将对已提交的CA订单与CSR一并提交到证书颁发机构CA获取到域名验证信息,调用验证模块进行域名验证;

17)重复步骤11)-13)完成ACME客户端B的证书签发过程。

7.根据权利要求6所述的一种ACME集中管理系统的负载均衡方法,其特征在于,对于具有竞争关系的多个ACME客户端中的其余ACME客户端,按照步骤14)-17)依次完成证书签发过程。

8.根据权利要求3所述的一种ACME集中管理系统的负载均衡方法,其特征在于,所述的步骤11)中,通过ACME客户端请求的ACME目录URL中的token获取到的订单的策略所绑定的域名验证方式进行所有权验证。

9.根据权利要求8所述的一种ACME集中管理系统的负载均衡方法,其特征在于,当策略所绑定的域名验证方式为文件代理时,通过以下步骤完成域名所有权验证:

111)验证模块收到需要验证的域名和验证值,将域名作为Key,将验证值作为Value存储到KV存储器中;

112)证书颁发机构CA进行域名验证时,请求域名的HTTP或HTTPS地址,通过用户预先设置的到ACME集中管理系统的文件代理的规则,将证书颁发机构CA的域名所有权验证反向代理到验证模块并携带域名作为HTTP请求的Host头部字段;

113)验证模块通过获取反向代理的HTTP请求中的Host头部字段得到需要验证的域名;

114)验证模块通过域名在KV存储器获取到对应的验证值并通过HTTP文本返回给证书颁发机构CA。

10.根据权利要求8所述的一种ACME集中管理系统的负载均衡方法,其特征在于,当策略所绑定的域名验证方式为DNS CNAME授权时,通过以下步骤完成域名所有权验证:

1)验证模块收到需要验证的域名和验证值,将域名作为Key,将验证值作为Value存储到KV存储器中;

2)证书颁发机构CA进行域名验证时,请求域名的DNS TXT记录,该域名通过用户预先在其DNS解析服务配置的DNS CNAME记录指向验证模块提供的DNS解析服务所提供的DNS CNAME代理域名;

3)证书颁发机构CA所请求的域名验证请求将被代理验证模块提供的DNS解析服务;

4)DNS解析服务获取到证书颁发机构CA所请求的DNS CNAME代理域名的DNS TXT解析请求,通过提取请求中的域名前缀的方式得到所请求的域名;

5)验证模块通过域名在KV存储器获取到对应的验证值并通过DNS TXT记录方式返回给证书颁发机构CA。

一种ACME集中管理系统及其负载均衡方法

技术领域

[0001] 本发明涉及互联网通信技术领域，尤其是涉及一种ACME集中管理系统及其负载均衡方法。

背景技术

[0002] ACME(Automatic Certificate Management Environment，rfc8555)协议是互联网标准，根据该协议，首先用户通过下载方式在需要部署证书服务器节点上安装好ACME客户端，然后通过命令行指定CA(Certificate Authority，证书颁发机构)提供的目录URL，指定私钥类型，指定验证方式，指定验证路径(文件路径或DNS服务商API)，然后指定部署路径，证书重载命令，最后完成证书的申请部署，ACME客户端会周期性检查自己维护的证书列表是否需要更新，并自动化完成上次的申请动作。

[0003] 在实际应用中，ACME作为自动化证书申请标准，非常便利，也产生了多个基于ACME协议的证书自动化申请和部署的客户端，结合ACME的服务端(例如Let'sEncrypt免费证书)可以快速方便的获得SSL/TLS证书，导致了HTTPS的普及和HTTPS所依赖的SSL/TLS证书大规模应用，但也带来了管理的难题：

[0004] 1、企业可选择的提供ACME的商业CA很少

[0005] 商业CA签发的证书具有更高的可信度和服务保障，目前众多商业CA是不支持ACME协议，一方面是商业策略，例如目前DigiCert只对OV、EV开始尝试提供ACME支持，不对大规模用的DV提供，目前是Beta阶段。另一方面是支持ACME对传统CA来说有一定技术挑战和审计风险，通过API也能达到自动化的效果，如果企业想要通过ACME协议来自动化管理证书，又需要有多个可供选择的商业CA品牌，这就变得非常被动。

