

自动化证书管理国际标准和前沿研究综述

李龙鑫^{1,2}, 闫峥², 王海光³, 李铁岩³

(1. 西安电子科技大学广州研究院, 广东 广州 510555; 2. 西安电子科技大学网络与信息安全学院, 陕西 西安 710126;
3. 华为技术有限公司可信技术实验室谢尔德实验室, 新加坡 486035)

摘要: 随着全球数字化浪潮的推进, 全球网民数量和互联网服务访问量激增。与此同时, 钓鱼邮件、网络窃听和身份伪造等网络攻击行为也日益增多, 严重威胁互联网的生态安全。为解决这一问题, 公钥基础设施被广泛用于构建互联网通信双方之间的信任关系。近年来, 随着公钥证书需求量的激增, 证书管理效率低成为核心瓶颈。自动证书管理技术的出现, 标志着公钥基础设施进入一个新的发展阶段, 提升了公钥证书管理的效率, 推动了互联网安全加密通信的普及。然而, 目前尚未有综述对自动化证书管理相关研究进行系统性讨论和总结。为此, 围绕自动化证书管理环境(ACME)技术的发展情况展开全面调研, 对自动化证书管理技术的相关国际标准和学术研究等文献(涵盖2019年至今的相关标准和学术研究等文献)进行了梳理, 呈现了自动化证书管理技术的发展时间线, 并对现有文献进行了分类和归纳。此外, 提出了一套针对自动化证书管理研究的评价体系, 涵盖功能性、安全性、可用性和性能4个维度。基于这一评价体系, 对相关研究工作进行了分析与对比。最后, 探讨了现有自动化证书管理技术的主要问题和未来的研究方向。

关键词: 自动化证书管理; 公钥基础设施; 国际标准; 加密通信

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.AQ24264

Overview of international standards and cutting-edge research on automated certificate management

Li Longxin^{1,2}, Yan Zheng², Wang Haiguang³, Li Tieyan³

1. Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, China
2. School of Cyber Engineering, Xidian University, Xi'an 710126, China
3. Shield Lab, Trustworthiness Lab, Huawei Technologies Co., Ltd., Singapore 486035, Singapore

Abstract: With the advancement of global digitalization, there has been a significant increase in the number of internet users and internet service traffic worldwide. Concurrently, cyber-attack behaviors such as phishing emails, network eavesdropping, and identity forgery have become more prevalent, posing severe threats to Internet security. To address this issue, public key infrastructure is widely used to establish a trust relationship between the two parties of internet communication. In recent years, with the surge in the demand for public key certificates, the efficiency of certificate management has become a core bottleneck. The emergence of automatic certificate management technology marks the entry of public key infrastructure into a new stage of development, improving the efficiency of public key certificate management and promoting the popularization of secure encrypted communication on the internet. However, there is currently no comprehensive review that systematically discusses and summarizes

收稿日期: 2025-10-26; 修回日期: 2026-02-26

通信作者: 闫峥, zyan@xidian.edu.cn

基金项目: 国家自然科学基金资助项目 (No.U23A20300, No. 62072351)

Foundation Items: The National Natural Science Foundation of China (No.U23A20300, No.62072351)

the research related to automatic certificate management. Therefore, a comprehensive investigation was conducted on the development of ACME technology, and the relevant international standards and academic research on automatic certificate management technologies (covering relevant standards and academic research from 2019 to the present) were sorted out. The development timeline of automatic certificate management technology was presented, and the existing literature was classified and summarized. In addition, a set of evaluation system for automatic certificate management research was proposed, covering four dimensions: functionality, security, usability, and performance. Based on this evaluation system, the related research work was analyzed and compared. Finally, the main problems of the existing automatic certificate management technologies and future research directions were discussed.

Key words: automated certificate management, public key infrastructure, international standards, encrypted communication

0 引言

随着互联网的快速普及与全球数字化转型的深入,网民与数字资源规模持续快速增长,各类门户网站大量涌现,提供了涵盖网上购物、网上银行、网上投票等多元化服务,显著提升了用户体验与业务效率。然而,网络犯罪活动也随之滋生,攻击者通过窃听、中间人攻击、身份伪造、钓鱼邮件和钓鱼网站等手段非法牟利,严重破坏了互联网生态环境,给用户与企业带来了巨大的经济损失。

为保障通信信道的安全性及机密性,传输层安全(transport layer security, TLS)协议被引入超文本传输协议(HTTP)中,形成了超文本传输安全协议(HTTPS)。HTTPS通过双方协商共享密钥,并采用对称加密算法对通信流量进行加密,从而确保传输内容的机密性。共享密钥的建立依赖于通信双方的身份认证与信任机制,该机制主要由公钥基础设施(public key infrastructure, PKI)体系支持。该体系中,证书颁发机构(certificate authority, CA)通过签发安全套接层协议(SSL)证书为服务提供方提供身份背书,以便用户验证服务提供方的真实性。尽管已有证书管理协议旨在规范证书签发流程,但在实际管理中仍涉及大量人工操作,流程复杂且易因人为失误或配置错误而导致证书获取失败。因此,HTTPS虽推出已久,但普及进程在很长一段时间内较缓慢^[1]。

随着互联网的快速发展,用户对SSL/TLS证书的需求急剧增长,传统人工管理方式已难以适应现实需求。在此背景下,自动化证书管理环境(automated certificate management environment,

ACME)协议应运而生,旨在通过自动化流程简化证书的颁发与管理,提升效率与可靠性。

自ACME协议面世以来,相关国际标准陆续发布与迭代,推动了ACME技术的持续发展。然而,目前尚缺乏对ACME技术发展脉络的系统性梳理与研究。为填补这一空白,本文围绕ACME技术的发展情况展开全面调研,收集并回顾了互联网工程任务组(internet engineering task force, IETF)、第三代合作伙伴计划(third generation partnership project, 3GPP)和国际电信联盟(international telecommunication union, ITU)等组织发布的标准与报告,以及学术界的ACME相关研究论文。在此基础上,本文梳理了ACME技术的发展时间线,按文献类型对相关研究进行了分类,并提出了一套针对ACME技术的评价体系,对现有研究进行了总结与对比分析。最后,本文指出了现有研究的不足,并展望了未来的研究方向。

本文的主要贡献如下。

1) 对ACME技术发展进行较为全面的调研,系统回顾了自该技术面世以来的相关国际标准与学术研究。

2) 提出了一套ACME技术评价体系,总结了现有研究的关注点与不足,并对相关研究进行了对比分析。

3) 揭示了现有ACME研究存在的问题,展望了ACME技术未来的发展方向。

1 背景知识

1.1 公钥基础设施

PKI是一套用于实现互联网参与方之间身份互认和信任建立的技术体系,主要负责密钥与证

书的管理^[2]。PKI技术支持用户之间进行加密通信,保障数据的完整性和机密性,并完成通信双方的身份验证。随着电子商务、网上银行和电子政务等应用的广泛普及,PKI在信息安全保障中的作用日益凸显。

PKI的起源可以追溯至20世纪70年代,其伴随着数字签名技术及非对称加密算法的发展而兴起。1978年,Kohnfelder^[3]首次提出证书的概念。1988年发布的ITU-T X.509证书^[4]历经演进,已发展至X.509v3版本。20世纪90年代末至21世纪初,随着互联网的发展与电子商务的兴起,PKI被广泛应用于电子商务领域。1995年,IETF成立了PKIX工作组,致力于将X.509标准化并应用于互联网环境中。近年来,伴随着移动通信设备的普及和云计算技术的发展,PKI技术也在持续演进以适应新的应用需求。

典型的PKI系统架构和工作流程如图1所示。该系统主要由CA、注册机构(registration authority, RA)、证书库、密钥对、终端实体、证书撤销列表(certification revocation list, CRL)或在线证书状态协议(online certificate status protocol, OCSP),以及证书透明度(certification transparency, CT)日志组成。其中,CA负责签发、管理和撤销数字证书,为每个用户的公钥签发证书,并确保这些证书的有效性。RA负责验证用户的个人信息,确保只有合法用户能够从CA处获取证书;在部分实现中,RA与CA由同一机构承担。证书库是存储和发布证书信息的地方,通常是一个公开可访问的数据库或目录服务器。每个用户都拥有一对密钥,其中包含用户持有的私钥和包含在证书中公开分发的公钥。终端实体是指使用数字证书保护通信的个人或设备。CRL或OCSP用于检测证书是否已被撤销。CT日志是一种不可篡改的日志系统,记录所有证书签发信息,以支持公开审计和透明监管。

典型的PKI工作流程涵盖证书请求、签发、存储、撤销和验证等环节。用户首先通过RA提交证书申请,RA完成身份核验后转交CA;CA签发证书,并将证书信息存储在证书库中,供其他用户查询和下载。在证书验证过程中,可以通过CRL或OCSP检查证书的撤销状态。此外,

CT日志为证书签发过程提供了公开审计能力,增强了整个体系的透明性与可追溯性。

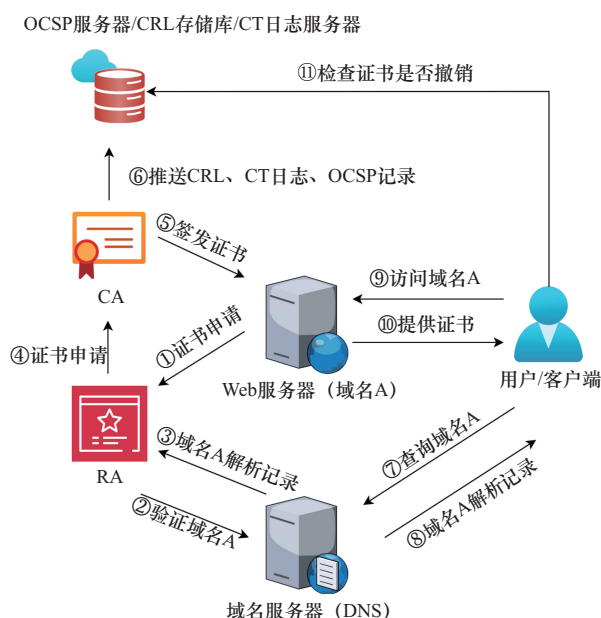


图1 PKI系统架构和工作流程

1.2 传输层安全协议

TLS协议是当前互联网中应用非常广泛的加密协议,主要用于在通信过程中提供隐私保护和数据完整性保障,其典型的应用就是HTTPS。事实上,TLS协议已成为网站安全的标准之一,目前绝大多数的网站与服务启用了该协议,以保障用户数据在传输过程中的安全性和通信的机密性。

TLS协议于1999年由IETF提出,旨在替代此前存在安全漏洞的SSL协议。TLS协议历经多次版本迭代,目前最新版本为TLS 1.3,对应的标准文档为RFC 8446。这些更新不断增强了TLS的安全性及传输性能,使其成为当今互联网中最主流的加密协议之一。

TLS协议主要包含握手协议与记录协议两部分。其中,握手协议与PKI系统紧密关联,服务器与客户端的身份认证均依赖于PKI体系。握手过程如下:客户端首先向服务器发送一个内含支持的TLS版本、加密套件等信息的Hello消息;服务器收到消息后回复一个内含选定的加密套件和其他参数的Hello消息。随后,双方进行证书交换和身份认证,并基于交换的信息生成会话密钥。在该过程中,服务器的身份认证使用X.509

