ACME 客户端软件的创新—硬件化

零信技术国密 HTTPS 加密自动化管理解决方案的第一个产品是学习国际 SSL 证书自动化解决解决方案，开发一个 ACME 客户端软件-SM2cerBot，但是这个国密 ACME 客户端软件在上个月已经从官网下线了，很多用户来咨询为何下线。本文就讲一讲这个话题，并重点介绍我们的解决方案的第二个产品—国密 ACME 客户端硬件：零信国密 HTTPS 加密自动化网关。讲清楚我们的研发历程，意在能为用户提供双算法 SSL 证书自动化管理解决方案选型决策参考。

一、 国密 ACME 客户端软件遇到的难题

由于 SSL 证书有效期将缩短为 47 天，SSL 证书自动化管理已成为必然选择。国际 SSL 证书自动化管理解决方案是在 Web 服务器上安装一个客户端软件—ACME 客户端，如 CertBot，再配置 ACME 服务提供商的 ACME 服务参数，就可以自动化完成 SSL 证书申请、验证和部署了。这个方案非常成熟，不仅有 RFC8555 国际标准可依据，而且有两大 ACME 服务提供商(LE 和 GTS)免费为用户提供 90 天有效期的 RSA/ECC 算法 SSL 证书，从 2013 年开始，已经为全球用户自动化签发了超过 200 亿张 SSL 证书，仅 LE 一家的有效 SSL 证书就超过 5 亿张。

但是，这个非常成熟的国际 SSL 证书自动化解决方案并不能解决所有问题，如：用户 Web 服务器无法安装 ACME 客户端软件，或者用户的系统正在运行，一刻也不能停机启用 ACME 服务。而我国正在大力推广普及应用商用密码算法实现 HTTPS 加密，这就需要 ACME 服务支持国密 SSL 证书的自动化申请和部署，但不能像国际 ACME 解决方案那样拿到 SSL 证书就可以了，还需要改造 Web 服务器支持国密算法实现国密算法 HTTPS 加密。

零信国密 ACME 客户端软件—SM2cerBot 就是一个既能自动化完成双算法 SSL 证书的申请，又能自动化完成双 SSL 证书的部署，还能自动化完成 Web 服务器软件升级支持国密算法的一个 ACME 客户端软件，按理说这个解决方案已经是一个最佳解决方案了，能同时满足国密合规和全球信任的 HTTPS 加密应用需求。但是，在实际用户环境使用过程中就遇到大困难了，主要有：

(1) 对业务系统伤害大：由于需要卸载和重新编译原 Nginx 服务器软件，以便支持国密算法，这个改动对已经运行的应用系统伤害很大，可能会导致业务系统无法运行，这个风险太大，因为用户业务系统可能是政务系统或网银系统，不能停止服务。

(2) 操作系统适配难：常用的操作系统是 Ubuntu 和 CentOS 或其他国产操作系统，这些系统已经发布了很多版本，ACME 客户端需要在各个版本上编译适配，这个工作量巨大，但让用户自己去编译又太难为用户了。

(3) 业务不能中断：用户的业务系统正在运行，不能中断，也不能轮换中断，也就是说用户的 Web 服务器根本不能动，既不能或不允许安装任何第三方软件，也不允许 Web 服务重启。

也正是由于这些实际部署难题，零信技术决定放弃了国密 ACME 客户端软件的继续研发和技术支持，上个月决定下线这个客户端软件，不再向用户推荐这个解决方案，因为这不是一个适合于我国 SSL 证书自动化管理的解决方案，无法满足用户对现有业务系统零影响的实际应用需求。

二、 最佳解决方案—国密 ACME 客户端软件硬件化

国密 ACME 客户端软件遇到的核心问题在于会影响用户业务系统的正常运行，这是用户无法接受的，用户需要零影响现有系统的方案。零信技术想到了一个更好的解决方案—把国密 ACME 客户端软件安装在硬件服务器中，给用户一个集成了 ACME 客户端软件的软硬一体机，这样就可以实现不改造用户原有系统，不在用户 Web 服务器上安装任何软件，由这个一体机来完成双算法 SSL 证书的自动化申请和部署，并自动化实现 HTTPS 加密，由这个一体机来替代原先由用户 Web 服务器完成的这些工作，这个一体机就是现在大家已经看到的产品—零信国密 HTTPS 加密自动化网关。

这个解决方案的核心思想是不仅要把原先需要安装 SSL 证书的 Web 服务器或其他网关设备的 SSL 证书部署和 HTTPS 加解密功能都转移到这个国密 ACME 客户端硬件上，还要加上双算法 SSL 证书的自动化申请、域名验证和部署等工作，还要支持国密算法(SM2/SM3/SM4)。所以，国密 ACME 客户端硬件就等于高性能网安硬件平台+支持国密算法的 Nginx+高速密码卡+ACME 客户端软件+国际 SSL 证书+国密 SSL 证书+WAF 系统，实际上就是一个内置私钥和证书的密码机(HSM 设备)，不仅提供 ACME 客户端功能，而且还能保证 SSL 证书密钥安全，保证密钥不出硬件，不经过任何人的人工手动处理，比传统的人工申请 SSL 证书有多人经手密钥更安全。