[0006] 2、大量ACME客户端节点重复申请新证书，导致失败率过高，成本增加

[0007] 正常使用的ACME客户端是部署在每台WEBSERVER服务器上，生成独立ACME账户，对于同一个域名申请证书，会导致大量CA域名所有权验证，从而导致申请时间长，失败率高，甚至会触发CA速率限制(例如Let'sEncrypt每周限制5份)，导致无法申请证书。同时对于使用ACME来适配商业CA，如果重复申请新证书，目前的商业CA普遍的计费策略会导致费用增加。

[0008] 3、证书验证时间长，因缓存等问题造成签发失败率过高，维护成本高

[0009] 为了验证域名所有权，需要通过多种方式进行验证，比如DNS、HTTP文件验证。DNS验证会有一个验证值生效时间的问题，当在域名服务商处添加好验证值，而验证值未能及时生效，造成签发失败。而HTTP文件验证需要用户有较高的运维知识，需要确保文件能够被正确访问到，如ACME协议中的.well-known/acme-challenge/<token>路径，实际操作过程中容易出错。

[0010] 4、ACME客户端因网络或CA故障不能自动切换证书品牌

[0011] 当使用ACME客户端申请证书时，目前的客户端自动化过程中证书申请、续期是和一个固定的地址进行通信，因网络抖动(光缆挖断)或CA出现重大bug造成自动化证书更新

不成功。申请过程不能够智能的切换申请渠道,造成证书申请失败。

[0012] 5、无法感知到证书申请失败的情况

[0013] 目前的ACME客户端是直接与CA提供的ACMEURL地址通信(例如Let'sEncrypt的https://acme-v02.api.letsencrypt.org/directory),当网络发生抖动,或CA故障等原因造成请求失败时,也无法感知到,无法及时作出调整。

发明内容

[0014] 本发明的目的就是为了克服上述现有技术存在的缺陷而提供一种ACME集中管理系统及其负载均衡方法。

[0015] 本发明的目的可以通过以下技术方案来实现:

[0016] 一种ACME集中管理系统,该系统分别连接ACME客户端以及多个证书颁发机构CA,包括ACME卸载模块以及分别与ACME卸载模块连接的统计模块、策略模块、验证模块和通知模块,所述的ACME卸载模块与ACME客户端通信,并且与多个证书颁发机构CA通信。

[0017] 该系统的工作流程包括以下步骤:

[0018] 1)ACME客户端向ACME卸载模块发起证书申请,ACME卸载模块进行数据解析卸载;

[0019] 2)ACME卸载模块通过策略模块设定的策略选择证书颁发机构CA并提交订单到对应的证书颁发机构CA开始申请证书,

[0020] 3)ACME卸载模块通过验证模块设置验证值并通过证书颁发机构CA对订单进行验证;

[0021] 4)验证通过后ACME卸载模块通过通知模块签发申请状态通知,并通过统计模块统计数据。

[0022] 一种ACME集中管理系统的负载均衡方法,包括以下步骤:

[0023] 1)用户通过ACME集中管理系统创建ACME目录URL获得URL地址,并且携带与订单绑定的token;

[0024] 2)ACME客户端通过ACME目录URL获取API列表;

[0025] 3)ACME客户端通过调用newNonce函数与newAccount API完成账户的注册;

[0026] 4)ACME客户端通过调用newNonce函数与newOrder API将域名信息带入ACME集中管理系统;

[0027] 5)ACME集中管理系统通过AMCE客户端请求的ACME目录URL中的token获取到对应的策略,具体为:Token绑定订单的主证书颁发机构CA和备用证书颁发机构CA,当主证书颁发机构CA签发失败时,自动切换到备用证书颁发机构CA;

[0028] 6)ACME集中管理系统通过ACME客户端请求的ACME目录URL中的token获取到对应的订单信息;

[0029] 7)ACME集中管理系统创建一个包含域名待提交到证书颁发机构CA且未带有CSR的CA订单;

[0030] 8)ACME集中管理系统返回携带订单ID以及用以域名所有权验证的ACME Authorization数据,并在此步中欺骗ACME客户端表示ACME客户端的域名已通过验证,并发送已通过验证信息,由此跳过由传统ACME客户端来自动配置完成ACME验证域名验证的过程;

[0031] 9)ACME客户端生成私钥和CSR,通过调用newNonce函数与finalizeOrder函数提交订单ID与CSR到ACME集中管理系统;

[0032] 10)ACME集中管理系统将待提交的CA订单与CSR一并提交到证书颁发机构CA获取到域名验证信息,调用验证模块进行域名验证;