标准证书,并依托PKI体系进行证书有效性验证。一旦证书验证通过,双方将基于交换的信息生成一个共享会话密钥,握手过程结束,随后所有数据均通过该加密通道进行传输。

正是由于TLS握手协议依赖PKI体系,而现代网页系统中广泛应用的HTTPS构建在TLS之上,因此现代网页系统的安全性高度依赖于PKI证书管理体系。通过PKI体系,TLS协议能够实现服务器与客户端的双向身份认证与安全通信,从而保障整个网页系统的安全性。

2 ACME 发展情况和文献分类

本节将对ACME技术的发展情况进行梳理,描绘其演进时间线,并对相关研究进行分类与分布分析,以把握该技术的发展状况。

2.1 ACME 技术发展概况

基于对ACME相关研究文献的调研,本文绘制了如图2所示的ACME技术发展时间线(截至2024年年底,后文对相关文献的分析均基于本时间线)。

2016年,IETF与电子前沿基金会共同启动

了ACME-v1协议^[5]的开发。该协议旨在标准化证书管理流程,支持客户端与CA自动交互,实现证书的申请、续期与撤销。

2019年,Aas等^[5]对Let's Encrypt项目进行工作总结。同年,IETF通过了两项ACME相关国际标准,其中的RFC 8555标志着ACME协议标准化的开端,RFC 8657则规范了认证机构授权(certification authority authorization, CAA)DNS记录的格式,以支持ACME的自动化验证。

2020年,IETF相继发布了RFC 8737、RFC 8738与RFC 8739标准,拓展了ACME协议的适用场景。与此同时,Kfoury等^[6]在学术界提出了去中心化ACME协议的研究构想。

2021年,IETF通过了RFC 8823与RFC 9115两项标准,将ACME引入内容分发网络(content delivery network, CDN)及电子邮件系统。同年,Mueller等^[7]也实现了适用于电子邮件场景的ACME方案。

2022年,基于区块链的域名控制验证(B-DCV)^[8]在Kfoury等^[6]的工作基础上进行了改进。Sujatanagarjuna等^[9]致力于提高ACME撤销

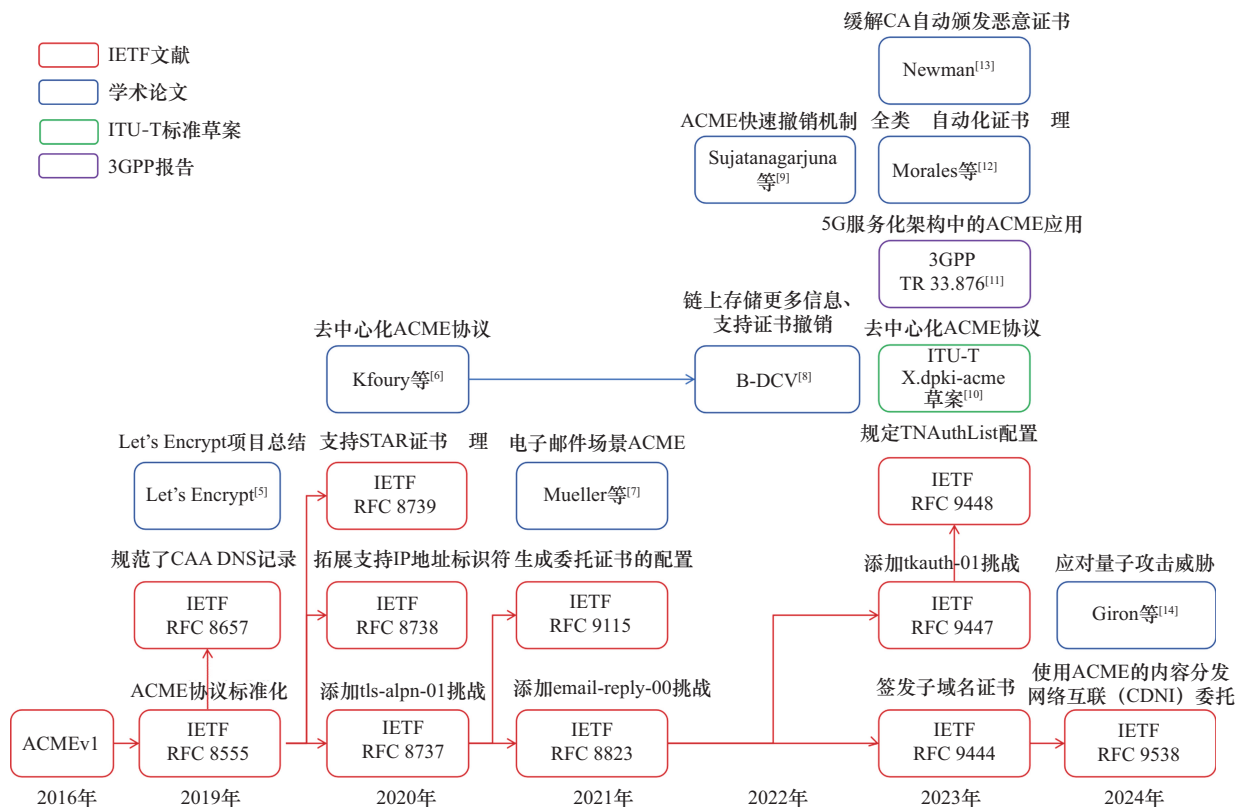


图2 ACME技术发展时间线

机制的效率。

2023年, IETF再度通过3项ACME相关标准, 即RFC 9444、RFC 9447和RFC 9448, 通过添加新的验证方式增强了协议能力。同年, ITU-T提出了关注去中心化PKI环境下ACME应用的草案“ITU-T X.dpkgi-acme”^[10]; 3GPP发布技术报告TR 33.876^[11], 该报告聚焦于5G服务化架构中的ACME应用; Morales等^[12]推动了各类验证强度证书的自动化颁发; Newman^[13]针对CA自动化签发过程中可能出现的恶意证书问题提出了缓解方案。

2024年, IETF持续更新ACME技术标准, 吸纳了RFC 9538。同时, Giron等^[14]增强了ACME协议的安全性以应对量子攻击威胁。

2.2 ACME 相关研究分类

本次调研共收集了21份相关文献, 涵盖11份IETF标准、1份3GPP报告、1份ITU-T标准草案和8篇学术论文。

根据ACME技术的发展脉络, 本文将文献划分为5类, 即基础ACME协议、ACME安全增强、标识符与应用场景扩展、短期证书管理和去中心化ACME方案。ACME研究分类如图3所示。

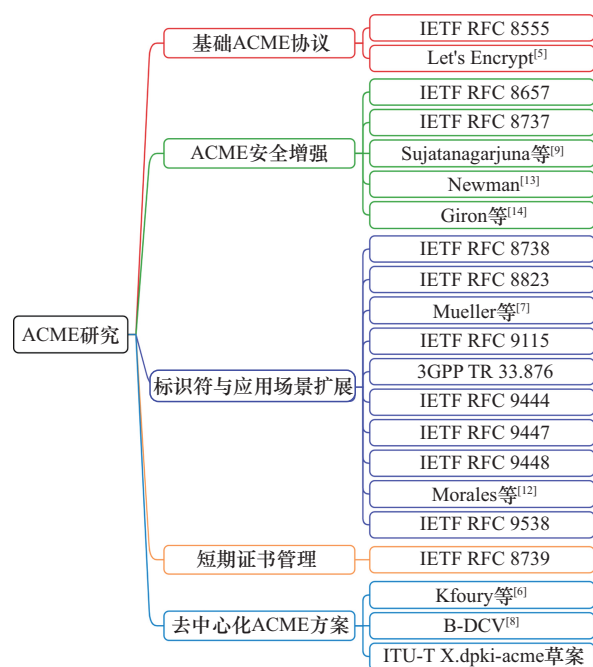


图3 ACME 研究分类(2019年至2024年)

从文献数量来看, ACME技术的发展与标准制定工作主要由IETF主导推进。同时, ITU与

3GPP也开始关注ACME协议, 正在推进相关研究与标准草案的制定工作。

除基础协议研究外, 文献整体分布表明, 当前ACME的研究和标准工作主要集中在标识符与应用场景扩展方面, 旨在不断拓展ACME的适用范围与生态系统。其次是ACME安全增强研究, 主要通过改进安全配置、引入新安全机制及采用更强密码算法等手段, 提升协议的安全性。其余研究聚焦于短期证书管理与去中心化ACME架构, 但相关文献数量相对较少。

3 评价指标

为更好地对比和评估ACME相关标准和研究, 本文建立了一套评价体系, 主要包括功能性、安全性、可用性和性能4个维度, 如图4所示。

3.1 功能性指标

功能性指标包括证书申请、证书更新、证书撤销和证书验证。

(1) 证书申请

证书申请是指对外开放有效域名证书获取的通道, 确保证书申请者能够成功获得并使用域名证书。若方案提供证书申请渠道, 则符合该项指标。

(2) 证书更新

证书更新是指替换即将过期的域名证书, 确保域名证书持续有效。若方案能够有效使用新的合法域名证书替换旧的证书, 则符合该项指标。

(3) 证书撤销

证书撤销是指在域名证书到期前主动宣布证书无效, 以应对证书私钥泄露和证书误用等问题。若方案具有转换有效证书为无效证书的机制, 则符合该项指标。

(4) 证书验证

证书验证是指验证域名证书的有效性, 确保通信双方身份的真实性。若方案提供有效的机制检验域名证书是否有效, 则符合该项指标。

在量化分析时, ACME相关研究每满足一个功能性指标即可获得1分, 最终取所有指标得分的平均值作为该维度的评估结果。

3.2 安全性指标

安全性指标包括CA单点故障、证书透明度、

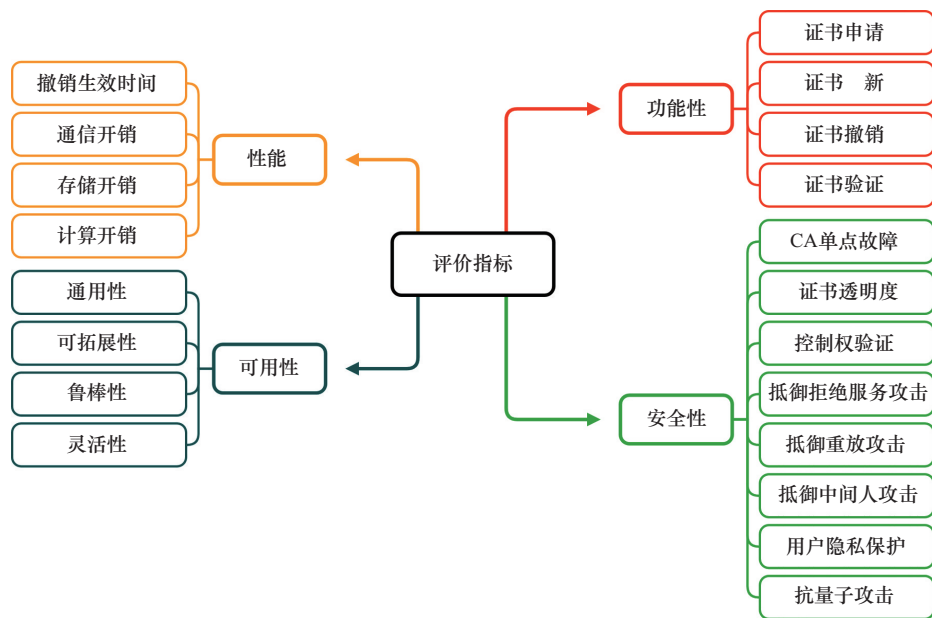


图4 评价指标

控制权验证、抵御拒绝服务攻击、抵御重放攻击、抵御中间人攻击、用户隐私保护和抗量子攻击。

（1）CA 单点故障

CA 单点故障是指单个 CA 签发恶意的公钥证书或中断正常的证书管理服务所引发的风险。若方案能够缓解或避免 CA 单点故障，则满足该项指标。

（2）证书透明度

RFC 9162 对证书透明度进行了规定。证书透明度是指通过公开的日志记录机制，允许公众查看和验证证书，以增强 PKI 的可信性。若方案设计了可公开查询的日志记录，则满足该项指标。

