零信技术，双算法 SSL 证书自动化领导者

2026 年 2 月 4 日

昨天，零信技术发布了证书自动化重磅产品—免费国密 ACME 公共服务和开源国密 ACME 客户端，上线就收到的大量的关注。至此，零信技术终于正式完成了全系列双算法 SSL 证书自动化产品，历时 4 年多鼎力打造。本文讲一讲这些产品是如何打造出来的，分别服务哪些用户群，各自又有何独家特色，非常值得正在评估双算法 SSL 证书自动化解决方案的用户阅读并收藏。

一、 国际 SSL 证书自动化的成功经验非常值得学习和借鉴

国际 SSL 证书自动化之路**始于** 2015 年底由 Mozilla 牵头发起的 Let's Encrypt (简称 LE) 免费 SSL 证书自动化公共服务，**火于** 2019 年 3 月发布了 RFC 8555 ACME 国际标准之后，**普及于**国际云平台大厂的全面支持，特别是 CDN 厂商 Cloudflare 的率先默认免费支持 SSL 证书自动化配置使用。

这就是国际 SSL 证书自动化的发展历程，更是国际 SSL 证书自动化之路的成功经验，非常值得我国学习和借鉴。更具体一点，总结以下 3 点：

(1) 有牵头单位，领头羊，这个牵头单位是浏览器厂商

只有这样，才能让大家坚信这事能成，才能吸引更多的志同道合者参与，因为 SSL 证书是否可用取决于浏览器是否信任，浏览器才是主宰者。国际 SSL 证书自动化的领头羊是火狐浏览器的业主—Mozilla，并专门为此项目成立了一个独立的非盈利机构 ISRG。随后，谷歌浏览器鼎力支持，并也推出了自己的免费 SSL 证书自动化公共服务-GTS。

为何证书自动化这事是由浏览器发起，而不是 CA 机构呢？一方面这是要革 CA 的命，不可能由 CA 发起，很少有人愿意自己革自己的命。而浏览器是 SSL 证书消费者，早就不满意 CA 机构的不作为，这就是为何笔者连续多年参加了十几次 **CA/浏览器论坛** 国际会

议时只听到浏览器厂商的喋喋不休和 CA 们的默不做声的原因。Let's Encrypt 和 GTS 的推出，就是要革 CA 的命，他们成功了，取得了全球 SSL 证书市场第一和第二的地位，分别占 49%和 14%的市场份额。

(2) 有国际标准，标准制定单位当然必须是领头者

LE 从 2015 年底推出免费 SSL 证书自动化公共服务，到 2018 年就已经成为了全球第一大 CA，可见用户是何等的喜欢证书自动化和免费 SSL 证书。因为全球用户已苦人工管理证书太久了—长达 20 多年，一旦有人提供证书自动化服务，那就是星星之火即刻燎原！

值得敬佩的是：LE 已经火到了全球第一市场份额，但是并没有独家享受这个成功成果，也并没有申请什么专利保护，而是基于自己的丰富的证书自动化实践经验联合相关单位共同制定了 RFC8555 ACME 国际标准，让全球业界都可以依据这个标准来普及 SSL 证书自动化。这个标准的制定是全球普及 SSL 证书自动化的根本，其结果是现在 90%以上的 SSL 证书都是自动化签发和部署的。制定标准功不可没！

(3) 有生态支持，必须有 SSL 证书生态各方的共同参与

有了国际标准，大家就可以依据标准来实现各种云服务的 SSL 证书自动化了。率先实现 SSL 证书自动化的是国际云服务大厂，如亚马逊云、微软云、谷歌云等，还有 CDN 服务商，如 Cloudflare、Akamai、Fastly 等，还有网安厂商，如思科、F5、Citrix 等。有意思的是：全球第一、第二、第三大 CA 机构并没有积极参与，甚至极力阻止缩短 SSL 证书有效期国际标准的落地。云厂商和 CDN 厂商只好从 CA 机构定制中级根证书并利用 CA 机构传统 API 实现证书自动化签发，这使得 CA 机构的市场份额从原先的第 1 和第 2 位降到了现在第 5 和第 8 位。