[0033] 11)验证模块收到需要验证的域名和验证值,通过文件代理和DNS CNAME授权设置验证值;

[0034] 12)ACME集中管理系统调用CA证书获取API,证书颁发机构CA完成域名验证后签发并返回证书内容;

[0035] 13)ACME集中管理系统按照ACME协议方式将证书内容返回给ACME客户端,完成证书签发过程。

[0036] 所述的步骤7)中,当订单在多个ACME客户端形成竞争关系时,通过对订单加互斥锁避免多个ACME客户端同时请求同一ACME目录URL带来的冲突,并且对后续的同一请求采取挂起的方式。

[0037] 所述的步骤7)中,对于取到互斥锁的ACME客户端,ACME集中管理系统创建一个包含域名待提交到证书颁发机构CA且未带有CSR的CA订单。

[0038] 在按照步骤1)-13)完成具有竞争关系的多个ACME客户端中的ACME客户端A的证书签发过程后,对于具有竞争关系的多个ACME客户端中的ACME客户端B,通过以下步骤完成证书签发过程:

[0039] 14)ACME集中管理系统释放ACME客户端A的互斥锁后,ACME客户端B获取到互斥锁,ACME客户端B获取ACME客户端A创建的CA订单号;

[0040] 15)ACME客户端B重复步骤8)-9);

[0041] 16)ACME集中管理系统将对已提交的CA订单与CSR一并提交到证书颁发机构CA获取到域名验证信息,调用验证模块进行域名验证;

[0042] 17)重复步骤11)-13)完成ACME客户端B的证书签发过程。

[0043] 对于具有竞争关系的多个ACME客户端中的其余ACME客户端,按照步骤14)-17)依次完成证书签发过程。

[0044] 所述的步骤11)中,通过ACME客户端请求的ACME目录URL中的token获取到的订单的策略所绑定的域名验证方式进行所有权验证。

[0045] 当策略所绑定的域名验证方式为文件代理时,通过以下步骤完成域名所有权验证:

[0046] 1101)验证模块收到需要验证的域名和验证值,将域名作为Key,将验证值作为Value存储到KV存储器中;

[0047] 1102)证书颁发机构CA进行域名验证时,请求域名的HTTP或HTTPS地址,通过用户预先设置的到ACME集中管理系统的文件代理的规则,将证书颁发机构CA的域名所有权验证反向代理到验证模块并携带域名作为HTTP请求的Host头部字段;

[0048] 1103)验证模块通过获取反向代理的HTTP请求中的Host头部字段得到需要验证的域名;

[0049] 1104)验证模块通过域名在KV存储器获取到对应的验证值并通过HTTP文本返回给证书颁发机构CA。

[0050] 当策略所绑定的域名验证方式为DNS CNAME授权时，通过以下步骤完成域名所有权验证：

[0051] 1111)验证模块收到需要验证的域名和验证值，将域名作为Key，将验证值作为Value存储到KV存储器中；

[0052] 1112)证书颁发机构CA进行域名验证时，请求域名的DNS TXT记录，该域名通过用户预先在其DNS解析服务配置的DNS CNAME记录指向验证模块提供的DNS解析服务所提供的DNS CNAME代理域名；

[0053] 1113)证书颁发机构CA所请求的域名验证请求将被代理验证模块提供的DNS解析服务；

[0054] 1114)DNS解析服务获取到证书颁发机构CA所请求的DNS CNAME代理域名的DNS TXT解析请求，通过提取请求中的域名前缀的方式得到所请求的域名；

[0055] 1115)验证模块通过域名在KV存储器获取到对应的验证值并通过DNS TXT记录方式返回给证书颁发机构CA。

[0056] 与现有技术相比，本发明具有以下优点：

[0057] 一、通过本系统在ACME客户端<->本系统<->CA之间的代理，能够完成证书签发状态的统计，避免多服务器节点对同一证书的申请的验证频繁，搭配相关策略，能够有效提高证书颁发成功率。

[0058] 二、当多个ACME客户端节点同时申请证书时，通过采用先处理第一个请求，并挂起等待其他请求，直到第一个请求响应后，获得订单号，其他请求通过重颁发机制快速对此订单进行重颁发的处理方式，可以无需产生新订单，同时跳过域名验证，快速签发证书副本。