（3）控制权验证

通过控制权验证，可以确保只有合法域名所有者才能获得证书，从而提高系统的整体安全性和可信度。若方案支持控制权验证机制，则满足该项指标。

（4）抵御拒绝服务攻击

攻击者可能向 CA 发送大量的恶意请求试图使 PKI 服务能力瘫痪。若方案部署措施缓解或防御拒绝服务攻击，则满足该项指标。

（5）抵御重放攻击

重放攻击是指攻击者通过截取和重复发送有效通信消息造成相关逻辑二次触发，从而实现网

络欺诈。若方案采取防御措施抵御重放攻击，则满足该项指标。

（6）抵御中间人攻击

中间人攻击是指攻击者在通信双方不知情的情况下，介入双方的通信链路对通信内容进行监听、篡改或伪造。若方案部署了中间人攻击防护措施，则满足该项指标。

（7）用户隐私保护

用户隐私越来越受到用户的重视和法律法规的保护，因此需要考察方案是否考虑了用户隐私保护（例如，对用户的 CA 账户的统一资源定位器（URL）、个人或主体敏感信息等进行保护）。若方案采取了用户隐私保护措施，则满足该项指标。

（8）抗量子攻击

随着量子计算机的出现，传统密码学体系面临挑战。因此，ACME 协议和公钥基础设施是否具备抵御量子攻击的能力将成为后量子时代的重要考量指标。若方案具备抵御量子攻击的能力，则满足该项指标。

在量化分析时，ACME 相关研究每满足一个安全性指标即可获得 1 分，最终取所有指标得分的平均值，作为该维度的评估结果。

3.3 可用性指标

可用性指标包括通用性、可扩展性、鲁棒性

和灵活性。

(1) 通用性

通用性是指所提技术方案是否适用于各类应用场景，具备全场景通用能力。若方案能够适用于不同应用场景，则满足该项指标。

(2) 可扩展性

可扩展性表明系统面对增长的工作负载，能够保持性能和效率。若方案能够有效拓展以应对更大负载，则满足该项指标。

(3) 鲁棒性

鲁棒性是指证书管理方案能够在各种场景下保持稳定可靠运行。例如，在证书管理账户正常运作时能够有效进行证书管理，而在证书管理账户丢失的情况下，仍然能够完成必要的证书管理工作。若方案能够在管理账户正常和丢失情况下都支持证书管理，则满足该项指标。

(4) 灵活性

灵活性是指证书管理方案能够灵活实现不同类型和级别的证书管理。从标识符数量来看，证书类型包括单域名证书和多域名证书；依据验证强度，可进一步分为域验证（domain validated, DV）证书、组织验证（organization validated, OV）证书和扩展验证（extended validation, EV）证书。如果方案能够满足所有常见类型的证书管理，则被认为完全符合要求。若方案仅能覆盖不同标识符数量的证书管理，或者仅能处理不同验证强度级别的证书管理，则被认为部分符合要求。否则，方案将被认为不符合要求。

在量化分析时，ACME 相关研究在通用性、可扩展性和鲁棒性等指标上，每满足一项指标即计1分。在灵活性指标方面，完全满足计1分，部分满足计0.5分，不满足计0分。最终取各项指标得分的平均值，作为该维度的评估结果。

3.4 性能指标

性能指标包括撤销生效时间、通信开销、存储开销和计算开销。

(1) 撤销生效时间

撤销生效时间是指从证书撤销请求发出到撤销信息正式生效所需的时间，该时间越短，表明证书撤销的实时性越强。过长的撤销生效时间会削弱数字证书的可信度^[15]。因此，在 ACME 协

议的研究中，应充分考虑如何优化撤销生效时间。

(2) 通信开销

通信开销是指在网络传输过程中传输数据所消耗的带宽资源。其是评估协议系统性能的常用指标之一，能够反映协议的通信效率及其对设备能耗的影响^[16-17]。若不考虑通信开销，则可能导致 ACME 协议无法应用于资源受限环境（如物联网和无线传感网络）。

(3) 存储开销

存储开销是指在管理和维护数字证书过程中所占用的存储资源。占用存储资源的数据主要包括证书透明度日志、证书文件和证书撤销列表。主流 CA Let's Encrypt 披露，其每日签发的证书超过 400 万份，存储半年内产生的 CT 日志至少需要 5 TB。统计分析显示，当前全球主流网站使用的数字证书文件平均大小约为 2 KB。本文将在上述数据的基础上，对自动化证书管理过程中的存储开销进行理论分析。

(4) 计算开销

计算开销是指与证书申请、更新、撤销和验证等操作相关的资源消耗。根据这些操作的时间开销可以衡量计算开销。如果不考虑计算开销，那么高计算开销的 ACME 协议方案可能会增加系统的响应时间，难以应对大规模的证书请求，从而影响协议执行效率。

在量化分析时，将撤销生效时间以 1 d 作为评估基准。撤销生效时间为 1 d，得 0.5 分；撤销生效时间小于 1 d，得 1 分；撤销生效时间大于 1 d，得 0 分。该设定依据当前主流 CA 普遍采用的撤销生效时间标准。对于通信开销、存储开销和计算开销，均以基础 ACME 协议的性能为参照。性能优于基础 ACME 协议，得 1 分；性能弱于基础协议，得 0 分。最终，取所有相关指标得分的平均值作为该维度的评估结果。

4 ACME 文献综述

本节对现有 ACME 技术文献进行系统回顾，并基于前文提出的评价体系对相关文献展开对比分析。表 1 汇总了现有文献的主要关注点及其存在的不足，进一步，从 4 个评价维度对现有文献进行了对比，结果见表 2。此外，为直观展示不同研究

表 1 ACME 研究汇总

ACME 研究	状态	关注点	不足
IETF RFC 8555	国际标准	ACMEv2 协议	存在 CA 单点故障风险, 撤销机制效率低
IETF RFC 8657	国际标准	ACME 的 CAA DNS 记录配置	泄露用户账户 URI
IETF RFC 8737	国际标准	新挑战方法 tls-alpn-01	要求设备支持应用层协议协商 (ALPN) 扩展
IETF RFC 8738	国际标准	支持验证 IP 地址标识符	存在 CA 单点故障风险
IETF RFC 8739	国际标准	支持 STAR X.509 证书管理	缺少证书撤销机制
IETF RFC 8823	国际标准	新挑战方法 email-reply-00 以支持安全/多用途互联网邮件扩展 (S/MIME) 证书	存在 CA 单点故障风险, 专用于邮件系统
IETF RFC 9115	国际标准	生成委托证书所需 ACME 配置文件	存在 CA 单点故障风险, 存在流氓 CDN 任意申请恶意证书风险
IETF RFC 9444	国际标准	为子域名获取 CA 签名的证书	利用主域名签发恶意子域名证书
IETF RFC 9447	国际标准	权威令牌挑战机制 tkauth-01, 验证非互联网资源	存在 CA 单点故障风险, 令牌机构单点故障
IETF RFC 9448	国际标准	ACME 权威令牌的 TNAuthList 配置	存在 CA 单点故障风险, 专用于安全电话身份 (STI) 证书
IETF RFC 9538	国际标准	使用 ACME 的内容分发网络互联 (CDNI) 委托	存在 CA 单点故障风险, 专用于 CDNI 场景
ITU-T X.dpki-acme ^[10]	草案	基于区块链的自动化 X.509 域名证书管理的框架和方法	去中心化 ACME 协议部分缺失
3GPP TR 33.876 ^[11]	技术报告	5G 服务化架构中的自动化证书管理应用	存在 CA 单点故障风险, 专用于电信网络
Let's Encrypt ^[5]	学术论文	第一个实现自动化证书管理的 CA	存在 CA 单点故障风险, 仅支持域名证书管理
Kfoury 等 ^[6]	学术论文	去中心化 ACME 协议	证书管理账户丢失后无法操作, 仅支持单域名证书管理, 链上存储消耗大, 不支持证书撤销
Mueller 等 ^[7]	学术论文	实现 S/MIME 证书和密钥自动化管理	存在 CA 单点故障风险, 专用于邮件系统
B-DCV ^[8]	学术论文	去中心化域名控制验证实现	证书管理账户丢失后无法操作, 仅支持单域名证书管理, 链上存储消耗大
Sujatanagarjuna 等 ^[9]	学术论文	提高 ACME 协议中的证书撤销效率	存在 CA 单点故障风险, 比特币钱包丢失后无法撤销
ACMEH ^[12]	学术论文	增强 ACME 以支持 DV、OV 和 EV 类型证书管理	存在 CA 单点故障风险, 可验证凭证颁发机构单点故障
Newman ^[13]	学术论文	缓解 CA 自动颁发恶意证书	存在 CA 和 OIDC 令牌颁发者合谋和单点故障风险
Giron 等 ^[14]	学术论文	应对量子计算机对 ACME 协议中传统密码算法的威胁	存在 CA 单点故障风险, 量子密码的性能开销大, 量子密码证书存储开销大

之间的差异, 本节开展了量化对比分析, 结果如图 5 所示。

4.1 基础 ACME 协议

2019 年 3 月 12 日, ACMEv2 协议标准 RFC 8555 发布, 该标准极大地简化了 SSL 证书的管理流程, 促进了 HTTPS 的普及。RFC 8555 规范了 ACME 客户端与服务端之间的交互流程, 实现了从证书申请、域控制权验证、证书签发到部署的全自动化流程, 如图 6 所示。用户仅需在 Web 服务器上使用 ACME 客户端软件即可完成 SSL 证书的自动化申请与部署。该标准支持 DNS-01、

HTTP-01 及 TLS-SNI-01 共 3 种验证方法。DNS-01 通过向 DNS 记录中添加文本 (TXT) 记录验证所有权; HTTP-01 通过向指定 URL 发送 HTTP 请求验证所有权; TLS-SNI-01 则通过配置 SSL 证书并在服务器上提供正确的主题备用名称 (subject alternative name, SAN) 字段来验证所有权。RFC 8555 还提供了证书续期和撤销接口, 支持通过定时任务实现证书自动续期, 提升了证书生命周期的管理效率。在安全性方面, ACME 协议采用 HTTPS 传输协议消息, 并使用 JSON Web 签名 (JSON Web signatures, JWS) 进行消息签名与验

