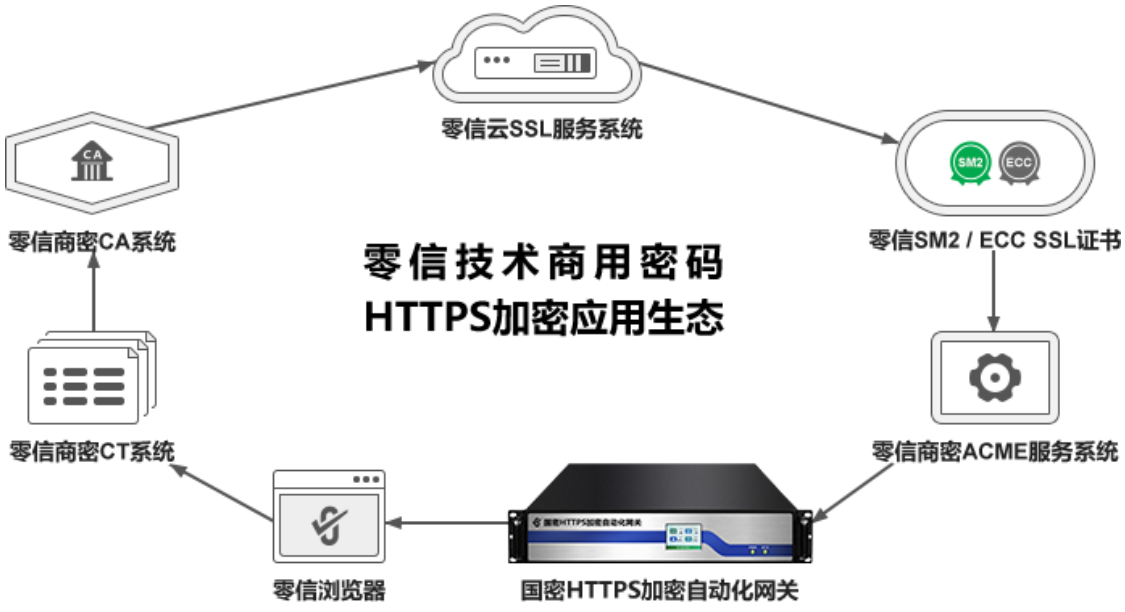
打造后量子密码 HTTPS 加密应用生态

零信技术今天发布了《后量子密码 HTTPS 加密全生态产品就绪时间表》的新闻，本文详细讲一讲这个全生态产品的更详细的内容，以帮助用户了解后量子密码 HTTPS 加密技术，并充分理解只有现在实现了双算法 SSL 证书的自动化管理才能确保将来实现后量子密码 HTTPS 加密的无缝升级，两者是密切相关的。

一、 传统密码 HTTPS 加密应用生态简介

零信技术历时 4 年打造了国密证书自动化管理生态和国密证书透明生态，这两个生态产品实现了双算法(SM2/ECC) SSL 证书的自动化管理，也就是打造了传统密码 HTTPS 加密应用生态，这个生态至少包括 7 大产品：国际 RSA/ECC 算法 SSL 证书和商密 SM2 算法 SSL 证书通过零信云 SSL 服务系统对接多家国际 CA 和多家商密 CA 实现多通道自动化签发，零信商密 CA 系统负责签发双算法(RSA/SM2)内网 SSL 证书，零信商密 CT 系统则是为 CA 机构签发商密 SSL 证书提供商用密码算法证书透明日志服务的 CT 系统，零信商密 ACME 服务系统为零信国密 HTTPS 加密自动化网关提供双算法 SSL 证书自动化证书申请和证书下发服务，零信国密 HTTPS 加密自动化网关则是一个通过商用密码产品认证的内置 ACME 客户端、集 https 加密加速、https 卸载转发、商密算法模块、WAF 防护、负载均衡、双向认证等多项功能于一体的专用于 Web 网站系统 https 加密的硬件网关产品，零信浏览器则是一个完全免费的、干净无广告的、从底层同时支持 RSA/ECC/SM2 三算法的和支持国际和商密证书透明的通用浏览器。

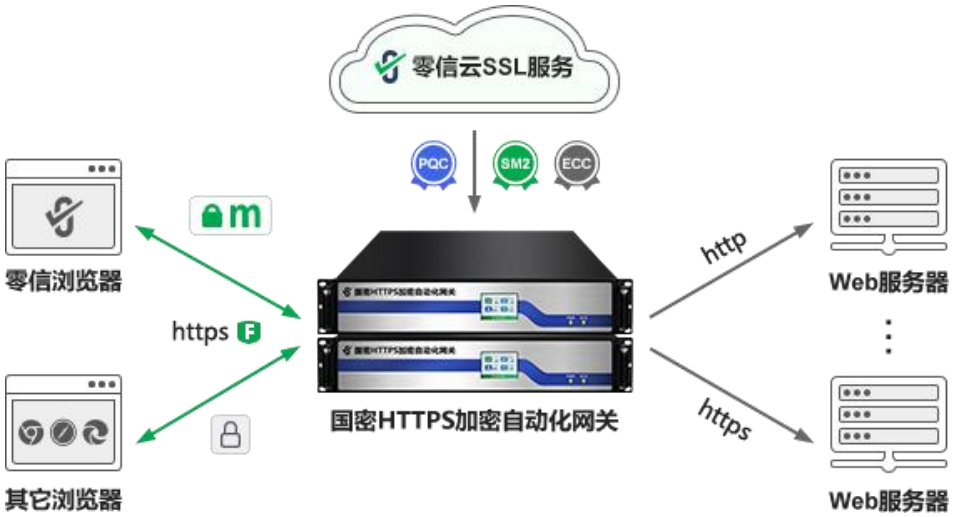


零信技术打造的商密 HTTPS 加密应用生态全系列产品构成了一个端云一体的原 Web 服务器零改造的双算法 SSL 证书自动化管理解决方案，零信浏览器安装在最终用户电脑上，零信国密 HTTPS 加密自动化网关部署在用户机房的 Web 服务器前面，自动化实现自适应密码算法的 HTTPS 加密和 WAF 防护，自动化配置的 SSL 证书已经提前实现 90 天有效期，并在 2028 年 12 月之前实现 47 天有效期，提前满足国际标准不断缩短 SSL 证书有效期的合规要求。