[0059] 三、本发明基于ACME协议，结合ACME卸载模块、统计模块、策略模块、验证模块和通知模块，实现了更高效的证书签发申请以及可视化的申请图表和更低的签发成本

附图说明

[0060] 图1为ACME集中管理系统的原理框图。

[0061] 图2为负载均衡的方法流程图。

具体实施方式

[0062] 下面结合附图和具体实施例对本发明进行详细说明。

[0063] 实施例

[0064] 如图1所示，本发明提供一种ACME集中管理系统及其负载均衡方法，本发明的基本流程如下：

[0065] 首先，ACME客户端发起证书申请，ACME卸载模块进行数据解析卸载，通过策略模块指定的策略开始申请证书，验证值通过验证模块快速设置，申请状态及时通过通知模块告知，最后形成了统计模块能看到的数据。

[0066] 如图2所示，本发明提供的负载均衡方法流程如下：

[0067] ACME卸载模块是整个系统的核心，它提供了token鉴权，ACME客户端API，对接各个CA系统的功能，如图1所示，所有的功能流程都是从ACME卸载模块开始的，具体流程为：

[0068] 1)用户到本系统创建ACME目录URL(参考https://tools.ietf.org/html/

rfc8555#section-7.1.1)获得如https://acme.certcloud.cn/acme/directory/TjI2c2h6cGNfaDAyeUhBVTZfMWEzMWQ3ODg3ODgwMmMzYTI2NTU5MDZ1地址,携带着与订单绑定的token,如TjI2c2h6cGNfaDAyeUhBVTZfMWEzMWQ3ODg3ODgwMmMzYTI2NTU5MDZ1;

[0069] 2)ACME客户端通过ACME目录URL获取到API列表;

[0070] 3)ACME客户端通过调用newNonce与newAccount API完成账户的注册;

[0071] 4)ACME客户端通过调用newNonce与newOrder API携带域名信息(如example.com)到本系统;

[0072] 5)本系统通过AMCE客户端请求的ACME目录URL中的token获取到对应的策略,本系统判断是否允许继续;

[0073] 6)本系统通过ACME客户端请求的ACME目录URL中的token获取到对应的订单;

[0074] 7)订单可能会在ACME客户端A和ACME客户端B形成竞争关系,通过对订单加互斥锁来解决多个ACME客户端同时请求同一ACME目录URL带来的冲突问题,对后续同一请求采取挂起方式;

[0075] 8)假设ACME客户端A获取到互斥锁,本系统将创建一个包含域名example.com待提交到CA的CA订单(没有CSR);

[0076] 9)本系统返回携带订单ID和ACME Authorization数据(用于域名所有权验证),本系统在此处欺骗ACME客户端表示该域名example.com已通过验证,跳过由传统ACME客户端来自动配置完成ACME验证域名验证的过程(在后续收到CSR后通过验证模块自动完成域名验证);

[0077] 10)ACME客户端生成私钥和CSR,通过调用newNonce与finalizeOrder提交订单ID与CSR到本系统;

[0078] 11)本系统将待提交CA订单与CSR一并提交到CA获取到域名验证信息,调用验证模块进行域名验证;

[0079] 12)验证模块收到需要验证的域名example.com和验证值,通过文件代理和DNS CNAME授权设置验证值,具体为:

[0080] 当策略所绑定的域名验证方式为文件代理时,通过以下步骤完成域名所有权验证:

[0081] 1)验证模块收到需要验证的域名和验证值,将域名作为Key,将验证值作为Value存储到KV存储器中;

[0082] 2)证书颁发机构CA进行域名验证时,请求域名的HTTP(80端口)或HTTPS(443端口)地址,例如http://example.com/.well-known/pki-validation/fileauth.txt,通过用户预先设置的到ACME集中管理系统的文件代理的规则,将证书颁发机构CA的域名所有权验证反向代理到验证模块并携带域名example.com作为HTTP请求的Host头部字段;

[0083] 3)验证模块通过获取反向代理的HTTP请求中的Host头部字段得到需要验证的域名example.com;

[0084] 4)验证模块通过域名example.com在KV存储器获取到对应的验证值并通过HTTP文本返回给证书颁发机构CA;

[0085] 当策略所绑定的域名验证方式为DNS CNAME授权时,通过以下步骤完成域名所有权验证:

[0086] 1)验证模块收到需要验证的域名和验证值,将域名作为Key,将验证值作为Value存储到KV存储器中;

