一次技改完成两次 HTTPS 加密技术革命

HTTPS 加密技术是浏览器厂商 Netscape 于 1994 年发明的，使用 SSL 证书实现从浏览器到服务端的数据传输加密。这是一个革命性的发明创造，使得明文 HTTP 互联网成为了密文 HTTPS 互联网，才使得互联网有了商用价值，使得实验室的互联网技术在全球范围得到了普及使用，才有了今天人们已经离不开的互联网服务。这个技术在 31 年后今天即将迎来一次技术革命—缩短 SSL 证书有效期，彻底从人工申请和部署 SSL 证书变革为自动化申请和部署，这个技术革命的目的是为了迎接下一个真正的技术革命—后量子密码 HTTPS 加密。两次技术革命都需要系统升级改造，这是逃不过的改造，本文讨论是否有可行的技术方案能把这两次技术革命升级改造一次搞定。

一、 SSL 证书从人工管理到自动化管理的技术革命

SSL 证书从诞生到现在都是由浏览器信任的 CA 机构为用户签发 SSL 证书，用户拿到证书后手动在 Web 服务器或网关设备上部署 SSL 证书，再启用 HTTPS 加密，保障网站数据传输安全，这个业务流程 31 年了一直没有变。但是，在万物互联的今天，互联的万物都需要实现 HTTPS 加密，就无法由人工来完成 SSL 证书申请和部署了，这就需要一次技术革命。

其实，这个技术革命早在 2015 年就开始了，这就是由 Mozilla 牵头发起 Let's Encrypt 自动化签发和部署 SSL 证书，并于 2019 年发表了 RFC 8555 自动化证书管理环境(ACME)国际标准，在全球范围得到了积极响应并大量实施，目前全球 11 亿张有效 SSL 证书中已有 8 亿张 SSL 证书都是自动化签发和部署的，有力保障了全球万物互联的数据传输安全。而在 2015 年全球有效 SSL 证书只有两百多万张，十年时间 SSL 证书签发量翻了 550 倍，这就是自动化的威力。

既然这个技术革命早就开始了，为何笔者又说这次技术革命即将到来呢？因为即使已经有 80%以上的 HTTPS 加密都已经实现了 SSL 证书自动化管理，但这不是强制项，人们还在习惯 31 年已经形成的习惯人工申请和部署 SSL 证书，严重阻碍了 SSL 证书的普及应用，这就需要革命！

谷歌早在 2023 年 3 月 3 日就发布了"Move Forward, Together"(一起面向未来)的革命计划—强制缩短 SSL 证书有效期为 90 天，全面拥抱 SSL 证书自动化管理，这就是要革传统 SSL 证

书人工管理的命。但是，就像任何革命一定会遭遇反对一样，这场技术革命遭到了 CA 机构和用户的反对，导致了这场革命直到 2024 年 5 月 16 日才有了成功的眉目—分步缩短 SSL 证书有效期的国际标准的制定，这是一个各方妥协的革命，分三步完成：2026 年 3 月 15 日缩短 SSL 证书有效期为 200 天，2027 年 3 月 15 日为 100 天，2029 年 3 月 15 日为 47 天。

也就是说，这次的技术革命到来时间是明年 3 月 15 日，这场即将到来的 HTTPS 加密技术革命的目的是要实现 SSL 证书自动化管理，从传统的人工管理革命为自动化管理。这就要求 SSL 证书用户采取合适的技术措施完成系统升级改造，实现 SSL 证书自动化管理。而我国则需要实现双算法(RSA/SM2)SSL 证书的自动化管理，同时完成系统国密改造以支持 SM2 国密算法，实现自适应密码算法的 HTTPS 加密自动化。

二、 HTTPS 加密从传统密码到抗量子密码的技术革命

为了应对将来的量子计算可能会秒破现在正在使用密码算法，需要新的抗量子密码算法，这些算法可以保护数据免遭使用当前传统计算机和未来的量子计算机发起的攻击。这些算法就是后量子密码(Post-Quantum Cryptography，简称 PQC)。

尽管向后量子密码的过渡在量子计算机问世之前就开始了，但仍然存在紧迫的威胁。攻击者现在收集加密数据，目的是在量子技术成熟后解密数据，这就是“先收集-后解密”的安全威胁，因为许多机密数据的价值往往会持续多年，有些个人机密数据会伴随人的一生，因此现在开始过渡到后量子密码，对于防止未来发生机密数据被解密至关重要。这种威胁模型是迫切过渡到后量子密码的主要原因之一。

