(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114677136 A
(43)申请公布日 2022.06.28

(21)申请号 202210315106.5

(22)申请日 2022.03.29

(71)申请人 上海帝熙科技有限公司
地址 201512 上海市金山区金山卫镇秋实路688号(金山第二工业区经济小区)

(72)发明人 蓝剑波

(74)专利代理机构 江阴市权益专利代理事务所(普通合伙) 32443
专利代理师 王凯

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 30/06(2012.01)

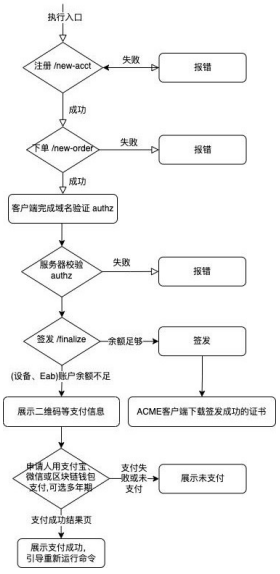
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种ACME商业证书无头模式交付方式

(57)摘要

本发明公开了一种ACME商业证书无头模式交付方式，在申请时余额不足之时，返回支付信息来让申请人执行收款;收款后，命令重新执行直接签发证书的方案，其特点是交互过程都在命令行终端或者后台静默，全程无需浏览器或其他准备工作，从而最大程度保留了ACME标准流程的体验。并且这一种ACME商业证书无头模式交付方案是无需线下、线上合同，无需浏览器预支付的商业证书的ACME分发模式，证书申请人只需执行ACME命令，即可在终端获得支付二维码等信息，完成支付后即可签发付费证书;得益于ACME的自动化优势，申请人无需填写若干个申请表单，从而简化商业证书的签发、支付以及部署流程。



CN 114677136 A

1.一种ACME商业证书无头模式交付方式,其特征在于:交付方式的具体过程为:

1)ACME客户端用new-account接口注册设备,ACME或CA服务器根据是否带有eab凭据,给设备单独余额账户或给eab凭据一个余额账户;

2)ACME客户端本地下单,服务器暂时不扣费,标记为未支付,返回订单下单成功,并返回域名验证信息;

3)ACME客户端去完成ACME服务器要求的域名验证,并触发每个域名的authz接口,让ACME服务器去检查应答挑战是否通过;

4)ACME客户端生成Private Key和CSR文件,调用finalize接口上传CSR,ACME服务器判断是否存在域名相同证书,确定是否需要再次计费,检查该账户下是否一个月内有域名一样的证书,如果有就直接用已签发的证书来重签名,不重复计费,ACME服务器扣费逻辑检查下余额是否足够,如果不足,在响应的JSON数据中返回支付二维码unicode信息或直接返回非JSON的数据(后者只有部分客户端支持,需要判断UserAgent)或区块链以太坊收款契约并引导重新运行命令;如果余额足够直接扣除费用(付款后重新执行就是走此逻辑),订单标记为已支付,再调用CA / PKI签署接口,签发证书;

5)证书签发后,让订单详情接口返回一个certificate属性,带上证书下载链接,如果还未签发、等待的时间超过3秒,直接返回状态为processing,让客户端在30秒后刷新订单状态直到返回certificate属性为止。

一种ACME商业证书无头模式交付方式

技术领域

[0001] 本发明涉及互联网通信技术,更具体地说,涉及一种ACME商用领域的交付技术。

背景技术

[0002] ACME(Automatic Certificate Management Environment,RFC8555)自动化证书管理环境,是一套用于TLS数字证书的自动化申请、验证、部署一套完整的自动化协议。根据该协议,签署证书过程,用户只需提前配置好DNS-01、HTTP-01、TLS-ALPN-01应答方式,申请签发过程客户端会自动根据ACME服务器所返回的应答要求自动完成应答挑战,无需人工解析DNS、上传文件。在CA自动检查通过后,即可签发SSL证书;然后也可以给证书设置定时作业,在到期日之前提前续签证书,从而大幅度减少人工成本。

