请果断更换不支持证书自动化的 SSL 网关

2025 年 11 月 10 日

笔者从多家合作伙伴和多个大客户得到一个重要信息：在向客户推荐零信国密 HTTPS 加密自动化网关时，很多客户会问同一个问题：我们已经部署了 SSL 网关，是否有证书自动化软件解决方案？笔者给出的答案是：无论是软方案还是硬方案，如果现有网关不支持 SSL 证书自动化，则必须升级换代！请果断废弃不支持证书自动化的 SSL 网关！本文详细讲一讲缘由，供关键信息基础设施运营单位 IT 主管们决策参考。

一、 我国关键信息基础设施系统面临五大技改难题

我国关键信息基础设施系统的国密改造工作从 1999 年发布了《商用密码管理条例》就正式开始了，整整 26 年了，还在进行中，可见整个生态改造有多难。目前常用的技术方案就是前置部署 SSL 网关，实现双算法（RSA/SM2）自适应 HTTPS 加密，这就要求用户不仅要采购 SSL 网关(SSL VPN 网关)，还要向 CA 采购 SSL 证书，并人工部署到 SSL 网关上使用。这是目前通行的国密改造技术方案，所以才有了用户所讲的已经部署了 SSL 网关的现状。

但是，新的问题来了，一是云计算算力的不断增强，二是量子计算机能秒破正在使用的密码算法，使得国际标准组织已经制定了不断缩短 SSL 证书有效期的时间表：明年 3 月 15 日起 CA 只能签发 200 天有效期证书，2027 年 3 月 15 日只能签发 100 天证书，2029 年 3 月 15 日只能签 47 天证书。这个情况告诉用户后，有些用户的第一个反应是赶紧在明年 3 月 15 日之前多买点一年期证书，这当然是大错特错的选择，不应该再花冤枉钱去买证书了。明智的用户会问：是否有什么更好的解决方案？国际上的解决方案是什么？

国际上的解决方案是在 Web 服务器上安装一个证书自动化客户端软件-CertBot，由这个软件来实现自动化证书申请、签发和部署，非常好的方案，但是不适用于我国，因为这个方案只能申请到国际算法 SSL 证书。所以，零信技术才牵头制定《自动化证书管理规范》密码行业标准，支持双算法 SSL 证书自动化管理，目前还是草案阶段。

也就是说，我国关基系统面临国密改造和证书自动化改造两大难题，第三个难题是国际 SSL 证书供应链很不稳定，无论是技术原因还是地缘政治原因都有可能遭遇 SSL 证书断供或吊销的风险，所以，关基系统不仅需要支持证书自动化，还需要支持自动切换证书签发 CA。

第四个难题就是必须尽快启用后量子密码(PQC) HTTPS 加密，因为传统密码算法(RSA/ECC/SM2)加密的流量现在就面临“先收集后解密”的安全威胁。也就是说，即使所有关基系统完成了国密算法 HTTPS 加密改造，攻击者仍然可以先收集这个已加密的机密数据，待量子计算机可用时解密这些机密数据，这就要求现在就必须启用已经成熟实施的混合算法后量子密码 HTTPS 加密。全球互联网流量中有 **47%**流量已经实现了后量子密码加密，但是我国关基系统没有一个网站已启用！鉴于已存在的这个安全威胁，后量子密码 HTTPS 加密改造比国密 HTTPS 加密改造更紧迫，更需要马上实施，早一点支持 PQC 加密，机密数据就早一点在将来是安全的。而第五个难题是要求在 2030 年 1 月 2 日之前所有系统都必须支持纯后量子密码算法 HTTPS 加密。

二、 唯一可行方案只有升级换代已有 SSL 网关设备

SSL 网关由于是实现 HTTPS 加密的唯一关键设备，当然就应该由 SSL 网关来解决以上五大技术难题，如果现有已部署的网关包括 WAF 设备，不能解决这些难题，用户只有两条路：一是要求现有网关厂商升级支持证书自动化、支持多通道获取双算法 SSL 证书、支持后量子密码 HTTPS 加密，这就是“**升级**”的思路；如果不能升级支持，那就只能废弃已部署的旧网关，更换为支持这些功能、能解决以上五大难题的新的硬网关或软网关系统，这就是“**换代**”的思路。关基用户也只有这两条路可走。

先讲一下为何说突击采购 SSL 证书是大错特错的想法。有这个想法的用户肯定是没有想到上面讲的第一个思路—要求现有网关厂商支持证书自动化，因为固有思维是 SSL 证书找 CA 申请，网关硬件问题找网关厂商，很多单位这两个产品分属于不同部门管理，现在是 SSL 证书缩短了有效期，马上想到的突击采购 SSL 证书也是正常思维，但这是错误的解决问题思路，因为这只能拖延一年，其结果是多花了一年的证书冤枉钱。

