

国密 ACME 客户端开源和免费国密 ACME 公共服务

2026 年 1 月 7 日

关心证书自动化的读者一定知道有许多开源的国际 ACME 客户端,如 CertBot, Let's Encrypt 官网推荐了 90 个,这些开源的 ACME 客户端大大推动了国际 SSL 证书自动化管理的普及应用。我国要想普及国密 SSL 证书,当然离不开国密 SSL 证书自动化,离不开国密 ACME 客户端和国密 ACME 公共服务。零信技术作为国内领先的国密 ACME 技术开发商,也是《自动化证书管理规范》密码行业标准的牵头制定单位,终于在完成了国密 ACME 商用产品-零信国密 HTTPS 加密自动化网关的研发后有空研发公益性质的国密 ACME 客户端并完全开源,同时向公众免费提供国密 ACME 公共服务。本文讲一讲这件大事,希望业界同行能同零信技术一道共同为普及国密 ACME 服务做贡献。



一、 ACME 不是一个产品而是一个生态

ACME 是“自动化证书管理环境”的英文缩写,也是一个英文单词,意思是“终极”,RFC8555 标准用这个单词作为技术标准的缩写的意思非常明确:这是 SSL 证书管理的终极解决方案,没有再好的解决方案了。这个解决方案不是一个产品,而是一个生态(环境),不仅仅是自动化申请证书的问题,涉及到相关生态的多个产品。

第一个是需要有 CA 机构能够提供 ACME 服务,能依据 ACME 标准接收证书申请和执行域名控制权验证,并签发 SSL 证书供 ACME 客户端下载部署。当然,这个用于签发 SSL 证书的根证书必须是预置四大浏览器信任的。

第二个就是 ACME 客户端,能承担 SSL 证书的申请,包括私钥和 CSR 生成,提交 CSR 到 ACME 服务端,证书签发后能及时取回并配置到 Web 服务器中启用使用。这个客户端最大

的难度是适配各种操作系统和 Web 服务器, 如果不是收费软件, 就只能发挥互联网公益精神, 让各路高手无私奉献了。还有就是必须取得用户的信任, 因为这个软件是安装在用户的 Web 服务器上的, 目前的解决方案是开源。

第三个就是密码中间件, 如常用的 OpenSSL, 这个非常重要, 能提供 HTTPS 加密所需的各种密码算法支持。

还有一个参与方就是浏览器了, 这个第四方虽然不直接参与 ACME 服务, 但是浏览器的密码算法支持和信任签发 CA 根证书都是离不开的重要元素。这也为何四大浏览器都在积极推动 ACME。

二、 打造国密 ACME 生态难在哪?

要想打造国密 ACME 生态, 当然也得参照国际 ACME 生态, 但是比国际生态还要难, 难在对应国际 ACME 生态的如下四个方面:

第一: 就是必须有 CA 机构提供常用国密浏览器信任的国密 SSL 证书和四大国际浏览器信任的国际 SSL 证书 ACME 服务, 国内能同时签发双算法 SSL 证书的 CA 机构屈指可数, 并且都还是传统的人工申请 SSL 证书的业务模式, 目前还没有国内 CA 机构可以提供国密 ACME 服务。

第二: 目前市场上没有可用的国密 ACME 客户端软件, 更不用提开源的了。为什么没有呢? 因为巧妇难为无米之炊, 没有第一个前提条件, 那来第二个要素。即使有热心人想开发, 也得有 ACME 服务可以对接才行。

第三: 由于常用 Web 服务器软件不支持国密算法, 所以国密 ACME 服务不能仅提供 ACME 客户端和 ACME 服务端, 还得提供 Web 服务器国密算法支持中间件。目前常用的有铜锁 SSL 和 openHiTLS。

第四: 目前支持国密算法的国密浏览器都是收费软件, 零信浏览器除外, 这也是我国普及国密 HTTPS 加密的一个最大的难点。

三、 零信技术明知道路艰险, 但仍坚持前行

零信技术在成立时就是定位成为密码应用自动化领导者, 第一个立项项目就是 SSL 证书自动化管理, 也就是要自己打造整个国密 ACME 生态产品, 因为求人不如求己。零信技术历时 4 年多打造完成的国密 ACME 全生态产品彻底解决了以上四大难题, 全球独家打造了国密 ACME 生态所需的三大产品:

第一：国密 ACME 服务：零信云 SSL 服务系统（含 ACME 服务系统）不仅对接了多家国际 CA 提供国际 SSL 证书 ACME 服务，而且对接了多家国内 CA 提供国密 SSL 证书 ACME 服务，自动化签发的双算法 SSL 证书全球信任和国密合规。

第二：国密 ACME 客户端：包括本次开源的免费的 SM2cerBot 软件和收费的国密 HTTPS 加密自动化网关，前者需要用户部署在自己 Web 服务器上，同时还需要自己部署国密算法支持中间件；后者是用户 Web 服务器零改造的解决方案，不仅解决了证书自动化难题，而且还解决了国密改造和后量子密码迁移难题。

第三：国密浏览器：零信浏览器是一个完全免费的、干净无广告的、支持国密算法、国际算法和后量子密码算法的通用浏览器，这彻底解决了普及国密 HTTPS 加密缺乏浏览器支持的难点。也正是由于好用并且免费，零信浏览器已经成为第一大市场份额的国密浏览器。

零信技术通过 4 年多的努力，已经完成了整个国密 ACME 生态所缺的所有产品，特别是这次免费提供国密 ACME 公共服务和开源国密 ACME 客户端，将为推动国密 ACME 服务的发展做出历史性的贡献，将加速我国普及应用商用密码算法实现 HTTPS 加密，不仅有力保障我国网空安全，而且为全球互联网安全提供了中国方案。

梦虽遥，追则能达；愿虽艰，持则可圆。零信技术愿通过免费国密 ACME 服务和开源国密 ACME 客户端携手业界同行一起为普及国密 HTTPS 加密做贡献。

王高华

2026 年 1 月 7 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 251 篇(共 73 万 9 千多字)和英文 110 篇(15 万 0 千多单词)。