为此，美国国家标准技术研究院(NIST)于 2024 年 11 月 12 日发布了 NIST IR 8547 《过渡到后量子密码标准》的公开征求意见草案，该报告描述了 NIST 从易受量子攻击的密码算法过渡到后量子数字签名算法和密钥建立方案的预期方法，确定了现有的易受量子攻击的密码标准以及信息技术产品和服务需要过渡到的抗量子密码标准，旨在促进与行业、标准组织和相关机构的合作，以促进和加速后量子密码的采用。NIST 列出了迈向 PQC 标准过渡时间表，目标是到 2035 年尽可能低降低量子风险。目前正在广泛使用的安全密码算法 RSA-2048 和 ECC-256 将在 **2030 年弃用，2035 年禁用**，这就是传统密码算法的死期，要求业界必须提前做好所有相关系统和产品向 PQC 算法的迁移工作。

也就是说，2029 年 12 月 31 日之前面临的技术革命是 HTTPS 加密必须迁移到抗量子密码算法上，所有系统都需要升级改造支持后量子密码 HTTPS 加密。这是用户必须面对的即将到来的又一个技术革命，这个技术革命要求用户必须升级改造现有系统以支持后量子密码算法。

三、 两次技术革命需要两次系统升级改造

谷歌在“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”。的确如此，缩短 SSL 证书有效期的技术革命的最终目的是为了抗量子攻击，因为现在的密码算法无法对抗即将到来的量子计算。而不断缩短 SSL 证书有效期的主要目的就是实现自动化更新 SSL 证书，为自动化更新支持后量子密码算法提供了技术手段，保证了在条件成熟时可以无缝无感地过渡到抗量子算法，两次技术革命的最终目的还是为了第二次抗量子技术革命。

缩短 SSL 证书有效期是 SSL 证书用户必须面临的一次革命，这次革命的到来时间是 2026 年 3 月 15 日，最终完成时间是 2029 年 3 月 15 日。而弃用传统密码算法启用后量子密码算法则又是一次 SSL 证书用户面临的革命，这次革命到来的时间是 2029 年 12 月 31 日，因为 2030 年必须弃用现在正在使用的密码算法了，包括 RSA-2024 算法、ECC-256 和 SM2 算法。

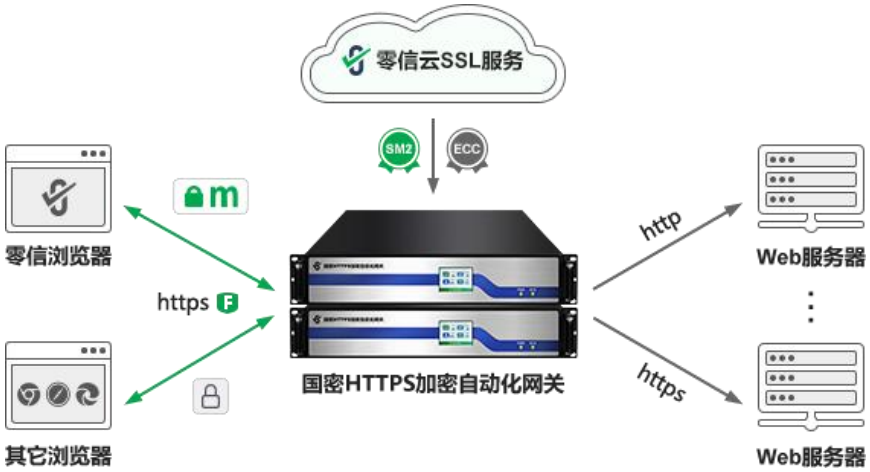
2026 年 3 月 15 日的技术革命要求用户提前实施 SSL 证书自动化管理技术升级改造，彻底丢弃传统的 SSL 证书人工管理。2029 年 12 月 31 日的技术革命要求用户提前实施 HTTPS 加密的后量子密码支持，这也要求用户完成系统升级改造。SSL 证书用户也就是所有网站运营者和管理员都必须拿出行动计划来尽快完成 2026 年的技术革命，同时还需要提前考虑如何完成 2029 年的技术革命，而不是只考虑 2026 年的技术革命，两次革命有相关性，都是为了保障 HTTPS 加密安全。