[0003] 虽然ACME技术有自动化、快捷等优势,但很少有商用CA在零售市场采用和推广ACME技术(截止2022年之前,只有DigiCert、Sectigo、GlobalSign、BuyPass、SSL.com等少数商业CA采用了ACME,而且都需要先往CA控制台预存入金额或提前签署合同),因此ACME的自动化优势并未惠及市场大多数付费证书使用者。

[0004] 商业原因:CA也有商业方面考虑,例如ACME是Let‘s Encrypt的技术与标准,推广养成用户习惯后,容易造成合同流失。

[0005] 技术原因:ACME协议的设计本身是不支持付费服务的接入的,要实现支付目前业界基本上都是借助了Web页面来让用户主动去预支付,或者签署合同实现商业结算。

[0006] 上面的技术原因分析中,ACME协议本身设计也是计费不友好的,并且其商用可扩展性有限,几乎无法在不借助外部介质的情况下实现零售的商业化(例如提前在浏览器网页内购买付费证书额度,或者签署合同)。这样就让用户的使用成本上升了不止一点(要提前注册网页上面的账号、或者跟商务人员对接)。而ACME有此弊之因,是因发起ACME标准的CA(Let’s Encrypt)不需要考虑到付费证书的业务需求(其签发的90天证书都是公益性质的不收费):,所以付费SSL证书机构和经销商难以在不改造ACME的前提下,来实现商业化普及。具体到技术细节结合《附录一:流程说明》可以看出造成无法商业扩展的原因为:

1)ACME签发过程UI交互界面:ACME通常是在命令行甚至没有UI交互界面的情况下静默实现证书的申请和更替;而支付行为是需要返回一个完整的参数的;我们无法在没有UI交互界面的环境、在无三方介质的情况下实现费用的收取;

2)ACME客户端和服务器的交互的数据结构:ACME交互数据为JSON(严格说是application/jose+json),具体每个接口返回的各个字段的作用(包括展示形式)都是固定的,如何将服务器返回的支付信息展示出二维码供支付宝/微信/区块链钱包识别,并兼容现有客户端,是及其困难的一件事情;

目前市面上主流的ACME商用方案,均采用了Web网页界面来实现集中化管理,提前进行域名的验证,提前对用户实现额度和授权的发放,需要客户与CA或者证书售卖公司签约付款、或者提前在CA或证书售卖公司充值,才可以签发付费证书。此方案不能说不不方便,但依旧存在使用复杂、流程过多、脱离了ACME本身的意义;本发明就是为了回归ACME本

身的意义,让付款过程也能在ACME指令的执行过程之中完成,从而让用户脱离Web浏览器界面,关注单纯的证书产品交付过程,而不再打开CA或证书售卖公司的浏览器界面去关心余额是否足够等问题或合同是否该续费的问题。

发明内容

[0007] 针对现有技术中存在的相关问题,本发明的目的在于提供一种ACME商业证书无头模式交付方式,在申请时余额不足之时,返回支付信息(二维码、区块链收款地址等),来让申请人执行收款;收款后,命令重新执行直接签发证书的方案,其特点是全部交互过程都在命令行终端或者后台静默(区块链合约交易),全程无需浏览器或其他准备工作,从而最大程度保留了ACME标准流程的体验。

[0008] 本发明的目的是这样实现的:

一种ACME商业证书无头模式交付方式,交付方式的具体过程为:

1)ACME客户端用new-account接口注册设备,ACME或CA服务器根据是否带有eab凭据,给设备单独余额账户或给eab凭据一个余额账户;

2)ACME客户端本地下单,服务器暂时不扣费,标记为未支付,返回订单下单成功,并返回域名验证信息;

3)ACME客户端去完成ACME服务器要求的域名验证,并触发每个域名的authz接口,让ACME服务器去检查应答挑战是否通过;

4)ACME客户端生成Private Key和CSR文件,调用finalize接口上传CSR,ACME服务器判断是否存在域名相同证书,确定是否需要再次计费,检查该账户下是否一个月内有域名一样的证书,如果有就直接用已签发的证书来重签名,不重复计费,ACME服务器扣费逻辑检查下余额是否足够,如果不足,在响应的JSON数据中返回支付二维码unicode信息或直接返回非JSON的数据(后者只有部分客户端支持,需要判断UserAgent)或区块链以太坊收款契约并引导重新运行命令;如果余额足够直接扣除费用(付款后重新执行就是走此逻辑),订单标记为已支付,再调用CA / PKI签署接口,签发证书。