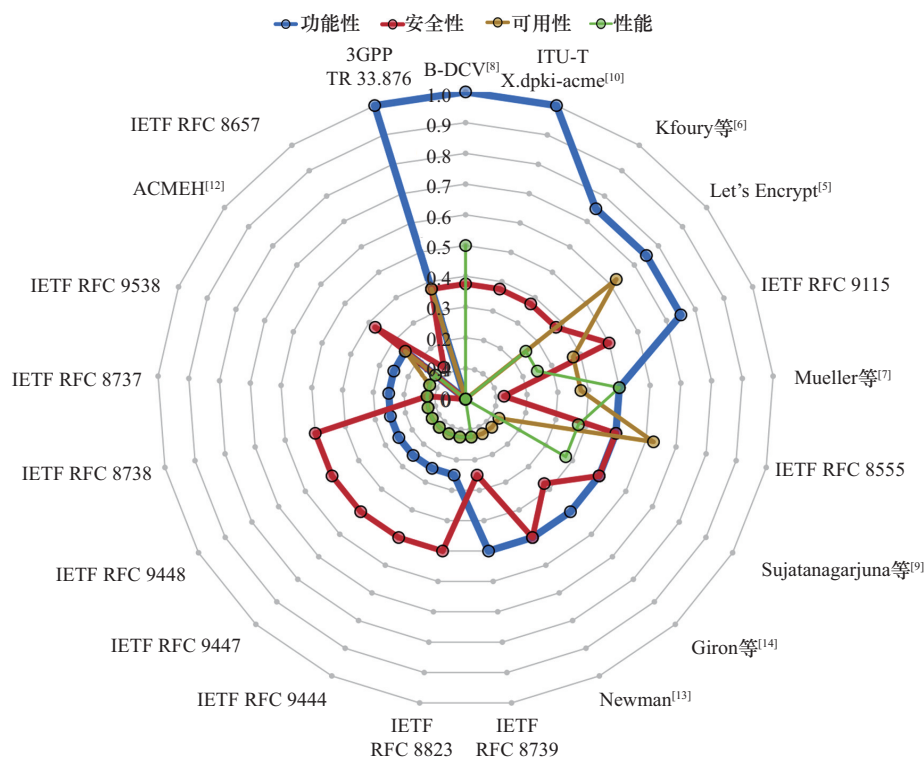


图5 ACME研究量化对比

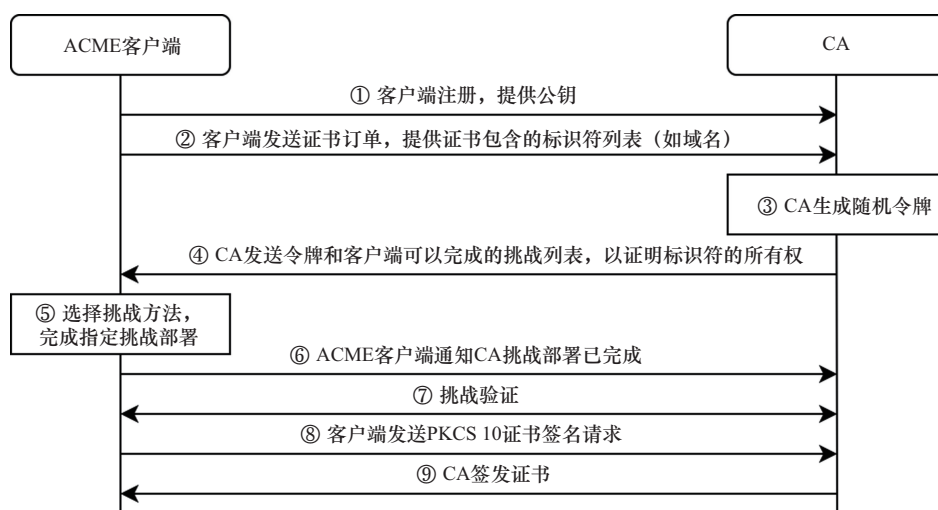


图6 RFC 8555协议流程

证；通过非重复 nonce 值抵御重放攻击，并通过对请求进行速率限制来抵御拒绝服务攻击。然而，该标准未涉及CA单点故障、证书透明度、用户隐私保护和抗量子攻击等问题。在可用性方面，该方案可以通过增加CA服务器、带宽、内存和存储资源来应对工作负载增长，具备良好的可扩展性。此外，该标准支持管理具有不同标识符数量的DV证书，并允许基于私钥证明的证书撤销，从而在

一定程度上满足了灵活性需求，并符合鲁棒性要求。然而，基于CRL或OCSP的证书撤销机制效率较低，Let's Encrypt与DigiCert等CA的撤销生效周期约为1 d。在性能方面，在采用ECDSA P-256算法的情况下，单次通信开销约为4 730 B；每日存储400万份证书至少需要8 GB内存。

Aas等^[5]系统地介绍了Let's Encrypt项目的进展情况。作为首个实现ACME客户端与服务

器的免费自动化 CA, 该项目显著加速了域名证书的普及, 并迅速发展为主流的 CA 之一。该方案主要涉及证书的申请、更新与撤销。在安全性方面, 其通过证书透明度和控制验证^[18]来抵御中间人攻击, 但对拒绝服务攻击、重放攻击及用户隐私保护等方面未进行详细讨论。在可用性方面, ACME 标准设计能够满足鲁棒性要求, 并部分满足灵活性需求。项目同时考虑了可扩展性, 其硬件安全模块每秒可以处理约 450 个签名请求。在性能表现上, 基于 CRL 与 OCSP 的证书撤销生效周期约为 1 d; 采用 ECDSA P-256 算法时的通信开销约为 4 730 B; 每日存储 CT 日志和 400 万份证书的开销为 35.78 GB。

4.2 ACME 安全增强

2019 年 11 月, IETF 采纳了 RFC 8657 标准。该标准为 DNS 记录引入了账户 URI 与验证方法两项扩展参数, 以增强 CAA 策略的控制粒度。其中, 账户 URI 参数用于标识特定 CA 账户, 验证方法参数则用于限定 ACME 协议所采用的域控制权验证方式。此外, 为保障 CAA DNS 记录的时效性, 该标准建议 CA 将读取的 CAA DNS 记录设置为短期有效, 或在颁发证书前重新验证 CAA 策略。该标准不涉及具体的证书管理功能, 因此不满足任何功能性指标。在安全性方面, 该标准通过使用域名系统安全扩展 (DNSSEC) 来保护 CAA DNS 记录, 防范全局中间人攻击。然而, 由于 CAA DNS 记录本身公开可访问, 引入账户 URI 参数可能导致第三方推断不同域名之间的关联, 带来一定的信息泄露风险。其余安全性指标、可用性指标与性能指标在此标准中均未予以规定。

2020 年 2 月, IETF RFC 8737 标准制定完成, 该标准旨在解决 TLS 服务名称指示 (server name indication, SNI) 挑战中存在的安全漏洞。此类漏洞允许攻击者非法验证其他域名的控制权, 其成因在于部分大型服务商未能对不同用户的域名进行有效隔离, 导致某一用户可以响应其他用户的 TLS SNI 请求。为解决此问题, 该标准定义了一种基于 TLS 的应用层协议协商 (application-layer protocol negotiation, ALPN) 扩展的新型 ACME 挑战, 即 `tls-alpn-01`。该挑战要求 ACME 客户端提供自签名证书 (该证书须包含 ACME 标

识符和 SAN 扩展, 其中 ACME 标识符扩展携带挑战密钥授权的 SHA-256 摘要), ACME 服务器随后通过 TLS 连接验证返回的证书是否符合预期。该标准主要聚焦于证书申请阶段的域控制权验证, 其灵活性沿用 RFC 8555 的多标识符证书申请机制。每日签发 400 万份证书将产生约 8 GB 的存储开销。其他安全性、可用性和性能指标未在该标准中予以考虑。此外, 不支持 ALPN 扩展的设备将无法使用 `tls-alpn-01` 挑战。

2022 年, Sujatanagarjuna 等^[9]为提高证书撤销过程的安全性和效率, 将 BlockVoke 协议^[19]扩展到现有的 ACME 协议中。该方案修改了 ACME 的证书申请与撤销流程, 并添加了一种额外的挑战验证机制。在证书申请阶段, 证书持有人使用比特币钱包私钥对 CA 提供的安全随机数进行签名作为挑战响应, 同时持有人与 CA 的比特币钱包的聚合地址将被记录在证书扩展字段中。当需要撤销证书时, 证书持有人或 CA 只需从该聚合地址发起一笔证书撤销交易到任意比特币地址, 即可宣告证书作废。在安全性方面, 该方案实现了控制验证, 并对拒绝服务攻击和中间人攻击进行了讨论, 同时解决了传统 OCSP 查询中可能泄露用户浏览历史的问题。其证书管理的灵活性来源于 ACME 标准协议。在性能方面, 受比特币共识机制限制, 该方案的证书撤销生效平均时间约为 240 s, 每日 400 万份证书的存储开销约为 8 GB。该方案未讨论其他的安全性、可用性和性能指标。

2023 年, Newman^[13]提出了一种缓解 CA 自动签发恶意证书的方法。该方法主要针对基于 OIDC (OpenID connect) 的自动化 CA, 在验证证书申请者提供的 OIDC 令牌后自动签发证书, 并将 OIDC 令牌和证书时间戳嵌入证书中, 同时记录在 CT 日志中。此外, CA 采用了一种基于 Guillou-Quisquater 签名的零知识证明方法^[20]来防止证书中的 OIDC 令牌签名被滥用于控制权验证。Newman 为 Sigstore CA^[21]提供了该方案的原型系统。在安全性方面, 该方案支持证书透明度与控制验证, 并实施了重放保护机制, 同时讨论了证书信息隐私保护问题。然而, 该方案存在 CA 与 OIDC 令牌颁发者的合谋与单点故障风险。

在可用性方面, 该方案基于 ACME 标准设计, 能够满足部分灵活性需求。在性能方面, 每日 400 万份证书及相关 CT 日志的存储开销约为 35.78 GB, 其他性能指标未进行讨论。

2024 年, Giron 等^[14]为应对量子计算机对 ACME 协议中传统加密算法的威胁, 提出了一个基于后量子密码学算法^[22]的证书自动颁发方案。然而, 后量子密码签名会显著增加 HTTP 挑战的通信开销, 为此该团队提出了一种新的挑战方法。首先通过传统证书完成 TLS 身份认证, 然后 ACME 客户端向 CA 发送证书签名请求, 最后由 CA 自动签发后量子证书, 但该方法仅适用于已有传统证书的申请者。在具体实现上, 该团队将开放量子安全项目^[23]中的后量子密码库集成到 ACME 服务器 Pebble 中, 并使用 NIST 后量子密码标准中的 Falcon-512 算法和 Dilithium2 算法替换传统的 RSA 和椭圆曲线签名算法 (ECDSA)。尽管新挑战方法尝试控制开销激增, 但证书签发效率仍低于传统密码算法, 通信与存储开销也为传统方案的数倍。例如, 当采用 Falcon-512 算法时, 通信开销达 13 465 B, 单个证书的存储开销为 7 157 B, 每日 400 万份证书的存储开销约为 28.628 GB; 当采用传统的 ECDSA P256 算法时, 通信开销为 4 730 B、存储开销为 8 GB。后量子密码方案在可扩展性方面仍面临挑战。在安全性方面, 该方案提供了重放保护、控制验证和抗量子攻击能力, 但依旧无法规避 CA 单点故障问题。该方案延续了 ACME 标准中对多域名 DV 证书的支持, 能够部分满足灵活性需求。