四、 零信技术创新实现一次微改造完成两次技术革命必须的技术改造

零信技术在四年前创立之时就定位为用户提供 SSL 证书自动化管理解决方案，同时提供国密 SSL 证书和国际 SSL 证书自动化管理。因为那个时候全球就已经开始普及使用 SSL 证书自动化管理技术，但是我国目前基本上还是空白。鉴于国密 SSL 证书自动化管理无法套用国际 SSL 证书自动化管理的方案，因为商用密码体系在目前各种系统中是普遍不支持，要想实现国密 HTTPS 加密自动化，不仅仅是要实现国密 SSL 证书的自动化管理，而且还需要自动化完成国密算法支持升级改造。

为了帮助 SSL 证书用户轻松完成即将到来的缩短 SSL 证书有效期技术革命必须完成的系统升级改造，零信技术的创新方案是微改造、零业务中断的方案，一个网关同时完成双算法 SSL 证书自动化管理和国密改造，而原 Web 服务器则是零改造。这是一个端云一体的解决方案，用户只需在原 Web 服务器前面部署零信国密 HTTPS 加密自动化网关即可，由零信网关自动化对接零信云 SSL 服务系统，自动化完成 47 天有效期的双算法 SSL 证书的自动化申请和部署，

自动化实现国密 HTTPS 加密和 WAF 防护，并且是自适应加密算法，免费配套的零信浏览器实现国密 HTTPS 加密，而其他不支持国密算法的浏览器实现国际算法 HTTPS 加密。



零信技术为缩短 SSL 证书有效期的技术革命提出的创新方案不仅可以帮助 SSL 证书用户轻松应对即将到来的 2026 年技术革命，而且零信技术已经正在研发后量子密码 HTTPS 加密的自动化实现，这就是零信技术打造国密证书自动化管理生态全系列产品的优势，只要零信浏览器和零信网关支持后量子密码 HTTPS 加密，到时候用户只需免费升级零信浏览器，零信网关只需自动化免费完成软件升级，就可以让用户无感地完成后量子密码 HTTPS 加密升级改造工作。

如下图所示，零信浏览器英文官网已经实现了国际 ECC 算法 SSL 证书的后量子密码(ML-KEM768) 混合密钥协商机制的 HTTPS 加密，而国密 SM2 算法的 SSL 证书的后量子密码(ML-KEM768)混合密钥协商机制的 HTTPS 加密也正在紧锣密鼓地研发中，预计年底前零信浏览器和零信国密 HTTPS 加密自动化网关都将支持国密算法 SM2DH-MLKEM768，率先实现 SM2 抗量子混合密钥协商机制 HTTPS 加密，这就是零信技术独家拥有的全生态产品的独特优势！

也就是说，如果用户选择了零信技术 SSL 证书自动化管理技术革命的微改造方案，将来就可以完成免费自动化完成后量子密码 HTTPS 加密技术革命的技术改造工作，这是一箭双雕的完美解决方案，高瞻远瞩地一次投资完成必须的两次技术革命技术改造，省钱、省事。这是零信技术的独特优势，为用户提前考虑和布局，帮助用户轻松应对现在和将来的 HTTPS 加密安全威胁。

五、 两次技术革命既然是必须的，那就选择一次完成

正如谷歌推动缩短 SSL 证书有效期是为了轻松过渡到抗量子密码所言，既然完成两次 HTTPS 加密技术革命是必须的，那就应该在规划第一次技术革命时想到第二次技术革命，把两次技术革命所需要的技术改造一起规划，选择一次完成的先进技术方案，而不是头痛医头脚痛医脚，只有这样才是最节省投资和减轻升级改造负担的最佳解决方案。

缩短 SSL 证书有效期的技术革命将于 2026 年 3 月 15 日到来，2029 年 3 月 15 日结束，后量子密码 HTTPS 加密的技术革命将于 2029 年 12 月 31 日到来，这两场技术革命都是所有网站运营者必须应对的，必须进行改造的，选择一次完成两次革命才是唯一正确选择。

王高华

2025 年 7 月 14 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 219 篇(共 65 万 2 千多字)和英文 96 篇(13 万 1 千多单词)。