而由于 HTTPS 加解密工作已经从 Web 服务器迁移到了 ACME 客户端硬件上，减轻了 Web 服务器 20-30%的算力负担，让 Web 服务器可以专用于处理用户业务系统。这个功能实际上就是传统 SSL 网关的作用，这就是为何零信技术命名这个国密 ACME 客户端硬件为“国密 HTTPS 加密自动化网关”的原因，简称“零信网关”。

三、 零信网关不仅仅是一个国密 ACME 客户端硬件

零信网关不仅仅是一个实现 ACME 功能的、自动化申请和部署双算法 SSL 证书的硬件 SSL 网关，而且还集成了 WAF 模块，这是考虑到 HTTPS 流量通过网关卸载后如果不加分析直接转给后面的 Web 服务器，那么用户还需购置 WAF 设备，这增加了用户系统复杂性和可靠性，不如直接在 HTTPS 加密流量卸载后增加一个流量清洗功能，拦截恶意流量和放行干净流量，给后面的 Web 服务器更大的安全保障。

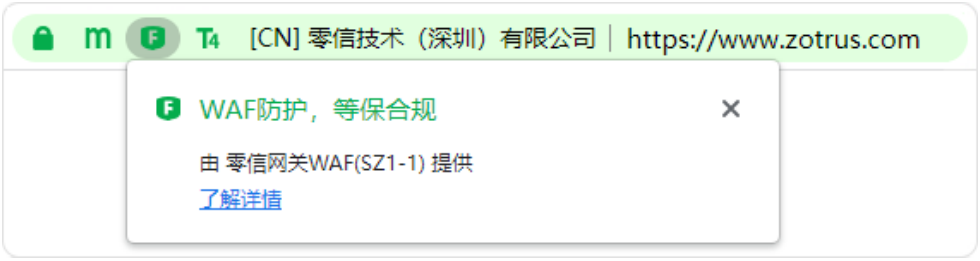
零信网关内置 WAF 模块是一个基于开源 ModSecurity 系统开发的 Web 应用防火墙，其高性能 WAF 防护功能通过权威第三方测试平台 WAFER 评测结果是：检测能力为 A 级(最高级别)，识别能力为 A 级(最高级别)，真阳识别率高达 97.34%(还有提升空间)。而用户常用的传统 WAF 设备都不支持 SSL 证书自动化管理，需要用户手动配置 SSL 证书到 WAF 设备上实现 HTTPS 加密方式的 WAF 防护。

零信网关不仅支持 SSL 证书自动化管理，不是销售一个没有 SSL 证书的裸机给用户，而是销售一个包 5 年最多 255 个网站的双算法 SSL 证书(国密 OV SSL 证书+国际 DV SSL 证书)的自动化管理硬件给用户，而且硬件本身也是包用 5 年，出故障机器免费直接更换。

零信网关不仅包双算法 SSL 证书，还能保证双 SSL 证书不会因为各种原因断供而中断为网关自动化配置 SSL 证书，因为零信云 SSL 服务系统已经对接了多家国际 CA 和国密 CA，可以可靠地为用户网站签发国际 SSL 证书和国密 SSL 证书，用户还可选择熟悉的 SSL 证书品牌。

零信技术双算法 SSL 证书自动化管理解决方案不仅仅有国密 ACME 客户端硬件，也不仅

仅是打包了双 SSL 证书，不仅仅是集成 WAF 功能，而且还免费配套提供不限用户数的、干净无广告的国密浏览器—零信浏览器。零信浏览器不仅优先采用国密算法实现 HTTPS 加密，而且浏览器地址栏的加密锁标识后面增加显示一个 WAF 防护标识，明确告知网站访问者正在访问的网站不仅实现了国密 HTTPS 加密，还实现了 WAF 防护，符合国密合规和等保合规的双合规要求。



四、国密 ACME 客户端软件硬件化是最佳的双算法 SSL 证书自动化管理解决方案

ACME 客户端软件是实现 SSL 证书自动化管理的必需软件，在 RSA 密码体系已经完美集成到所有 IT 产品和互联网基础设施中的今天，要想实现 HTTPS 加密，的确只需要一个能自动化完成 SSL 证书申请和部署的软件即可，当然特别情况如老旧系统不能安装 ACME 客户端软件除外。

但是，我国的商用密码算法还远远没有达到普及支持的程度，所以，最佳解决方案是干脆不改造现有系统，无需安装任何 ACME 客户端软件，直接通过一个硬件设备来实现协议转换，让用户毫无痛苦地轻松实现双算法 SSL 证书的自动化管理，这才是用户真正想要的自动化证书管理解决方案。

王高华

2025 年 6 月 25 日于深圳