[0009] 5)证书签发后,让订单详情接口返回一个certificate属性,带上证书下载链接,如果还未签发、等待的时间超过3秒,直接返回状态为processing,让客户端在30秒后刷新订单状态直到返回certificate属性为止。

[0010] 相比于现有技术,本发明的优点在于:

这一种ACME商业证书无头模式交付方案,在申请时余额不足之时,返回支付信息(二维码、区块链收款地址等),来让申请人执行收款;收款后,命令重新执行直接签发证书的方案,其特点是全部交互过程都在命令行终端或者后台静默(区块链合约交易),全程无需浏览器或其他准备工作,从而最大程度保留了ACME标准流程的体验。

[0011] 并且这一种ACME商业证书无头模式交付方案是无需线下、线上合同,无需浏览器预支付的商业(收费)证书的ACME分发模式,证书申请人只需执行ACME命令,即可在终端获得支付二维码(或区块链支付地址、金额)等信息,完成支付后即可签发付费证书;得益于ACME的自动化优势,申请人无需填写若干个申请表单,从而简化商业证书的签发、支付以及部署流程。

附图说明

[0012] 图1为本发明一种ACME商业证书无头模式交付方式的流程图。

具体实施方式

[0013] 本发明涉及一种ACME商业证书无头模式交付方式，本发明是为了补齐RFC8555协议不支持原生商用这个短板。

[0014] ACME标准请求和响应格式：根据RFC8555之定义，ACME的请求与响应格式均为application/jose+json格式，其作为json结构的进一步约束版本，所有的响应与请求参数都有严格的类型要求，ACME服务器扩展的任何非RFC8555标准字段，均无法被客户端所理解，不论是展示或者去请求所返回的字段。

[0015] 但是一部分ACME客户端，在处理异常之时，会将消息字段或者完整的响应body进行原始输出。这样就给了操作空间来扩展交互界面，例如想展示非application/jose+json数据给客户端，甚至数据经过特殊unicode处理(用unicode字符拼出一张二维码)，在客户端实现二维码的展示也是可行的。

[0016] 本发明的具体过程为：

1)ACME客户端用new-account接口注册设备，ACME或CA服务器根据是否带有external account binding凭据(后简称eab凭据)，决定是否直接给设备单独余额账户或考虑到多设备给eab凭据一个余额账户。

[0017] 2)ACME客户端本地按照申请人给定的-d参数(域名)下单，服务器暂时不扣费，标记为未支付，返回订单下单成功，并返回域名验证信息。

[0018] 3)ACME客户端按照申请人给定的挑战应答方式去完成ACME服务器要求的域名验证(Domain Challenge)，并触发每个域名的authz接口，让ACME服务器去检查应答挑战是否通过。

[0019] 4)ACME客户端生成Private Key和Certificate Signing Request(后简称CSR)文件，调用finalize接口上传CSR，ACME服务器需要判断是否存在域名相同证书，来确定是否需要再次计费，检查该账户(根据第1步中的逻辑，账户可能是设备也可能是eab)下是否一个月内有域名一样的证书，如果有就直接用已签发的证书来重签名，不重复计费，ACME服务器扣费逻辑检查下余额是否足够，如果不足，返回支付二维码unicode或区块链收款信息并引导支付后重新运行命令；如果足够，扣除费用，订单标记为已支付，再调用CAPKI签署接口，签发证书，如果需要等待的时间过于旧(超过3秒)，考虑的客户端CURL库可能有默认超时问题，需要直接返回状态为processing，并返回retry-after:30头信息，让客户端在30秒后刷新订单状态。