[0087] 2)证书颁发机构CA进行域名验证时,请求域名的DNS TXT记录(例如:_dnsauth.example.com),该域名通过用户预先在其DNS解析服务配置的DNS CNAME记录指向验证模块提供的DNS解析服务(例如:NS为dcv.httpsauto.com)所提供的DNS CNAME代理域名(例如:example.com.dcv.httpsauto.com);

[0088] 3)证书颁发机构CA所请求的域名验证请求将被代理验证模块提供的DNS解析服务;

[0089] 4)DNS解析服务获取到证书颁发机构CA所请求的DNS CNAME代理域名example.com.dcv.httpsauto.com的DNS TXT解析请求,通过提取请求中的域名前缀的方式得到所请求的域名example.com;

[0090] 5)验证模块通过域名在KV存储器获取到对应的验证值并通过DNS TXT记录方式返回给证书颁发机构CA。

[0091] 13)本系统调用CA证书获取API,CA完成域名验证后签发并返回证书内容;

[0092] 14)本系统按照ACME协议方式将证书内容返回给ACME客户端,完成证书签发过程;

[0093] 15)本系统释放ACME客户端A的互斥锁,客户端B获取到互斥锁,客户端B将获取到客户端A创建的CA订单号;

[0094] 16)客户端B重复上述9-10;

[0095] 17)本系统将对已提交的CA订单与CSR一并提交到CA获取到域名验证信息,调用验证模块进行域名验证;

[0096] 18)重复12-14完成证书签发过程。

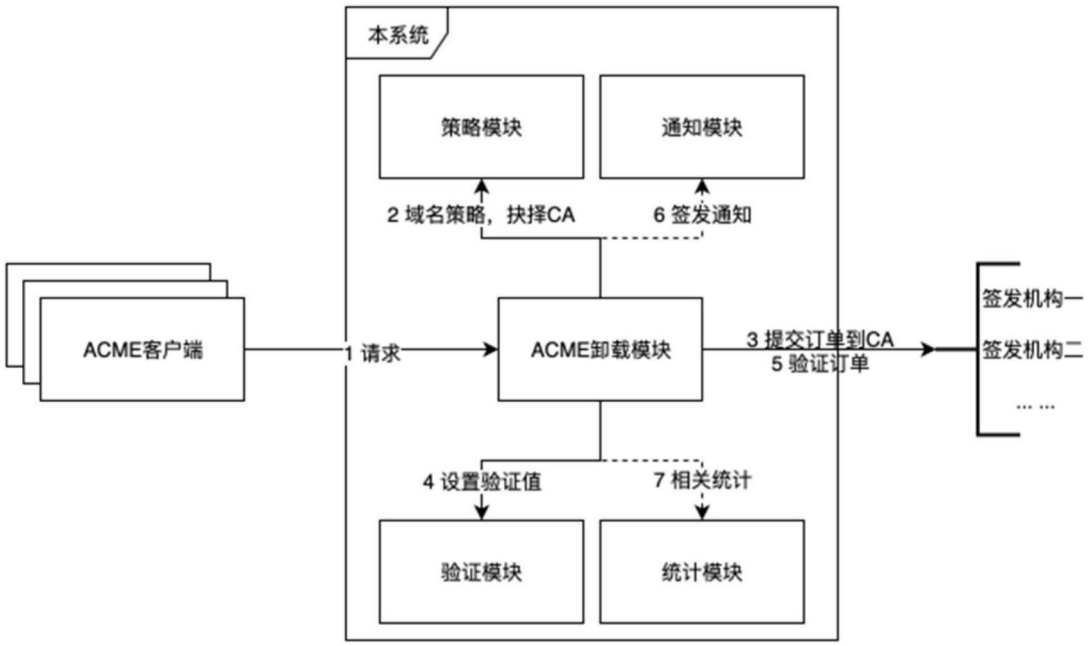

本系统
策略模块
通知模块
2 域名策略，抉择CA
6 签发通知
ACME客户端
1 请求
ACME卸载模块
3 提交订单到CA
5 验证订单
签发机构一
签发机构二
……
4 设置验证值
7 相关统计
验证模块
统计模块