如果要求网关厂商升级支持证书自动化这条路走不通，那就只能淘汰这个旧网关，采购新的支持证书自动化的网关了，这是不得已的解决方案，但这是一条必走的方案，也许旧网关正好到了该淘汰的使用年限了，那就果断地采购新的支持双算法 SSL 证书自动化的 SSL 网关。

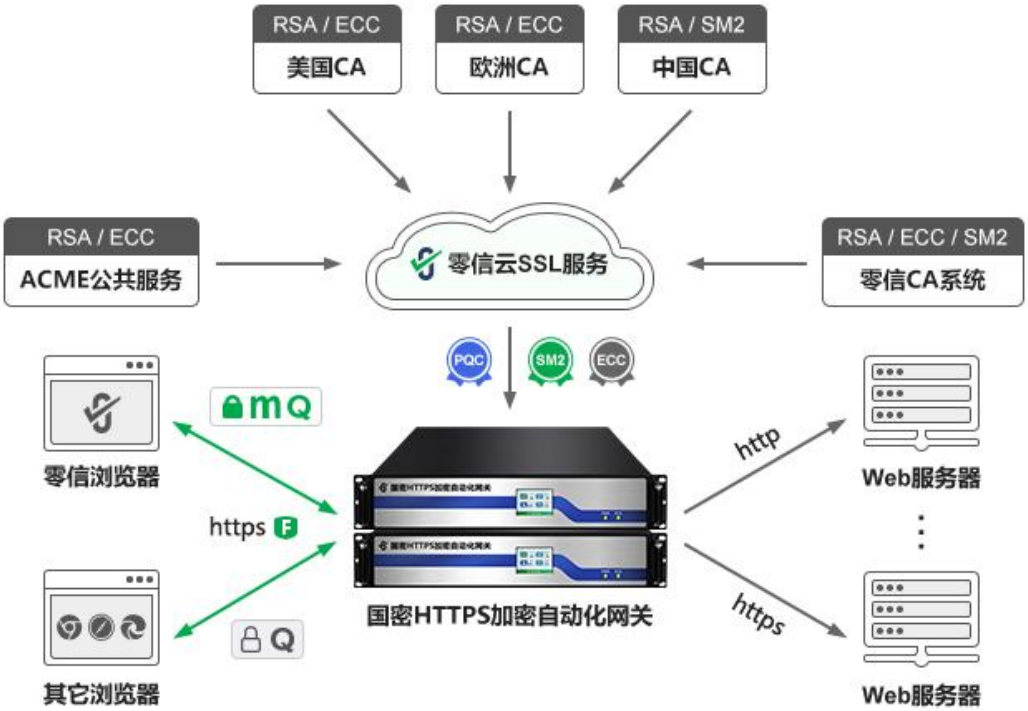
除了需要解决国密改造和证书自动化难题外，还需要解决其他三个难题，到目前为止，笔者并没有发现市场上有相应的解决方案和产品，怎么办？

三、 一个创新网关完美解决五大技改难题

上面讲到的第一条路—要求网关厂商升级支持证书自动化，网关厂商可能会答应用户将支

持，但是到目前为止，只有国际 SSL 证书支持证书自动化，没有国密 CA 提供国密 SSL 证书自动化服务，这就难住了网关厂商，巧妇难为无米之炊，这也是用户目前遇到的真实困难之一。

零信技术历时四年多打造的创新解决方案已经彻底解决了关基用户所面临的五大技改难题，这是一个端云一体的创新方案：一端为零信浏览器，同时支持商用密码和后量子密码算法，并优先采用 PQC 算法；另一端为零信国密 HTTPS 加密自动化网关，替代不支持证书自动化的传统 SSL 网关，也是部署在服务器前面，自动对接零信云 SSL 服务系统，支持多 CA 通道自动化申请和部署双算法证书（SM2/ECC）、实现混合 PQC 算法 HTTPS 加密，使得原 Web 服务器无需改造即可自动化完成商用密码改造和后量子密码迁移，实现 HTTPS 加密量子安全，保障关基数据在现在与量子时代的持续安全。



下面分别详细讲解零信技术是如何解决关基用户面临的五大技改难题的。

1. 国密改造难题和证书自动化难题

从目前大多数关基用户已经部署了 SSL 网关的情况来看，其实业界已经解决了国密改造难的问题，那就是原 Web 服务器零改造，只需前置部署 SSL 网关。但是，这个老方案遇到了新问题，就是 SSL 证书有效期将缩短为 47 天，不可能要求用户每个月向 CA 申请证书后人工部署到现有网关上去。这就要求现有网关能升级支持证书自动化，但是就如上面所讲，即使网关厂商愿意升级网关支持，但是没有国密 CA 支持国密 SSL 证书自动化，还是行不通。

