CDN 技术差距正在拉大，未来三年或决定生死

2026 年 1 月 26 日

零信技术与国内主流云平台对接基于 CDN API 的“双算法 SSL 证书自动化订阅服务”的过程中，看到了一个令人担忧的趋势：中国 CDN 服务与国际先进水平的技术差距，正在从“**跟随**”变为“**代差**”。这不是危言耸听，而是数据与事实的冷酷陈述。这种差距将直接决定谁能赢得政企核心客户，谁能成为下一代互联网基础设施领导者。

一、我们错过了什么？一场正在发生的技术革命

当前我国互联网正面临两场并行的密码技术革命：

(1) 第一场革命：国密算法从“可选”到“必选”。

随着网信办等四部委文件《互联网政务应用安全管理规定》的发布，国密算法 HTTPS 加密已成为所有服务政务系统的 CDN 服务的强制合规要求。政务市场，恰恰是 CDN 服务最稳定、最核心的收入来源之一。然而，我们的调研显示，目前仅有少数几个 CDN 服务商支持国密 SSL 证书 API 上传，支持国密 HTTPS 加密加速。

这意味着什么？意味着大多数 CDN 服务商，正在主动放弃一个由政策驱动的、确定性增长的千亿级市场。这不仅是技术能力的缺失，更是市场战略的误判。

(2) 第二场革命：后量子密码（PQC）从“未来时”进入“现在时”。

当中国 CDN 行业还在为 TLS 1.2 和传统国密算法支持而努力时，国际巨头已经奔向了下一个赛道—TLS 1.3+PQC。Cloudflare 于 2025 年 3 月宣布，在先前免费支持 SSL 证书自动化管理的基础上，再免费为所有 CDN 用户自动升级至支持混合 PQC 密码算法(X25519MLKEM768)HTTPS 加密。这一举动看似激进，实则深远：它意味着全球互联网流量的安全基线被瞬间抬高。

据第三方监测数据，截至 2025 年底，全球已有超过 **58%**的互联网流量受到 PQC 加密保护。国际 CDN 服务巨头们如 Cloudflare、Akamai、AWS(亚马逊)、Fastly 等均已全面支持 PQC 算法。美国、英国等政务 CDN 系统都已纷纷支持 PQC 算法。

而我国没有一个 CDN 服务支持 PQC 算法 HTTPS 加密，我们错过的不只是一项技术，而

是一个时代的安全标准定义权。量子计算机的威胁虽未降临，但已经存在“先收集后解密”安全威胁，这是国际 CDN 厂商快速支持后量子密码的根本原因。我国 CDN 服务如果现在不能马上布局支持，五年后 CDN 服务的所有政务数据、金融数据、商业数据等，将在量子计算面前成为明文，危及我国互联网安全甚至国家安全。

二、细节处的魔鬼：四大技术差距的深层解读

对比国际 CDN 服务，我国 CDN 服务正在从“跟随”变为“代差”，这不是危言耸听，而是事实陈述。主要体现在如下 4 个方面。

(1) 国密支持：“浅尝辄止”与“深度集成”的差距

支持国密算法的 CDN 大多停留在“可以上传国密 SSL 证书”的初级阶段。而真正用户需要的技术实现是将国密算法深度集成到 CDN 的每一个环节：

- **性能损耗**：国密 SM2 算法在相同安全强度下，性能优化是关键。国际服务商在硬件加速、协议栈优化上投入巨大，而国内多数方案性能损耗明显，用户体验极差。
- **协议兼容**：支持国密算法的 TLS 1.3 协议，是实现高性能国密 HTTPS 加密的基石。很遗憾，目前国内尚无 CDN 服务公开宣布支持，这导致国密应用无法享受 TLS 1.3 带来的大幅速度提升。
- **生态兼容**：浏览器、操作系统、中间件的国密适配也是短板，一个环节的“短板”就会导致整个生态链路失效。试想一下：如果国产操作系统真正支持国产密码算法，那还有“国密改造”这个词吗？再反问一下：既然是国产操作系统为何就不能原生支持国产密码算法呢？