图1

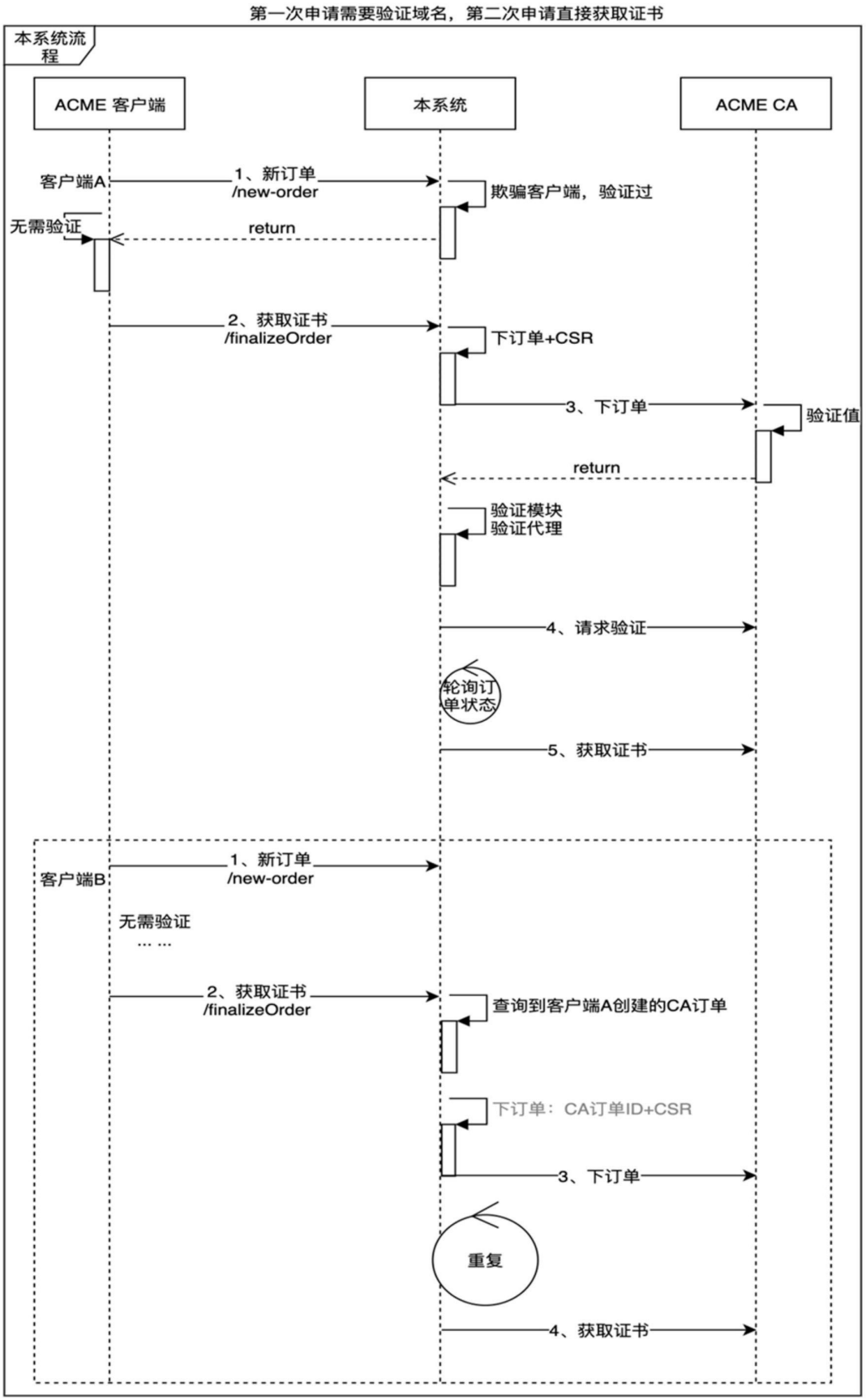

第一次申请需要验证域名，第二次申请直接获取证书
本系统流程
ACME 客户端
本系统
ACME CA
客户端A
1、新订单
/new-order
欺骗客户端，验证过
无需验证
return
2、获取证书
/finalizeOrder
下订单+CSR
3、下订单
验证值
return
验证模块
验证代理
4、请求验证
轮询订单状态
5、获取证书
客户端B
1、新订单
/new-order
无需验证
... ...
2、获取证书
/finalizeOrder
查询到客户端A创建的CA订单
下订单：CA订单ID+CSR
3、下订单
重复
4、获取证书

图2