4.3 标识符与应用场景扩展

2020 年 2 月, IETF RFC 8738 标准制定完成, 该标准旨在解决 ACME 仅支持域名标识符挑战的问题, 从而将其应用范围扩展至包含 IP 地址标识符的证书。该标准规定了如何利用现有的 ACME 验证挑战来确认 IPv4 和 IPv6 地址的控制权。标准中明确了 IP 地址标识符通过 HTTP 挑战或 tls-alpn 挑战进行控制验证, 但仅限于证书申请阶段。证书申请依据 RFC 8555 实现, 能够部分满足灵活性需求。在安全性方面, RFC 8738 与 RFC 8555 保持一致, 实现了控制权验证、重放攻击保护、拒绝服务攻击缓解及中间人攻击防

范。该标准的存储开销与 RFC 8555 一致, 约为 8 GB。然而, 该标准并未讨论其余安全性、可用性和性能相关指标。

2021 年 4 月, IETF 通过了 RFC 8823 标准。该标准定义了 email-reply-00 挑战机制, 旨在扩展 ACME 协议对安全/多用途互联网邮件扩展 (secure/multipurpose internet mail extensions, S/MIME) 证书的支持。该标准规定了 ACME 挑战邮件与响应邮件的格式。ACME 挑战邮件的主体头部包含 token-part1, 邮件体通常说明挑战目的, 并通过域名密钥识别邮件或 S/MIME 签名来验证其真实性。ACME 响应邮件的主体头部则是对挑战邮件的回复, 由 S/MIME 证书绑定邮箱后发送至 CA 邮箱。ACME 客户端将通过电子邮件获取的 token-part1 与通过 HTTPS 接收的 token-part2 组合, 形成 ACME 令牌。随后, 按照 RFC 8555 的规定计算密钥授权值, 并将其作为 ACME 响应邮件的邮件体。RFC 8823 规定 S/MIME 证书仅用于签名或加密, 其证书管理的灵活性与 RFC 8555 保持一致。在安全性方面, RFC 8823 遵循 RFC 8555 中的各项安全保护措施, 同时 email-reply-00 挑战的可靠性也依赖于电子邮件系统自身的安全性。根据理论估算, 每日存储 400 万份证书的存储开销约为 8 GB。然而, 该标准未考虑可用性指标及性能指标。

2021 年, Mueller 等^[7]指出, 在电子邮件场景中缺乏自动化的密钥管理机制, 导致加密电子邮件的使用率偏低。为解决这一问题, 该团队提出了一套基于 ACME 协议的 S/MIME 证书与密钥自动化管理方案, 并对开源 ACME 服务器 Pebble 进行了相应改造。此外, 该团队还基于开源邮件客户端 Thunderbird 实现了 ACME 客户端。该方案遵循 IETF RFC 8555 标准实现了自动化证书管理, 并依据 IETF RFC 8823 标准实现了邮件地址所有权验证。然而, 由于采用了中心化的 ACME 架构, 该方案无法避免 CA 单点故障问题, 且未探讨其他安全性指标。该方案基于 ACME 标准实现且专用于邮件系统, 能够满足证书撤销的鲁棒性要求, 并部分满足证书管理的灵活性需求, 但无法满足通用性需求, 可扩展性问题也未讨论。在性能方面, 基于 CRL 和 OCSP 的证书撤销

生效时间约为 1 d，每日存储 400 万份证书的存储开销约为 8 GB。与人工申请方式相比，该方案将证书申请耗时从至少 254 s 缩短到 3 s。

2021 年 9 月，IETF 通过了 Sheffer RFC 9115 标准，该标准允许标识符持有者（identifier owner, IdO）授权名称委托消费者（name delegation consumer, NDC）获取 X.509 证书，从而使证书主体表现为 IdO 的标识符，证书所绑定的公钥则对应由 NDC 控制的私钥。委托标识符证书申请流程如图 7 所示。该标准适用于 CDN 代表 IdO 进行 TLS 会话的场景，其中 CDN 对应 NDC。在协议中，IdO 充当 NDC 与 ACME 服务器之间的中间人。NDC 向 IdO 发起证书申请，IdO 将请求转换后提交给 ACME 服务器，进而完成整个证书申请流程。最终，NDC 可以直接从 ACME 服务器获取证书，该证书的标识符属于 IdO，而公私钥对属于 NDC。该标准也适用于短期自动续期（STAR）证书和非 STAR 证书，能够满足证书的申请、更新和撤销各项功能需求。在安全性方面，该标准与 RFC 8555 保持一致，但单点故障、证书透明度、保护用户隐私及保护抗量子攻击等问题未在标准中予以讨论。此外，恶意或已遭破坏的 CDN 可能利用 IdO 对其的信任随意生成网站证书。在可用性方面，该标准在灵活性与鲁棒性上与 RFC 8555 保持一致。在性能方面，基于 OCSP 或 CRL 的证书撤销生效时间约为 1 d，每日存储 400 万份证书的存储开销约为 8 GB。

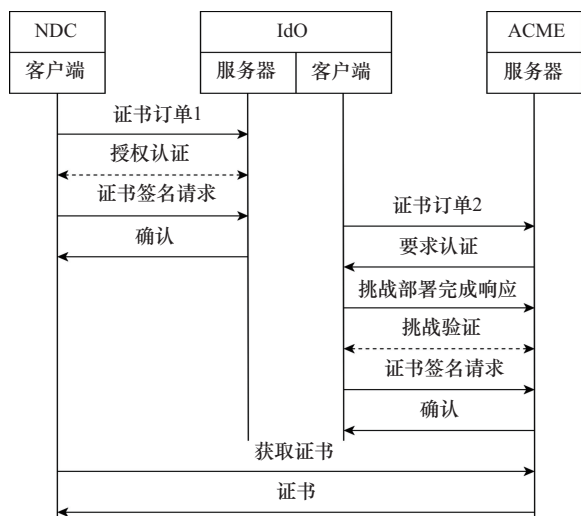


图 7 委托标识符证书申请流程

2023 年 7 月，3GPP 发布了技术报告 TR 33.876^[11]，该报告主要研究了 5G 系统中服务化架构（service-based architecture, SBA）环境下的自动化证书管理。该报告指出，随着互操作性和安全性需求的增长，5G SBA 环境对自动化证书管理协议和流程的需求愈发迫切。此外，该报告还探讨了若干关键问题，并针对每个问题提出了相应的解决方案或考虑因素。其中关键问题包括单一证书管理协议和流程、网络功能证书注册的安全保护、证书更新、证书机构层次结构的信任链、证书撤销过程、证书管理生命周期与网络功能（network function, NF）管理生命周期的关系、多个证书关联到单一网络功能、可信网络功能实例标识符、网络切片场景下的自动化证书管理等。解决方案涵盖证书注册和管理框架、使用证书管理协议注册和更新证书、确保 NF 证书初始注册的安全性、在 SBA 中实现交叉认证和基于 CA 的互联信任链、基于 OCSP 的证书撤销流程、解决证书生命周期管理与 NF 关系的问题、强化证书参数的安全保护、基于网络仓库功能的证书撤销查询、指示和验证证书目的、OCSP 装订、网络切片的自动化证书管理、为 NF 证书注册建立初始信任、批量证书更新的管理、使用 ACME 协议注册和更新证书、证书中唯一的 NF 标识符的确定和切片特定的初始注册程序。该报告特别强调了为支持服务切片和虚拟网络功能的自动化管理，在证书管理方面需采取的具体措施。该报告涵盖证书的申请、更新、撤销和验证整个流程，讨论了中间人攻击和重放攻击威胁，并强调了控制权验证的重要性。该报告以 ACME 标准为基础，能够支持多标识符证书管理和多种证书撤销方法，从而在保障系统鲁棒性的同时部分满足了管理的灵活性需求。然而，该报告未讨论 CA 单点故障、证书透明度、拒绝服务攻击防护、用户隐私保护和抗量子攻击问题。此外，该报告没有讨论性能方面的指标。

2023 年 8 月，IETF 通过了 RFC 9444 标准。该标准规定了如何使用 ACME 协议为子域名标识符申请并获取由 CA 签发的证书。若 CA 安全策略允许，ACME 客户端可以仅针对主域名进行挑战验证，而非对每个子域名逐一进行验证。该

表2 ACME 研究对比

ACME 研究	证书 申请	证书 更新	证书 撤销	证书 验证	CA单 点故障	证书透 明度	控制 验证	抵御拒 绝服务 攻击	抵御 重放 攻击	抵御中 间人 攻击	用户 隐私 保护	量子 攻击	通用性	可扩展 性	鲁棒性	灵活性	撤销 生效 时间	通信 开销/ B	存储 开销/GB	计算 开销/s
IETF RFC 8555	✓	✗	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	△	1 d	4 730	8	—
IETF RFC 8657	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	—	—	—	—
IETF RFC 8737	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 8738	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 8739	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 8823	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 9115	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✓	△	1 d	—	8	—
IETF RFC 9444	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 9447	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 9448	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	△	—	8	8	—
IETF RFC 9538	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	△	—	8	8	—
ITU-T X.dpk- acme ^[10]	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	—	—	—	—
3GPP TR 33.876 ^[11]	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	△	—	—	—	—
Let's Encrypt ^[5]	✓	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗	✓	✓	△	1 d	4 730	35.78	—
Kfoury等 ^[6]	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	—	8 160	8 160	—
Mueller等 ^[7]	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	△	1 d	—	8	3
B-DCV ^[8]	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	12 s	—	9 600	26.79
Sujatanagarajuna等 ^[9]	✓	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗	△	240 s	—	8	—
ACMEH ^[12]	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	—	8	8	—
Newman ^[13]	✓	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓	✗	✗	✗	✗	△	—	35.78	35.78	—
Giron等 ^[14]	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	△	—	13 465	28.628	—

注：✓表示满足或解决，✗表示不满足或未解决，△表示部分满足，—表示未考虑或未讨论。

标准要求在 ACME 授权对象中新增一个“允许子域名认证”的字段，用于表明是否允许对该标识符下的所有子域名进行授权。标识符列表中可以包含子域名，而“祖先域名”字段用于记录其对应的主域名。ACME 服务器将基于这些标识符创建订单对象，并返回指向相应授权对象的链接。然而，该机制也引入了潜在风险：攻击者可能利用已通过验证的主域名授权，为其恶意构造的子域名申请到合法证书。该标准专注于证书申请过程，其灵活性和安全性指标沿用 RFC 8555 的相应指标。根据理论估计，每日存储 400 万份证书的存储开销约为 8 GB。该标准并未讨论单点故障、证书透明度和用户隐私保护问题，也未涉及可用性指标和性能指标。

