双混合 PQC 算法 HTTPS 加密产品提前交付

2025 年 12 月 12 日

零信技术于 2025 年 8 月 8 日发布了后量子密码 HTTPS 加密全生态产品就绪时间表，计划：2025 年 12 月，零信浏览器和零信网关支持 ECC+MLKEM 和 SM2+MLKEM 双算法混合密钥封装机制，实现混合 PQC 算法 HTTPS 加密。这个计划提前完成并于今天交付使用，充分展示了零信技术在后量子密码领域的前瞻研究能力和产品落地能力，为我国早日启用商密后量子密码 HTTPS 加密保障关基系统安全提供了有力的技术支撑和普及应用支持，同时也为全球互联网提供了更多的混合 PQC 算法迁移方案，增强了 TLS 生态的韧性和安全性。

一、 提前交付的两个核心 PQC 产品是什么？

混合 PQC 算法 HTTPS 加密的两个核心产品是零信浏览器和零信 HTTPS 加密自动化网关，零信浏览器是混合 PQC 算法 HTTPS 加密的客户端，零信 HTTPS 加密自动化网关是混合 PQC 算法 HTTPS 加密的服务端，两端无缝实现了原 Web 服务器零改造的混合 PQC 算法 HTTPS 加密应用。

用户只需升级零信浏览器到 V2601 版本即可，已部署零信 HTTPS 加密自动化网关的用户也只需升级系统软件即可支持，完全免费支持双混合 PQC 算法 HTTPS 加密，满足用户后量子密码迁移的应用需要。这就是零信技术打造后量子密码 HTTPS 加密全生态产品的独特优势。

二、 混合 PQC 算法实现 HTTPS 加密为何非常重要?

全球互联网流量中已经 97%流量实现了 HTTPS 加密，中国大陆流量也已有 84%流量实现了 HTTPS 加密，但是这些流量以前都是采用传统密码算法如 RSA/ECC/SM2 算法实现 HTTPS 加密，未来的量子计算机可以轻松破解这些加密，为了防止“先收集后解密”的数据安全威胁，所以，全球互联网已经有 51%流量实现了混合 PQC 算法 HTTPS 加密，以确保 HTTPS 加密流量在量子时代的持续安全。

所谓混合 PQC 算法就是在 HTTPS 加密实现过程的密钥封装阶段采用传统密码算法和后量子密码算法混合来保护共享密钥，工作原理是在 HTTPS 握手时，并行使用传统密码算法（ECC 或 SM2）和 PQC 算法（MLKEM），笔者称之为“混密”模式，这是非常有战略智慧的解决方案，一是可以实现风险对冲，即使 PQC 算法未来发现漏洞，传统密码算法依然有效；二是可以实现平稳过渡，确保与旧系统的兼容，极大降低 PQC 迁移风险；三是提供了务实 PQC 迁移路径， 体现了从当前走向未来的稳健策略，降低了采用 PQC 的技术门槛和不确定性，使快速部署成为可能。

三、 零信技术混合 PQC 算法 HTTPS 加密的创新点有哪些?

全球目前已经实现的混合 PQC 算法是采用 X25519MLKEM768 算法，零信技术创新解决

方案是默认双端产品支持双混合 PQC 算法。全球独家具有如下 6 大技术创新点：

(1) 不仅支持国际算法混合算法 X25519MLKEM768，而且全球独家率先支持国密算法混合算法 SM2MLKEM768。

(2) 不仅仅是支持 SM2MLKEM768 算法，而且联合阿里铜锁 SSL 开源项目组队一起成功向国际组织 IANA 申请了 TLS 支持组协议编号-4590，使得 SM2MLKEM768 正式成为国际标准 TLS 协议组的四个后量子密码混合协议之一，这是拿到了普及应用 SM2MLKEM768 混合 PQC 算法的全球通行证。

(3) 不仅是零信浏览器支持 SM2MLKEM768 算法，而且服务端产品-零信 HTTPS 加密自动化网关也同时支持 SM2MLKEM768 算法，用户提供了一站式解决方案，而无需寻找多家供应商的支持。

(4) 零信浏览器和零信 HTTPS 加密自动化网关支持 SM2MLKEM768 的基础是依据 RFC 8998 (TLS 1.3 协议商用密码套件)支持 TLS 1.3 协议使用商密 SSL 证书和商用密码算法实现 HTTPS 加密，全球率先支持使用 TLS 1.3 协议在密钥交换中同时支持 SM2 算法和商密混合 PQC 算法 SM2MLKEM768。

(5) 不仅实现了混合 PQC 算法 HTTPS 加密，零信 HTTPS 加密自动化网关通过协同零信云 SSL 服务系统实现 HTTPS 加密必须的双算法(ECC+SM2) SSL 证书自动化管理，这也是全球独家一站式解决方案，不仅仅是提供了 PQC 网关或 PQC 浏览器。

(6) 不仅仅是 HTTPS 加密的混合 PQC 算法支持，而且是 HTTPS+WAF 防护的混合 PQC 算法支持，全球独家率先为用户提供一站式 HTTPS 加密和 WAF 防护的商密合规和 PQC 迁移解决方案。

四、 预计下一步 PQC 生态产品就绪时间还会提前

上述实现的混合 PQC 算法是在 HTTPS 加密握手过程中实现的密钥封装混合算法保护共享密钥，实现 HTTPS 加密所采用的 SSL 证书仍然是传统密码算法(RSA/ECC/SM2) SSL 证书。根据零信技术于 2025 年 8 月 8 日发布了后量子密码 HTTPS 加密全生态产品就绪时间表，下一个 PQC 产品就是在 2026 年 9 月份实现签发 PQC 混合算法 SSL 证书和支持混合算法 SSL 证书实现 PQC 算法 HTTPS 加密。

笔者预计有两种情况发生：一是依然提前实现并交付用户，二是此阶段可能会直接跳过，直接进入再下一个阶段—签发纯 PQC 算法 SSL 证书和支持纯 PQC 算法 SSL 证书实现 HTTPS 加密，这是一个关系到全球 Web PKI 生态从传统密码算法根证书到混合 PQC 算法根证书再到纯 PQC 算法根证书的迁移路线的大课题，笔者正在积极参与相关话题的国际讨论中，零信技术会根据全球 Web PKI 业界共识第一时间适时发布最新的下一步 PQC 生态产品，敬请持续关注零信技术动态。

王高华

2025 年 12 月 12 日于深圳