也就是说，与 SSL 证书应用生态相关的各方共同依据标准来为用户提供各种云服务、网络设备的证书自动化服务，这样才能实现 SSL 证书从 2016 年的 2 亿多张增长到现在 13 亿多张，其中 LE 从 2015 年底的零开始到现在 6 亿多张。这就是全生态支持证书自动化的威力。

二、 我国 SSL 证书自动化之路注定不同于国际证书自动化之路

我国 SSL 证书自动化之路当然必须借鉴国际证书自动化之路，但又有不同，相同的是也必须有一样的 3 个实现路径，不同的是必须是双算法 SSL 证书同时实现自动化，并且 Web 服

务器还得改造支持国密算法。同样可以总结以下 3 点：

(1) 同样必须有牵头单位，这个牵头单位是浏览器厂商、CA 机构或云平台厂商

对比国际 SSL 证书自动化之路是由浏览器厂商牵头的，国密证书自动化之路的确也是浏览器厂商—零信技术率先提出双算法 SSL 证书自动化相关产品和解决方案。鉴于我国的特殊市场情况，如果是 CA 机构或云平台厂商牵头，可能更容易普及国密 SSL 证书自动化。

(2) 同样必须有标准，国密标准，标准制定单位当然必须是领头者

对比国际 SSL 证书自动化之路的成功经验是制定标准，但是 ACME 国际标准只能解决国际算法 SSL 证书自动化问题，无法解决我国的双证书自动化难题。所幸的是：国家密码行业标准化技术委员会于 2023 年批准了由零信技术牵头联合多家 CA 机构和互联网公司立项制定《自动化证书管理规范》密码行业标准 GM/T，估计今年能完成标准发布工作。

(3) 同样必须有生态支持，有国密 SSL 证书生态各方的共同参与

对比国际 SSL 证书自动化之路的成功经验是全生态相关厂商的积极参与，国密 SSL 证书自动化就没有这么幸运，虽然早就参考国际 ACME 标准发布了国密 ACME 标准草案，但是到目前为止仅零信技术全系列产品支持，这是我国普及国密 SSL 证书自动化的最大问题—缺乏全生态支持。

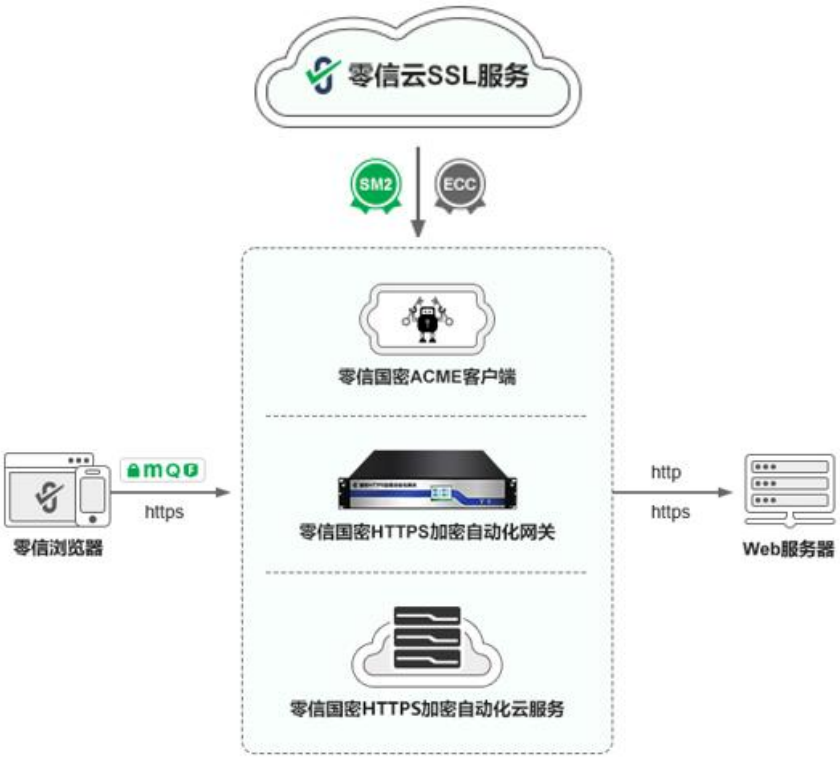
我国应该参考国际 SSL 证书自动化生态，各大云平台、各 CDN 服务商、各 CA 机构、各网安厂商都应该积极参与国密 SSL 证书自动化生态建设中，为用户提供双算法 SSL 证书自动化服务。只有这样才能真正普及国密 SSL 证书来保障我国网空安全。