2023 年 9 月，IETF 通过了 RFC 9447 标准，该标准定义了一种名为 tkauth-01 的通用权威令牌挑战机制，用于证明证书申请者对特定资源拥有有效的控制权。在此机制下，权威令牌被 ACME 客户端用于响应来自 ACME 服务器的挑战。该令牌通常有两种获取时机：一是在接收 ACME 挑战后，申请者向令牌颁发机构请求获取；二是在发起证书申请流程前已预先获得。该标准要求权威令牌必须与发起请求的特定 ACME 客户端正确绑定，从而防止令牌被用于重放攻击或其他用途的令牌攻击。

为获取权威令牌，ACME 客户端须向令牌颁发机构发送一个 HTTPS POST 请求，在获取权威令牌的过程中采用 TLS 协议来抵御中间人攻击。但在请求并获取权威令牌之前，必须建立 CA 和令牌机构之间的信任关系，以及 ACME 客户端和令牌颁发机构之间的信任关系。该标准仅适用于证书申请流程，其灵活性和安全措施与 RFC 8555 标准一致。此外，该标准未涉及单点故障、证书透明度、用户隐私保护和抗量子攻击等方面的安全考量。根据理论估计，每日存储 400 万份证书的存储开销约为 8 GB。该标准未对除此以外的可用性指标和性能指标进行讨论。

2023 年 9 月，IETF 通过了 RFC 9448 标准。该标准定义了 ACME 权威令牌的配置文件，用于为 VoIP 服务提供商自动化创建证书，以支持使用安全电话身份（secure telephone identity, STI）证

书定义的 TNAuthList 进行 STI 验证。该标准定义的 STI 证书请求过程是以 RFC 8555 标准规定的 ACME 协议为基础，结合 RFC 9447 标准中拓展的 ACME 权威令牌挑战方法来进行控制权验证的。该标准仅适用于证书申请场景，安全性方面主要沿用 RFC 8555 中的相关安全考虑，灵活性源于 RFC 8555 提供的证书管理能力。根据理论估算，每日存储 400 万份证书的存储开销约为 8 GB。该标准没有具体讨论其他性能方面的指标。

针对 ACME 协议仅支持 DV 类型证书管理的问题，Morales 等^[12]提出了高级自动化证书管理环境（ACMEH）协议，旨在实现对 DV、OV 和 EV 3 类证书的自动化管理。该协议在工作流程上与标准化的 ACME 协议保持一致，并采用 vp-01 挑战方法来完成控制权验证。具体而言，该协议要求 ACME 客户端通过万维网联盟（W3C）可验证凭证^[24]来证明其所声明的真实身份，获取该凭证的工作流程如图 8 所示。在功能性方面，ACMEH 主要聚焦于证书申请，具备支持全类型证书管理的能力，契合系统对灵活性的需求。在安全性方面，该方案虽考虑了控制权验证、中间人攻击与重放攻击等问题，但在应对拒绝服务攻击、CA 单点故障、用户隐私保护及证书透明性等方面仍存在不足。此外，可验证凭证的颁发机构亦存在单点故障的潜在风险。Morales 等^[12]通过理论分析指出，存储 400 万份证书的存储开销约为 8 GB，但未提供基于原型系统的其他具体性能测试结果。

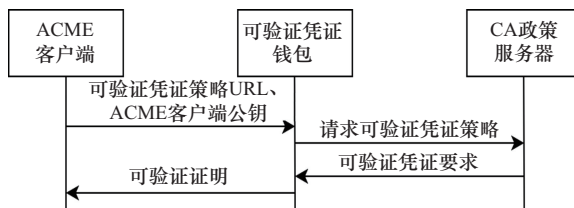


图 8 可验证凭证获取工作流程

2024 年 2 月，IETF 通过了 RFC 9538 标准。该标准定义了一种内容分发网络互联（content delivery network interconnection, CDNI）的元数据接口对象，旨在利用 RFC 9115 标准实现 X.509 证书的委派。CDNI 中的证书委托调用流程如图 9 所示。该标准允许上游内容分发网络（upstream

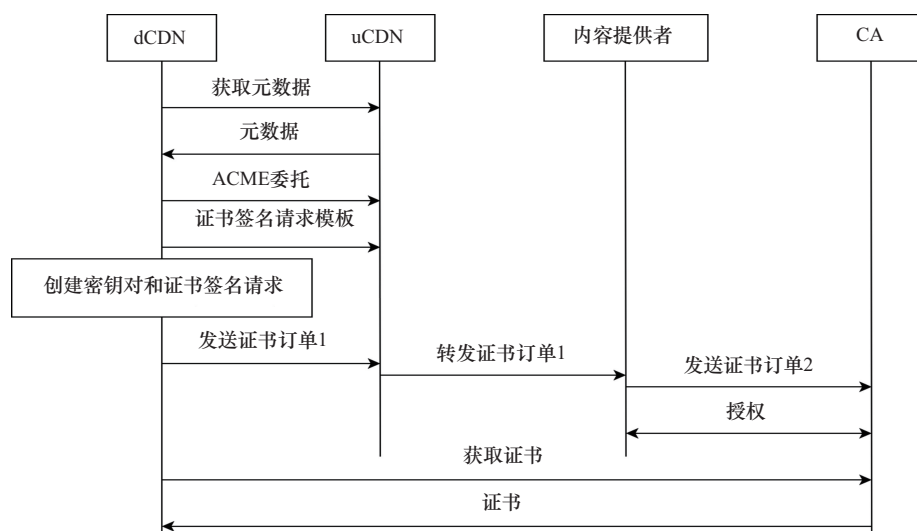


图9 CDNI中的证书委托调用流程

CDN, uCDN) 代表内容提供者在下游内容分发网络 (downstream CDN, dCDN) 上生成绑定指定域名和私钥的 X.509 证书, 从而实现安全的内容交付。RFC 9538 首先描述了通过足迹和功能广告接口 (footprint & capabilities advertisement interface, FCI) 公布 CDNI 委托元数据的实例, 其中 FCI 遵循 RFC 8008 的规定, 允许 dCDN 向 uCDN 发送 FCI 功能类型对象。RFC 9538 中规定的 ACME 委托元数据包括委托方法类型、时间窗口和相关属性信息等内容。此外, 这些元数据可以被用于描述 CDNI 中的 X.509 证书的颁发和管理过程, 从而实现 CDNI 框架下的证书授权和管理。该标准要求 ACME 委托过程必须遵循 RFC 8006 中元数据接口身份验证和机密性要求、关于 CDNI 请求路由的相关安全要求。该标准仅适用于证书申请, 在灵活性方面与 ACME 协议一致, 每日存储 400 万份证书的存储开销约为 8 GB。然而, 该标准没有讨论安全性、可用性和其他性能方面的指标。

4.4 短期证书管理

2020 年 3 月, ACME 协议的扩展方案被提出, 随后该方案被标准化为 IETF RFC 8739。该标准旨在实现对短期自动更新 (short-term, automatically renewed, STAR) X.509 证书的管理。STAR 证书的有效期极短, 通常为 24~72 h。由 CA 在 STAR 证书即将到期时自动为其续订, 从而简化证书管理流程并提升系统的安全性。STAR 证书自动续订流程如图 10 所示。

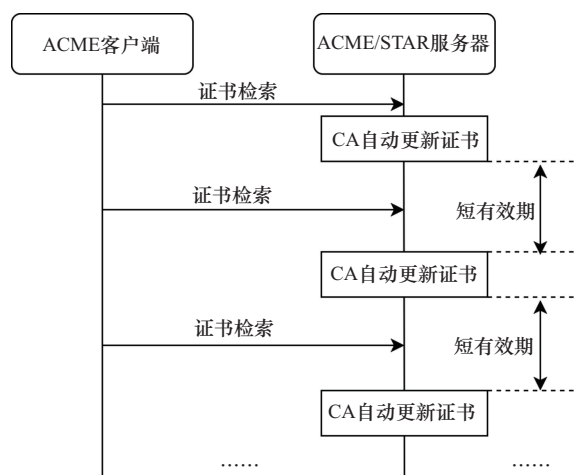


图10 STAR证书自动续订流程

STAR X.509 证书管理协议主要包括 3 个阶段, 即启动阶段、自动续订阶段和终止阶段。在启动阶段, ACME 客户端向 CA 发起请求, 申请创建一个 STAR 证书; 在自动续订阶段, CA 将定期自动重新签发 STAR 证书, 并将新签发的证书发布至指定下载目录; 在终止阶段, ACME 客户端请求 CA 停止该证书的自动续订服务。

该标准基于 RFC 8555 设计, 具备一定的灵活性。每日存储 400 万份证书的存储开销约为 8 GB。在安全性方面, RFC 8739 通过限制管理请求速率、设置更新周期下限等方式抵御拒绝服务攻击, 并使用不可猜测的 URL 来保护证书申请者的隐私信息。然而, 该标准不支持直接撤销 STAR 证书, 证书只能在过期后失效, 这在一定

程度上带来了安全风险。此外,该标准未对其他安全性指标、可用性指标及性能指标进行详细讨论。

4.5 去中心化 ACME 方案

为解决 ACME 协议中存在的中心化信任问题, Kfoury 等^[6]于 2020 年提出了一种基于区块链的去中心化 ACME 方案。该方案利用智能合约实现自动化域名控制验证与证书颁发,其基于区块链的域名控制验证流程如图 11 所示,其中 N_1 、 N_2 表示两个不同的随机数, $H()$ 代表哈希函数, $\parallel$ 代表拼接。该方案实现了证书申请、域名控制权验证、证书更新和证书验证。通过引入区块链技术,该方案实现了去中心化信任机制,避免了 CA 单点故障问题。同时,借助区块链的公开透明特性,确保所有证书操作均被记录和公开。然而,该方案仍存在若干局限性。其一,缺乏对自签名证书内容的约束策略,且不支持证书撤销机制;其二,该方案仅适用于证书管理账户未丢失的场景,无法满足证书管理账户丢失后的管理需求;其三,该方案仅支持单域名 DV 证书管理,无法满足多域名 DV 证书管理需求,灵活性受限;其四,该方案基于以太坊公有链实现,受限于工作量证明共识算法,吞吐量仅为 17 TPS (每秒交易数),难以满足大规模证书管理场景下的可扩展性要求;其五,在存储开销方面,每份证书需在区块链上记录约 272 B 的数据,考虑到当

前以太坊网络包含约 7 500 个节点,且每个节点均需保留完整的数据副本,以每日处理 400 万张证书计算,全网每日存储开销约为 8 160 GB,给系统带来了显著的存储压力。

2022 年, B-DCV 方案^[8]在前期工作^[6]的基础上进行了改进,实现了基于区块链的自动化域名所有权验证,并开发了一种用于建立安全会话的浏览器插件。该方案利用区块链的透明性和去中心化特性,能够满足证书透明度要求,同时有效解决 CA 单点故障问题。然而, B-DCV 仍存在若干局限性。在功能支持方面,该方案不支持多域名 DV 证书管理,难以满足灵活性需求。在鲁棒性方面,一旦证书管理账户丢失,将无法正常进行证书管理,系统缺乏有效的账户恢复机制。此外,该方案引入了一个新的第三方验证服务器实体,在证书验证环节可能引入新的单点故障风险。在性能方面,受限于以太坊平台约 17 TPS 的吞吐量,该方案的可扩展性有限,难以支撑大规模证书管理的应用需求。具体而言,证书申请平均耗时约为 26.79 s,主要原因是公有链吞吐量受限导致交易确认时间较长。根据现有以太坊区块链的出块速度,证书撤销生效时间约为 12 s。在存储开销方面,每份证书需要在单个区块链节点上存储约 320 B 的数据,以此计算,每日存储 400 万份证书的存储开销约为 9 600 GB。