二、 后量子密码 HTTPS 加密应用生态简介

后量子密码 HTTPS 加密应用生态是零信技术专为 HTTPS 加密从传统密码顺利迁移到后量子密码正在鼎力打造的又一个生态，这个生态至少包括 7 大产品：零信 PQC 密码机(HSM)及在此密码机中生成的 PQC 算法根证书，国际 ECC 算法+MLDSA 混合算法 SSL 证书、商密 SM2 算法+MLDSA 混合算法 SSL 证书、纯 PQC 算法 SSL 证书都是由零信 PQC CA 系统签发，零信 PQC CT 系统为 CA 机构签发 PQC SSL 证书提供 PQC 算法证书透明日志服务，零信 PQC ACME 系统为零信国密 HTTPS 加密自动化网关提供双算法 SSL 证书自动化证书申请和证书下发服务，零信国密 HTTPS 加密自动化网关提供支持 ECC+MLKEM 和 SM2+MLKEM 混合 PQC 算法和纯 PQC 算法的 HTTPS 加密和 WAF 防护服务，零信浏览器则是同时支持 ECC / SM2 / ECC+MLKEM / SM2+MLKEM / MLDSA+MLKEM 等多种密码算法和支持 PQC 算法证书透明的通用浏览器。

零信技术打造的后量子密码 HTTPS 加密应用生态全系列产品构成了一个端云一体的原 Web 服务器零改造的多算法(ECC/SM2/PQC) SSL 证书自动化管理解决方案，零信浏览器安装在最终用户电脑上，零信国密 HTTPS 加密自动化网关部署在用户机房的 Web 服务器前面，自动化实现自适应密码算法的 HTTPS 加密和 WAF 防护，自动化配置的传统算法 SSL 证书和 PQC 算法 SSL 证书为 47 天有效期证书，用户只需自动升级零信浏览器支持 PQC 算法，部署在用户机房的零信网关会自动升级支持 PQC 算法，使得用户系统无感地无缝迁移到后量子密码，完全免费升级支持后量子密码，用户无需再为后量子密码迁移费钱费心费力费事。



三、 后量子密码 HTTPS 加密全生态产品就绪时间表

零信技术根据国际共识的后量子密码迁移时间表制定了后量子密码 HTTPS 加密应用全生态产品就绪时间表，具体如下图所示，分 7 步完成。

具体每个阶段的产品就绪情况如下：

(1) 到 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。

(2) 到 2026 年 3 月，零信 CA 创建 ECC+MLDSA 和 SM2+MLDSA 双算法混合根证书和中级根证书，用于签发 PQC 混合算法 SSL 证书。

(3) 到 2026 年 9 月，零信浏览器和零信网关支持双算法 PQC 混合算法 SSL 证书自适应 4 种算法实现 PQC 算法 HTTPS 加密。

(4) 到 2026 年 12 月，零信 CA 创建纯 PQC 算法(MLDSA)根证书和中级根证书，用于签发纯 PQC 算法 SSL 证书。

(5) 到 2027 年 7 月，零信浏览器和零信网关支持纯 PQC 算法 SSL 证书实现 PQC 算法 HTTPS 加密。

(6) 到 2028 年 12 月，零信浏览器和零信网关支持国产 PQC 算法 SSL 证书实现国产 PQC 算法 HTTPS 加密。

(7) 到 2029 年 12 月，零信技术完成打造 HTTPS 加密 PQC 算法全生态产品，支持国际/国产 PQC 算法，助力用户实现无缝 PQC HTTPS 加密迁移。

四、 只有实现了 SSL 证书自动化管理才能无缝迁移到后量子密码 HTTPS 加密

从零信技术正在打造的后量子密码 HTTPS 加密应用生态简介可以看出，要想实现无缝顺利迁移到后量子密码 HTTPS 加密，必须先实现双算法 SSL 证书自动化管理，这就是谷歌在在“一起面向未来”计划中列出的实现 SSL 证书自动化管理的六大好处之一是“轻松过渡到抗量子算法”。

从零信技术后量子密码 HTTPS 加密应用全生态产品就绪时间表可以看出，所有工作都是零信技术在云端部署完成，实现为部署在用户端的零信国密 HTTPS 加密自动化网关自动化签发每个阶段所需的 PQC 混合算法 SSL 证书和纯 PQC 算法 SSL 证书，这是一个端云一体的解决方案，也是零信技术打造全生态产品的独特优势所在，用户无需寻求多家供应商的支持，只需现在就开始实现双算法 SSL 证书自动化管理，微改造部署零信国密 HTTPS 加密自动化网关，到时候就可以自动化实现后量子密码 HTTPS 加密，轻松完成 HTTPS 加密向后量子密码迁移，切实保障所有业务系统的不间断的 HTTPS 加密安全。

所有用户都必须现在马上行动起来，尽快完成 SSL 证书自动化管理技术革命，为无缝迁移到后量子密码 HTTPS 加密做好技术准备。

王高华

2025 年 8 月 8 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 223 篇(共 66 万 6 千多字)和英文 98 篇(13 万 3 千多单词)。