零信技术的解决方案就是 CA 可以不支持证书自动化，零信云 SSL 服务系统通过传统 API 对接 CA 系统为零信国密 HTTPS 加密自动化网关提供双算法 SSL 证书自动化管理服务，这就解决难题了，其他网关厂商也可以借鉴这个技术路线。但是，零信技术的独家解决方案是网关费用含双算法 SSL 证书，包 5 年最多 255 个网站的国际 DV SSL 证书和国密 OV SSL 证书，用户不需要向 CA 购买 SSL 证书，不采用不安全的共享密钥通配证书，实现了一站一密钥一证书，这是现有所有网关厂商都做不到的独家超值价值和独特优势。

2. SSL 证书供应链安全难题

要想解决 SSL 证书供应链不稳定的难题，就需要网关对接多家 CA 实现双算法 SSL 证书自动化管理，这又增加了网关厂商的升级改造难度。零信云 SSL 服务系统已经成功对接 7 家国际 CA 和 4 家国密 CA，实现了自动切换 CA 签发通道的双算法 SSL 证书自动化管理，确保一定能为网关可靠签发双算法 SSL 证书，彻底解决 SSL 证书断供和吊销难题。

用户也可以把这个解决思路告知网关厂商，只要网关厂商能依据《自动化证书管理规范》密码行业标准草案对接零信证书自动化服务系统，那就等于也具备了自动化证书管理能力和自动切换多家签发 CA 的能力，这样，用户只需购买零信技术的双证书自动化服务包即可，就可以利用现有 SSL 网关实现双算法 SSL 证书自动化管理和自动切换多 CA 通道签发证书。

3. 后量子密码迁移难题

解决这个问题可能比上述 3 个难题更难，因为这是一个改造密码生态的问题，不仅要求 SSL 证书支持后量子密码，不仅要求网关支持后量子密码，还要求浏览器支持后量子密码。这个难题估计现有网关厂商很难解决，即使答应用户升级现有网关支持。

零信技术已经发布了后量子密码 HTTPS 加密应用全生态产品就绪时间表，零信浏览器现在已经支持后量子密码混合协议 HTTPS 加密，零信国密 HTTPS 加密自动化网关也已经支持国际算法 ECC+PQC 混合协议 HTTPS 加密。零信技术正在研发支持 SM2+PQC 混合协议支持，后续支持纯国际 PQC 算法和国产 PQC 算法 HTTPS 加密。这些支持都是完全免费的，用户只要部署了零信国密 HTTPS 加密自动化网关，就可以免费无缝迁移到后量子密码，这是目前市场上唯一已经实现并且承诺完全免费升级支持的解决方案。这是零信技术拥有 HTTPS 加密全生态产品的独家优势。

4. WAF 防护和 IPv6 改造难题

零信网关不仅解决了以上五大难题，还顺带解决了 WAF 防护难题，内置高性能 WAF 系统，经权威的第三方在线测试软件 WAFER 测试，其攻击行为检测能力和识别能力都是 A 级(最高级别)，真阳检测率达到 97.34%，假阳误拦率为 0。用户不用花钱买 WAF 设备，也不用为 WAF 设备人工申请和配置双 SSL 证书，自动化实现 HTTPS 卸载流量的清洗，转发干净流量给后面的 Web 服务器。

零信网关还顺带解决了 Web 服务器的 IPv6 改造难题，只需在网关上配置 IPv4 和 IPv6 两个 IP 地址，就可以实现 IPv4 和 IPv6 双网络用户的 HTTPS 加密安全访问 Web 系统，提供可靠的 WAF 防护服务。

四、证书自动化和后量子密码是刚需，SSL 网关产品必须升级换代

实现双算法(SM2/RSA) SSL 证书自动化管理和后量子密码迁移是技术倒逼的刚需，唯一的解决方案是部署 SSL 网关。对于已经部署了不支持证书自动化网关的用户，有两个解决方案：一是要求网关厂商升级支持证书自动化，可以对接零信云 SSL 服务系统，支持多签发 CA 自动化签发双证书；如果网关厂商不支持升级，那就必须产品换代了，选用支持证书自动化的 SSL 网关。

请关基用户仔细研究分析和评估各厂家解决方案，果断更换不支持证书自动化的旧网关，因为早一天支持后量子密码就早一天保证了机密数据不再遭遇“先收集后解密”攻击，保证了数据资产在量子时代的安全。零信技术创新解决方案是一个端云一体的交钥匙方案(网关+证书+自动化)，遵循“密码敏捷原则”，不影响现有业务系统的正常运行，只需在现有网络架构上并联接入零信国密 HTTPS 加密自动化网关，在旧网关的 SSL 证书到期前完成新网关的考验，到时断开旧网关连接即可，轻松完成国密改造、证书自动化改造、多签发 CA 改造、后量子密码改造等多项必须的技术改造工作，切实保障关基数据在现在和量子时代的始终安全。

王高华

2025 年 11 月 10 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 237 篇(共 70 万 5 千多字)和英文 101 篇(13 万 8 千多单词)。