[0020] 5)证书签发后，让订单详情接口返回一个certificate属性，带上证书下载链接。

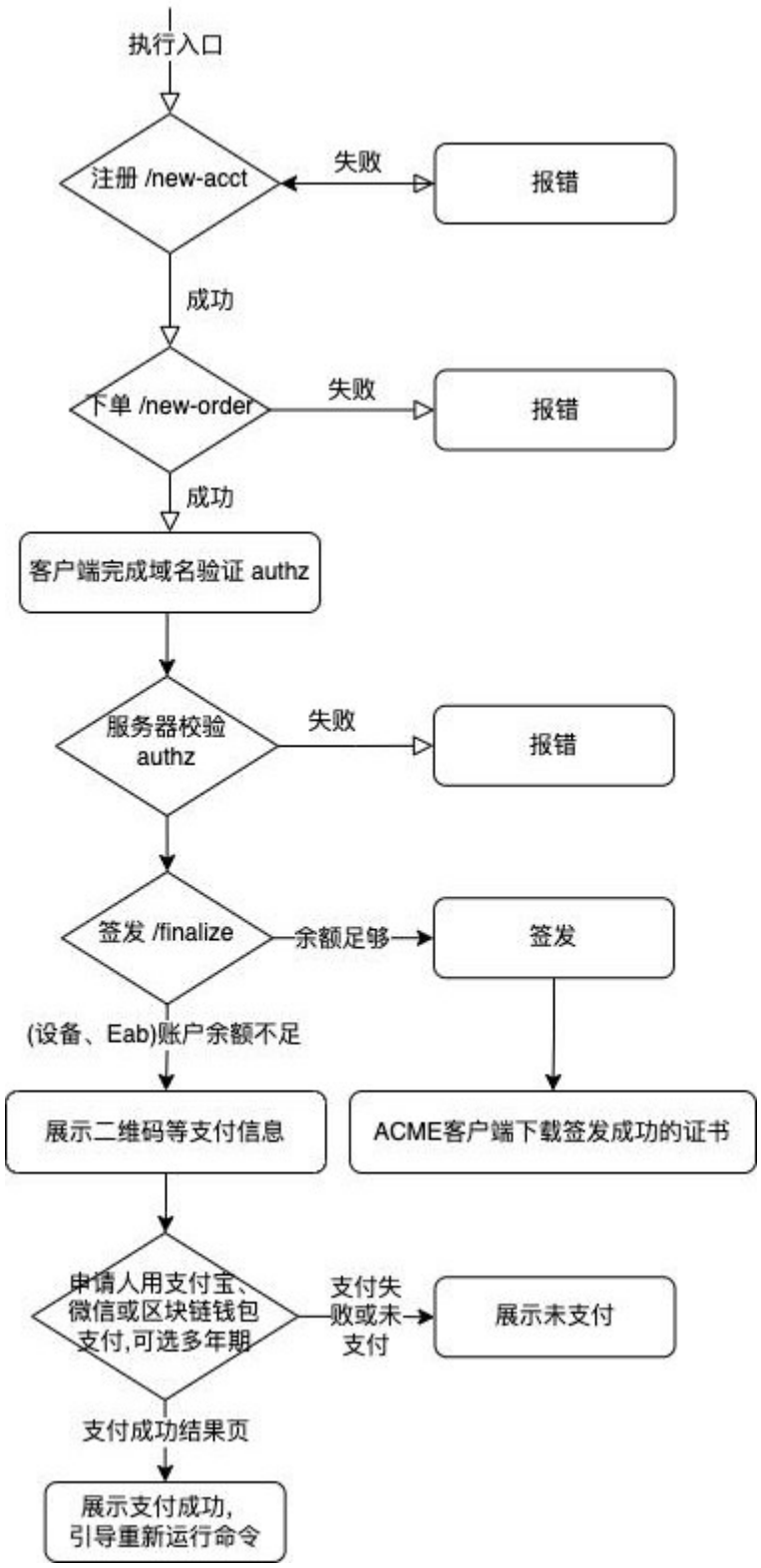

执行入口
注册 /new-acct
失败
报错
成功
下单 /new-order
失败
报错
成功
客户端完成域名验证 authz
服务器校验 authz
失败
报错
签发 /finalize
余额足够
签发
(设备、Eab)账户余额不足
展示二维码等支付信息
ACME客户端下载签发成功的证书
申请人用支付宝、微信或区块链钱包支付,可选多年期
支付失败或未支付
展示未支付
支付成功结果页
展示支付成功,引导重新运行命令

图1