(2) 证书管理：“手工时代”与“自动时代”的差距

SSL 证书的有效期马上(3 月 15 日)就要缩短为 200 天，并将进一步缩短为 47 天，Let’s Encrypt 上周宣布支持自动化签发 6 天有效期的 SSL 证书，这意味着将来国际标准极有可能缩短 SSL 证书有效期到 10 天。对于管理着数十万甚至百万域名的 CDN 平台而言，让用户每几天就手工上传更新证书，这是不能承受的巨大的运营负担和致命的安全风险（证书过期导致网站瘫痪）。

- **国际标准**：ACME 协议已成为证书自动化的全球标准，Cloudflare 等提供的自动化证书管理（包括自动申请、部署、续期、更换）完全免费。这不仅是一项功能，更是其吸引海量中小客户、构建生态壁垒的核心手段，也是其拿到全球 CDN 市场份额的杀手

锏。

- **国内现状**：虽然国密 ACME 标准草案也已经发布(零信技术牵头制定)，但是调研结果是：无一支持国际 ACME 标准，更不提国密 ACME 标准了。CDN 服务的每次证书更新，都需要客户先向 CA 申请证书，人工上传证书、启用 HTTPS 加密。这种低效模式，如何应对不断缩短的证书有效期？如何服务未来海量的物联网设备、边缘计算节点？

（3）后量子密码："集体失语"与"引领标准"的差距

这是最令人焦虑的差距，因为它关乎未来十年我国互联网的整体安全水平。

- **混合模式是唯一路径**：从传统密码算法迁移到 PQC 算法，必须经历一个漫长的"混合算法加密"阶段，即同时使用传统算法和 PQC 算法，确保双重安全和平滑迁移。

- **中国不能只有"国际混合"**：国际通用的 X25519MLKEM768 混合 PQC 算法我国必须支持，以融入全球互联网。但更重要的是，我们必须发展并推广已经获批 IANA 编号的国密混合 PQC 算法(SM2MLKEM768)。这不仅仅是赶紧为国密生态续命，更是在量子时代争夺国际话语权的战略之举。而现状是，我国 CDN 服务在这两条 PQC 技术路线上均为空白。

（4）服务理念："功能堆砌"与"安全即服务"的差距

国际领先 CDN 服务已将"安全"作为其服务的默认属性和核心卖点。HTTPS 加密、证书自动化管理、PQC 迁移、DDoS 防护、WAF 防护等被打包成一套无缝的"安全即服务"。

- **政务级标杆**：美、英等国建设的政务专用 CDN，默认支持混合 PQC 加密和 WAF 防护，为关基系统提供"交钥匙"的安全加速方案。

- **我们的反思**：国内 CDN 服务商是否还停留在"加速为主，安全为附加卖点"的旧模式？能否能为我国智慧政务、关基系统提供对标国际同行的一体化、合规化深度融合密码的安全加速解决方案？

三、零信技术合作倡议

既然看到差距，就应马上行动。零信技术历时四年，投入研发，成功打造了端云一体的**"双算法 SSL 证书自动化管理全生态解决方案"**，而"基于 CDN 服务的双算法 SSL 证书自动化订阅服务"就是这个生态的关键一环。

零信技术做到了什么？

(1) **一站式双算法支持：**打通了从国际 RSA/ECC 算法到国密 SM2 算法，再到国际混合 PQC 算法（X25519MLKEM768）和国密混合 PQC 算法（SM2MLKEM768）的全栈密码体系。

(2) **自动化无缝集成：**通过与各大云平台 API 对接，用户可以实现一键订阅、自动部署、全生命周期管理。证书申请、验证、部署、续期、算法轮转全部自动化，零人工干预。

(3) **助力合规与前瞻：**不仅帮助客户满足当下的国密合规要求，更通过双端(零信浏览器和零信 HTTPS 加密自动化网关)内置的混合 PQC 能力，为客户的“后量子密码迁移”铺平道路，实现“现在合规，未来安全”，并且同时满足国密合规和后量子密码迁移应用要求。