2023 年 8 月 10 日, ITU-T 提出了 X.dpk-acme

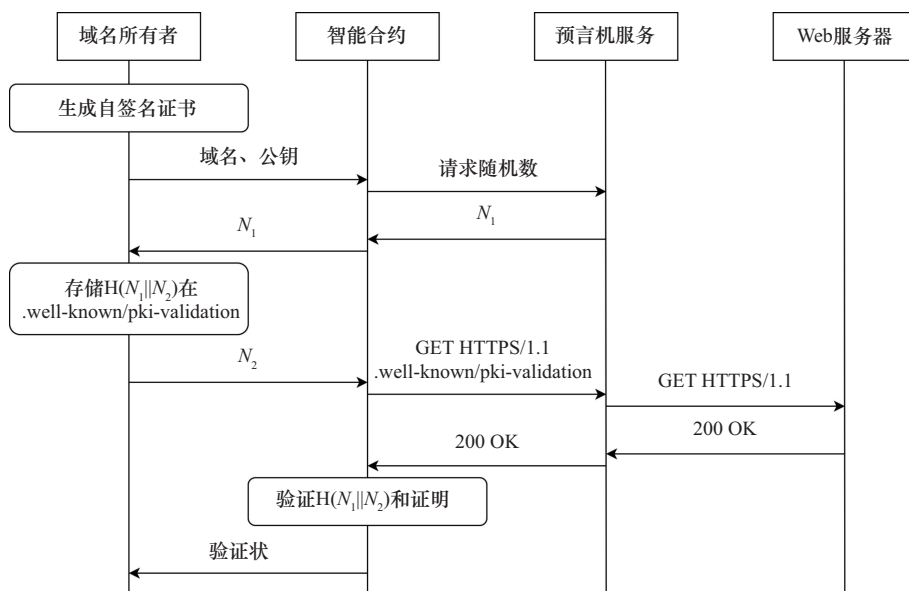


图 11 基于区块链的域名控制验证流程

草案^[10]，旨在开发一个融合分布式账本技术和ACME协议的框架，用于实现X.509域名证书的自动化管理，以解决传统集中式CA体系存在的单点故障问题，并提升系统的透明度与安全性。该草案的概念性架构如图12所示，通过引入智能合约和去中心化网络特性，提供一种可靠、透明的证书自动签发与管理机制。此外，该草案明确了涵盖证书申请、验证、更新和撤销的详细架构设计，并界定了各主要实体的职责。然而，草案中去中心化ACME协议的具体内容仍有待完善。

在安全性设计方面，该草案主要考虑了5个层面：第一，利用区块链技术消除CA单点故障风险；第二，通过ACME协议实现证书的自动化签发与管理，减少人为干预；第三，利用智能合约技术实现证书管理规则与逻辑的自动化执行，提高系统的可信度与安全性；第四，建立公开透明的审计机制，对所有证书管理交易进行审计，确保系统的公正性与透明度；第五，在证书管理过程中采用数据加密和身份认证等措施，保障数据安全。整体而言，该草案涵盖了证书申请、更新、撤销、验证等功能需求，在安全性方面考虑了单点故障、证书透明度和控制验证等问题，但其余安全性指标、可用性指标及性能指标尚未明确。

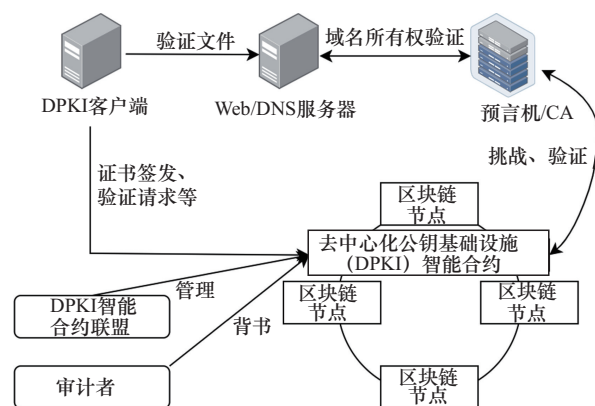


图12 ITU-T X.dpki-acme的概念性架构

4.6 归纳和分析

ACME协议的相关研究在工业界和学术界均取得了显著进展。ACME协议最初由Let's Encrypt项目^[5]提出和设计，随后由IETF标准化为RFC 8555^[6]，标志着该协议受到了国际认可。在

此基础上，IETF相继制定了系列国际标准（如RFC 8657、RFC 8737、RFC 8738、RFC 8739、RFC 8823、RFC 9115、RFC 9444、RFC 9447、RFC 9448和RFC 9538等），以扩展ACME协议的应用场景和证书管理能力。此外，3GPP也试图将RFC 8555中的ACME协议应用于5G核心网^[11]。与此同时，在学术研究方面，Mueller等^[7]、Sujatanagarjuna等^[9]、Morales等^[12]、Newman^[13]和Giron等^[14]的研究，或扩展了RFC 8555中标准化ACME协议的应用场景，或增强了协议的安全性。针对标准化ACME协议中存在的CA单点故障问题，ITU-T开展了标准化ACME协议的去中心化改造和国际标准研究^[10]。Kfoury等^[6]基于以太坊公有链开展了去中心化的ACME协议研究。B-DCV^[8]改进了Kfoury等^[6]的工作，实现了域控制权验证并开发了用于建立安全会话的浏览器插件。上述研究共同推动了ACME协议的完善与发展。

值得注意的是，去中心化ACME研究为未来去中心化PKI体系下的自动化证书管理提供了一定的启示。目前，标准化的ACME协议因其中心化架构，面临CA单点故障、证书操作缺乏透明性和证书撤销生效时间长等问题。区块链技术因其去中心化、不可篡改、可追溯和自动化等特性，被认为是应对这些问题的潜在解决方案。具体而言，其技术优势主要体现在4个方面：其一，区块链通过共识机制将传统集中式信任分散至多个共识节点，并利用基于密码学的链式结构确保数据的防篡改特性，从而消除对单一CA机构的依赖，增强抵御CA数据伪造的能力，缓解CA单点故障问题；其二，区块链上的每笔交易均公开透明且可追溯，使证书管理操作具备可监督性和可审计性，从而提高系统的透明度；其三，智能合约的引入使证书管理任务能够自动化执行，减少人工干预，提高管理效率；其四，由于区块链共识所需时间通常短于中心化ACME协议中CA更新证书撤销列表的周期，因此基于区块链的证书撤销机制能够提供更优的实时性。总体而言，区块链技术的特性在缓解中心化ACME的核心挑战方面展现出应用潜力。然而，去中心化ACME在功能、性能、隐私保护和标

准化等方面仍存在广阔的可研究空间。随着相关技术的演进和研究的深入,基于区块链的去中心化 ACME 有望成为未来网络中证书管理的主流。

5 ACME 现有问题和潜在研究方向

本节将根据第 4 节中对 ACME 相关文献的综述和讨论,总结现有研究的主要问题,并展望 ACME 技术发展趋势和潜在研究方向。

5.1 现有研究主要问题

(1) 存在 CA 单点故障

现有的 ACME 相关 IETF 标准均基于中心化 PKI 体系,普遍存在 CA 单点故障问题,这也是影响 PKI 系统和证书管理可信性的主要因素之一。尽管目前已经提出去中心化的 ITU-T X.dpk-acme 草案^[10]和部分去中心化 ACME 研究方案^[6],但从国际标准层面来看,目前尚未制定任何去中心化 ACME 的相关国际标准,去中心化 ACME 的标准制定仍处于草案阶段。

(2) 缺少通用性和灵活性

现有 ACME 相关研究方案和国际标准在通用性和灵活性方面均存在局限性。这些研究方案 and 标准往往仅针对其中的一种或几种场景(如互联网域名、电子邮件系统、通信网络或 CDN 等)设计,无法实现全场景通用。这一局限性主要源于证书主体标识符的多样性。证书主体标识符既可以是网络资源,也可以是非网络资源,这种多样性导致难以设计出一种能够适配所有主体标识符类型及应用场景的控制权验证方法。此外,目前只有 Morales 等^[12]提出的方案支持 DV、OV 和 EV 证书的自动化颁发,但需依赖可信的可验证凭证颁发者。

(3) 缺乏证书透明度要求

现有的 ACME 相关 IETF 国际标准并未提及或要求在自动化证书管理过程中实现证书透明度。对于公钥证书管理而言,证书透明度有助于审计证书签发行为、及时发现恶意证书。实际上,证书透明度已在 IETF RFC 9162 被标准化,且现代浏览器在进行证书验证时也逐渐开始检查证书透明日志,这间接推动了 CA 主动支持并实施证书透明度相关机制。相比之下,ITU-T X.dpk-acme 草案和部分学术界的研究方

案考虑并满足了证书透明度需求。因此,证书透明度相关要求应当在 ACME 国际标准中予以明确规定。

(4) 缺少用户隐私保护

现有 ACME 文献几乎均未提及用户隐私保护方面的措施。这可能是当前 ACME 方案的通用性局限,导致用户隐私保护需求不够明显。实际上,CA 在证书的某些属性中可能会记录证书主体背后控制人或组织的敏感信息。如果未来个人数字证书被纳入 ACME 自动化管理体系,隐私保护需求就会显著增加,因为个人数字证书可能涉及更多的敏感信息(如 ID、身份证号和家庭住址等)。因此,针对这些敏感属性内容实施适当的保护措施将变得尤为重要。

(5) 可拓展性问题

现有 ACME 相关标准尚未对可扩展性提出具体要求。在可拓展性方面,中心化 PKI 自动化证书管理系统往往通过升级 ACME 服务器的硬件配置和网络带宽来满足潜在的大规模证书管理需求。然而,目前基于公有链的去中心化 ACME 方案受限于区块链本身的低吞吐能力,难以满足日常大规模的证书管理需求。此外,由于区块链节点需保持全局账本的一致性,链上数据存储成本较高,随着系统的持续运行,存储压力也将逐渐增大。

(6) 缺少抗量子攻击能力

现有 ACME 国际标准主要依赖 RSA 加密算法和椭圆曲线加密(ECC)等传统密码学算法,尚未考虑量子计算带来的威胁。在学术研究方面,仅有 Giron 等^[14]尝试应对量子攻击挑战,但在实际落地应用上仍面临许多问题。目前,量子计算机已经能够利用 Shor 算法^[25]轻松破解传统密码机制,直接威胁到基于传统密码学算法的协议和系统,这是未来无法忽视的问题。

5.2 未来研究方向

(1) 消除 CA 单点故障

现有的 ACME 标准均无法避免 CA 单点故障问题,消除 CA 单点故障成为未来研究的重要内容。区块链技术能够提供多方之间的去中心化信任,有效解决单点故障问题。此外,基于区块链的智能合约技术能够实现去中心化自动化