三、 零信技术成功打造完整的全栈 SSL 证书自动化生态体系

零信技术从成立开始就定位为密码应用自动化技术提供商，首个解决方案就是双算法 SSL 证书自动化解决方案，历时 4 年多已经成功打造了三位一体、端云融合的全栈 SSL 证书自动化生态体系，满足不同用户的双算法 SSL 证书自动化需求。

第一个解决方案是参考国际 SSL 证书自动化的解决方案，基于国密 ACME 客户端的开源赋能方案，不仅提供开源国密 ACME 客户端软件，同时提供完全免费的国密 ACME 证书公共服务。不仅让用户可以免费使用双算法 SSL 证书自动化服务，而且让有开发能力的用户基于

国密 ACME 公共服务实现各种业务系统和各种设备的双算法 SSL 证书自动化。零信技术从一个技术提供者脱变为 SSL 证书自动化生态的构建者和标准落地应用推动者。



第二个解决方案是参考国际 SSL 证书自动化生态中云厂商和 CDN 服务商的经验，为国内 CDN 服务提供基于 CDN API 的“补丁式”双算法 SSL 证书自动化服务和与 CDN 厂商深度合作提供“原生融合”方案。这是最经济的实现 SSL 证书自动化规模化落地应用的最佳解决方案，避免了数百万互联网业务主体为证书自动化改造而“重复造轮子”，将证书自动化能力变成一项普惠服务。零信技术从一个技术提供者脱变为一个销售“永续安全状态”的互联网安全服务提供商和标准落地应用推动者。

第三个解决方案是参考国际 SSL 证书自动化生态中网安厂商的经验，为政府、金融等关键信息基础设施单位打造了一个硬件产品—零信 HTTPS 加密自动化网关，这是一个软硬件一体化的 SSL 证书自动化管理中台，它超越了简单的证书自动化管理，深度融合国际密码和国密算法硬件加速、后量子密码算法的平滑迁移能力、WAF 防护能力，以及多站点、多设备的集群化 SSL 证书统一管控能力。不仅可以为 Web 服务器提供双算法 SSL 证书自动化服务，而且还可以为其他需要 SSL 证书的网络设备和云服务提供双算法 SSL 证书自动化服务。零信技术不仅是在实践 SSL 证书生态的全面自动化，更在参与定义未来关键信息基础设施的安全架构规范。

四、 唯有证书自动化才能真正保障网络安全和数据安全

零信技术通过端云一体技术路线，成功实现了 SSL 证书自动化的三大技术方案：ACME 证书公共服务和客户端开源赋能、CDN 服务的 API 方式和原生融合、硬件网关的纵深守护和全局管控，共同构成了零信技术问鼎 SSL 证书自动化领导地位的坚实基座。

唯有证书自动化才能顺利完成国密改造和后量子密码迁移，才能真正保障我国网络安全和数据安全。零信技术通过“三位一体”SSL 证书自动化解决方案的扎实推进，必将在这场由自动化驱动的深刻密码技术革命中，成为 SSL 证书自动化市场的领导者，更将成为密码应用自动化时代的定义者与引路者。零信技术正在引领一个全栈可信、全程自动、全域智能的数字新时代。

王高华

2026 年 2 月 4 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 261 篇(共 76 万 4 千多字)和英文 116 篇(15 万 9 千多单词)。