但这远远不够！

零信技术的证书自动化订阅服务目前仍然需要用户在 CDN 控制台进行配置。这只是一个“外挂式”的补丁方案，无法发挥最大的效能和最好的用户体验。我国 CDN 服务需要的不是外部的“拐杖”，而是自身骨骼和肌肉的强健，需要原生自动化！另外，这种“外挂式”服务仅提供了双算法 SSL 证书自动化服务，国密算法和 PQC 算法还需要 CDN 服务系统支持才行。

因此，**零信技术发出最诚挚的合作倡议：**

零信技术愿意开放密码技术核心能力，与国内有远见的 CDN 服务商进行深度技术融合与战略合作，共同打造下一代安全加速平台。

(1) **原生集成方案：**将零信技术的双算法 SSL 证书自动化引擎，以 SDK 或模块形式，深度嵌入 CDN 系统的核心管理平台。让 CDN 服务商能为其用户提供原生的、无感的

“双算法证书自动化”服务，作为基础功能或增值服务。

(2) **联合产品研发**：针对政务、金融等关键行业，共同开发**“**国密合规与后量子密码就绪”的一体化 CDN 安全加速产品，满足最高等级的安全合规监管要求。

(3) **标准共建与推广**：共同推动国密混合 PQC 算法（SM2MLKEM768） 在行业内的落地应用，参考 RFC 国际标准，共同参与国家标准制定，构建中国自主的量子安全 HTTPS 加密应用生态。

对零信技术而言，技术开放带来的生态价值，远大于封闭的短期利益。零信技术的使命是“**推动密码技术普惠，守护数字世界安全**”，而 CDN 服务正是密码技术最广泛、最重要的应用场景之一。还有云 WAF 服务，也是必须原生支持 SSL 证书自动化、国密算法和后量子密码算法的云服务。

四、市场不会等待，未来三年是窗口期

CDN 市场正在分化，客户正在用脚投票、能否在激烈的市场竞争中胜出，CDN 服务提供商必须针对不同的客户群体拿出切实解决用户痛点的解决方案。

(1) **政务客户**：合规是红线，无法满足国密合规和未来 PQC 要求的服务商，将被直接排除在采购清单之外。

(2) **金融与央企客户**：对安全性、前瞻性的要求最高，它们必然会选择技术最领先、最能保障其数据“长期安全”的 CDN 服务商。

(3) **出海企业客户**：它们需要同时满足中国合规与全球标准，只有能提供“双 PQC 算法双合规”能力的 CDN，才能成为其首选。

(4) **高成长科技企业**：它们生于云时代，天然接受“自动化”、“零运维”、“默认安全”的理念，陈旧复杂的操作界面和安全配置，会被它们毫不犹豫地抛弃。

技术差距，最终都会体现在财务报表上，体现在市场份额上，体现在生死存亡上。未来三年，是我国 CDN 服务提供商补齐短板、换道超车的最后窗口期。一旦国际巨头凭借其技术、体验和生态优势，在高价值市场形成事实标准，再想追赶将难上加难。

五、并肩前行，共赴未来

零信技术深知，每一家 CDN 服务商都拥有一流的网络资源、调度能力和客户基础。而零

信技术所擅长的是密码技术的深度应用、证书自动化体系的构建以及对密码合规与未来趋势的洞察。

让我们将各自的优势结合起来：

- 您的**规模与节点** + 零信技术的**密码与自动化** = 构建技术壁垒
- 您的**市场与客户** + 零信技术的**合规与前瞻** = 赢得高端市场
- 您的**工程与运维** + 零信技术的**算法与协议** = 定义未来标准

提升 CDN 安全服务能力，不是为了应对法律法规的合规检查，而是为了赢得下一个十年。向国际巨头学习，不是为了模仿，而是为了超越。零信技术已准备好最详尽的技术方案、最开放的合作态度和最灵活的商务模式，期待与有远见、有魄力的 CDN 领导者对话。

让我们携手，不再谈论差距，而是共同定义下一代中国互联网安全加速服务的新高度。

王高华

2026 年 1 月 26 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 260 篇(共 76 万 1 千多字)和英文 115 篇(15 万 7 千多单词)。