执行, 契合 ACME 的需求。因此, 针对 CA 单点故障问题, 基于区块链的去中心化 ACME 改造成为一种潜在的解决方案。目前已有少量相关研究, ITU-T 也提出了一份关于去中心化 ACME 协议草案, 但具体协议内容仍有待完善, 相关工作仍在推进中。未来, 设计适用于去中心化 PKI 场景的 ACME 协议将成为一个重要的研究方向。

(2) 拓展 ACME 协议应用场景

现有 ACME 研究尚无法实现全场景通用, 拓展 ACME 协议应用场景并实现协议通用性是值得探索的方向。从国际标准演进来看, RFC 8555 发布后的后续标准主要致力于将 ACME 适配至新的业务需求 (如 CDN 场景下的证书管理) 和标识符类型 (如 IP 地址和电子邮件地址等)。此外, 从 3GPP 技术报告来看, 目前正在探索 ACME 在通信网络 5G/6G 服务化架构中的应用。可以预见, ACME 将在不同类型网络 and 行业中得到广泛应用。因此, 探索 ACME 的新业务场景, 设计新的 ACME 控制验证方法以拓展 ACME 的应用边界, 将是未来的重要研究方向。例如, 解决 ACME 在通信网络应用中的关键问题、探索 ACME 在物联网中的应用、实现去中心化 ACME 环境下 OV 和 EV 证书的签发、探索全场景通用的 ACME 方案等, 均具有较高的研究价值。

(3) 实现证书透明度和可审计

现有 ACME 标准并未明确要求实施证书透明度, 但证书透明度的实施有利于提高自动化证书管理的可信度。这一方向有望成为未来标准化工作的重点内容。当前实现证书透明度有两种途径: 一是依据 RFC 9162 部署集中式证书透明度日志, 二是利用区块链的不可篡改特性来实现证书透明度日志。集中式证书透明度日志方案虽然有效, 但仍面临单点故障风险。因此, 基于区块链实现证书透明度日志成为一种潜在的研究方向。借助区块链技术, 可以构建更可靠、更安全的证书透明度日志, 更好地满足证书审计的需求。然而, 如何在保障用户隐私的前提下实现证书的透明度和可审计, 仍是一个亟待解决的关键问题。

(4) 保护用户隐私

ACME 的隐私保护将成为重要的研究方向。现有 ACME 文献几乎均未提及用户隐私保护方面的措施, 但潜在的用户隐私安全问题不容忽视。随着 ACME 技术向支持更多证书类型拓展, 证书中的某些属性可能会记录与个人身份相关的敏感信息。因此, 必须考虑如何避免敏感数据被公开记录在区块链上或证书中。可以考虑利用公钥密码体系和零知识证明技术^[26]来实现证书属性的隐私保护, 甚至实现匿名证书, 从而在保证证书透明度和安全性的同时, 保护用户的隐私信息。

(5) 解决可扩展性问题

可扩展性直接关系到去中心化 ACME 系统的可用性和运行效率, 是去中心化 ACME 协议能否实现大规模落地应用的关键因素, 将成为未来研究的重要方向。当前主要瓶颈集中于区块链的吞吐能力与存储空间。针对这一问题, 可从两方面入手: 一方面, 利用区块链分片技术^[27]与链下计算提高去中心化 ACME 系统的吞吐量和处理能力; 另一方面, 采用链下存储^[28]与密码累加器^[29]等存储结构来节约链上存储资源。未来研究可从提高吞吐量和优化存储两个方向寻求突破, 从而增强去中心化 ACME 系统的性能与实用性。

(6) 探索更高效的后量子密码学证书管理

随着量子计算的发展, 传统密码学体系将受到更明显的冲击。因此, 增强 ACME 协议抗量子攻击能力, 对于保障数据和通信安全、抵御潜在量子威胁、推动 ACME 向后量子时代平稳过渡具有重要意义。然而, 当前后量子密码学算法的应用会带来较大的计算与存储开销。Giron 等^[14]提出的方案的开销是传统密码算法的数倍, 制约了实际应用落地。因此, 如何在为 ACME 引入后量子密码学算法的同时, 有效控制时空开销、提升签名效率将成为未来研究中的一项重大挑战。

6 结束语

本文系统梳理了自 ACME 技术诞生以来国内外相关文献, 涵盖主流国际标准组织的标准文档及学术界最新研究成果。通过对文献的系统回顾与分类归纳, 全面呈现了 ACME 技术的发展

脉络, 并深入分析了各阶段的研究重点与安全关注点。在此基础上, 本文总结了当前 ACME 技术面临的主要问题与发展趋势, 并指出了未来值得关注的研究方向。

参考文献:

- [1] Krombholz K, Mayer W, Schmiedecker M, et al. "I have no idea what I'm doing": on the usability of deploying HTTPS[C]//Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17). Berkeley: USENIX Association, 2017: 1339-1356.
- [2] Khan S, Luo F, Zhang Z J, et al. A survey on X.509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies[J]. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2529-2568.
- [3] Kohnfelder L M. Towards a practical public-key cryptosystem[D]. Cambridge: Massachusetts Institute of Technology, 1978.
- [4] X.509(11/88): The directory-authentication framework[S].
- [5] Aas J, Barnes R, Case B, et al. Let's Encrypt: an automated certificate authority to encrypt the entire web[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2019: 2473-2487.
- [6] Kfoury E F, Khoury D, Alsabeh A, et al. A blockchain-based method for decentralizing the ACME protocol to enhance trust in PKI[C]//Proceedings of the 2020 43rd International Conference on Telecommunications and Signal Processing (TSP). Piscataway: IEEE Press, 2020: 461-465.
- [7] Mueller T, Michalek A. Let's create! automated certificate management for end-users[C]//Proceedings of the 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). Piscataway: IEEE Press, 2021: 1-6.
- [8] Khoury D, Balian P, Kfoury E. Implementation of blockchain domain control verification (B-DCV)[C]//Proceedings of the 2022 45th International Conference on Telecommunications and Signal Processing (TSP). Piscataway: IEEE Press, 2022: 17-22.
- [9] Sujatanagarjuna A, Bochem A, Leiding B. Formalizing and safeguarding blockchain-based BlockVoke protocol as an ACME extension for fast certificate revocation[J]. Cryptography, 2022, 6(4): 63.
- [10] ITU. Proposal for new work item X. dpki-acme: framework and methodologies for the automation of domain name certificate management based on DLT: ITU-T SG17[EB]. 2023.
- [11] 3GPP. 3rd generation partnership project; technical specification group services and system aspects; study on automated certificate management in service-based architecture (SBA) (Release 18): 3GPP TR 33.876[R]. 2023.
- [12] Morales D A C, Wazan A S, Chadwick D W, et al. Enhancing the ACME protocol to automate the management of all X.509 web certificates[M]//ICT systems security and privacy protection. Cham: Springer Nature Switzerland, 2024: 265-278.
- [13] Newman Z. Reducing trust in automated certificate authorities via proofs-of-authentication[PP]. (2023-07-17) [2025-10-26]. arXiv: arXiv. 2307. 08201.
- [14] Giron A A, Schardong F, Perin L P, et al. Automated issuance of post-quantum certificates: a new challenge[M]//Applied cryptography and network security. Cham: Springer Nature Switzerland, 2024: 3-23.
- [15] Rivest R L. Can we eliminate certificate revocation lists? [M]//Financial cryptography. Berlin, Heidelberg: Springer, 1998: 178-183.
- [16] Jimenez-Peris R, Patino-Martinez M, Alonso G, et al. How to select a replication protocol according to scalability, availability and communication overhead[C]//Proceedings 20th IEEE Symposium on Reliable Distributed Systems. Piscataway: IEEE Press, 2001: 24-33.
- [17] Gallais A, Carle J, Simplot-Ryl D, et al. Localized sensor area coverage with low communication overhead[J]. IEEE Transactions on Mobile Computing, 2008, 7(5): 661-672.
- [18] Wendlandt D, Andersen D G, Perrig A. Perspectives: improving SSH-style host authentication with multi-path probing[C]//Proceedings of the USENIX 2008 Annual Technical Conference (ATC'08). Berkeley: USENIX Association, 2008: 321-334.
- [19] Garba A, Bochem A, Leiding B. BlockVoke-fast, blockchain-based certificate revocation for PKIs and the web of trust[M]//Information security. Cham: Springer International Publishing, 2020: 315-333.
- [20] Guillou L C, Quisquater J J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory[M]//Advances in Cryptology-EUROCRYPT' 88. Berlin: Springer, 1988: 123-128.
- [21] Newman Z, Meyers J S, Torres-Arias S. Sigstore: software signing for everybody[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 2353-2367.
- [22] Bernstein D J, Lange T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.
- [23] Stebila D, Mosca M. Post-quantum key exchange for the Internet and the open quantum safe project[M]//Selected Areas in Cryptography-SAC 2016. Cham: Springer International Publishing, 2017: 14-37.
- [24] Sedlmeir J, Smethurst R, Rieger A, et al. Digital identities and verifiable credentials[J]. Business & Information Systems Engineering, 2021, 63(5): 603-613.
- [25] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124-134.
- [26] 刘峰, 杨杰, 齐佳音. 区块链密码学隐私保护技术综述[J]. 网络与信息安全学报, 2022, 8(4): 29-44.
- [27] 唐海波, 张焕, 张召, 等. 区块链分片技术研究进展[J]. 软件学报, 2022, 33(10): 29-44.
- [28] Liu F, Yang J, Qi J Y. Survey on blockchain privacy protection techniques in cryptography[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 29-44.
- [29] 唐海波, 张焕, 张召, 等. 区块链分片技术研究进展[J]. 软件学报, 2022, 33(10): 29-44.

2025, 36(3): 1040-1064.

Tang H B, Zhang H, Zhang Z, et al. Research progress on blockchain sharding technology[J]. Journal of Software, 2025, 36(3): 1040-1064.

- [28] 蔡振华, 林嘉韵, 刘芳. 区块链存储: 技术与挑战[J]. 网络与信息安全学报, 2020, 6(5): 11-20.

Cai Z H, Lin J Y, Liu F. Blockchain storage: technologies and challenges[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 11-20.

- [29] 苗美霞, 武盼汝, 王贇玲. 密码累加器研究进展及应用[J]. 西安电子科技大学学报, 2022, 49(1): 78-91.

Miao M X, Wu P R, Wang Y L. Research progress and applications of cryptographic accumulators[J]. Journal of Xidian University, 2022, 49(1): 78-91.

[作者简介]



李龙鑫 (2000-), 男, 西安电子科技大学硕士生, 主要研究方向为网络安全、区块链、公钥基础设施证书管理等。



闫峥 (1972-), 女, 博士, 西安电子科技大学教授、博士生导师, 主要研究方向为信任管理、可信AI、隐私保护、网络安全等。



王海光 (1973-), 男, 博士, 华为技术有限公司高级研究员, 主要研究方向为5G/6G网络安全技术、可信网络、公钥基础设施证书管理等。



李铁岩 (1971-), 男, 博士, 华为技术有限公司高级技术专家, 主要研究方向为网络安全、数字身份与数据空间安全等。