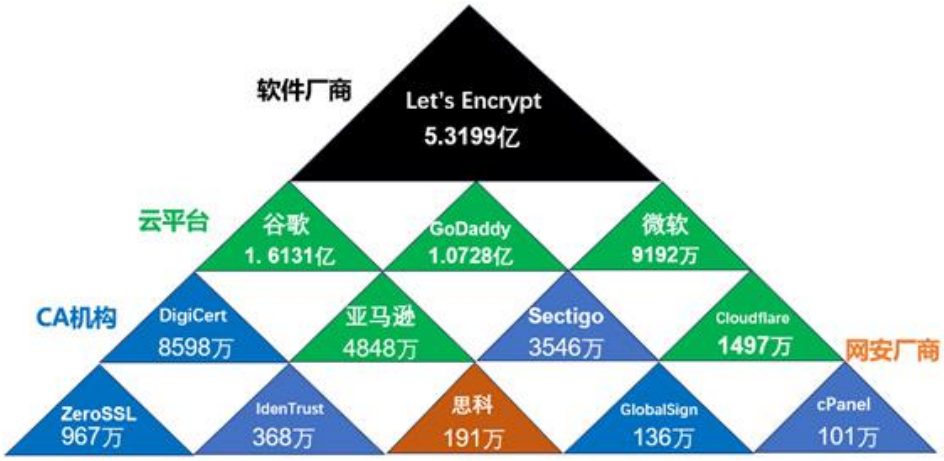
突击批量采购一年期 SSL 证书是下下策

全球 CA 将于 2026 年 3 月 15 日起只能签发最多 200 天有效期的 SSL 证书，笔者同多个 SSL 证书的大用户聊起这事时，几乎大家毫不犹豫地说：那就赶在明年 3 月 15 日之前把所有需要续期的 SSL 证书都提前采购。这绝对是一个浪费钱的下下策，笔者今天就讲一讲上上策是什么，值得所有 SSL 证书用户深思并做出正确的决策。

一、 SSL 证书已经不再是一个值得采购的产品

SSL 证书是实现 HTTPS 加密所必须的产品，自从 SSL 证书在 1994 年被发明以来就是用户必须采购的产品，但是 31 年后的今天，这个产品已经不再是一个值得采购的产品了。全球 11 亿张 SSL 证书中超过 80%的都是免费自动化签发的，也就是说，全球 80%用户都已经不再采购 SSL 证书，不再需要化一分钱。就连最不差钱的美国政府官网也是在使用 Let's Encrypt 自动化签发的免费 90 天 SSL 证书。



全球前十三大SSL证书提供商排名和证书签发量(2025.3.30统计)

用户不再采购 SSL 证书当然不等于 HTTPS 加密不需要 SSL 证书，国际解决方案是需要用户在 Web 服务器上安装一个 ACME 客户端软件，就可以一劳永逸实现自动化配置免费 SSL 证书实现 HTTPS 加密，不用花钱！或者可以使用 Cloudflare CDN 服务，也不用操心花钱去买 SSL 证书和安装 SSL 证书，启用服务就已经免费自动化配置好 SSL 证书和启用 HTTPS 加密！还在卖 SSL 证书的 CA 机构 DigiCert 和 Sectigo 已经从全球第一第二位跌到了第 5 和第 7 位。这些现实数据非常值得 CA 机构(包括 SSL 证书销售机构)深思：我还在销售 SSL 证书是否走错了方

向？当然也非常值得 SSL 证书用户深思：我还在大把花钱采购 SSL 证书是否值得？采购决策是否正确？

二、 SSL 证书有效期将缩短为 47 天，上上策是积极拥抱 SSL 证书自动化

逐步缩短 SSL 证书有效期为 47 天的国际标准已经落地，市场上又有完全免费的 SSL 证书可以自动化获取，为何 SSL 证书用户还要计划在缩短 SSL 证书有效期生效之日之前去抢购一批一年期 SSL 证书呢？这是稀缺性在作怪，这是惯性思维在作怪！毕竟这个人工申请证书的惯性动作已经习惯了 31 年。

请大家想一想，就算你突击采购了一年期 SSL 证书，你还得辛苦去服务器上安装，2027 年 3 月 15 日之前还是必须去实现证书自动化，为何不现在就马上拥抱 SSL 证书自动化，一劳永逸的解决这个问题呢？何必还要去多花一年的证书采购冤枉钱呢？只需马上采取行动实施证书自动化，那以后再也不用费心费钱去采购 SSL 证书和费心费工夫去安装 SSL 证书了，再也不用每年花钱了！有省心和省钱的方案，为何还要去做一点都不省心和不省钱的事情呢？所以，笔者才称“缩短 SSL 证书有效期为 47 天”是一场技术革命，一个从“人工管理”到“自动化管理”的技术革命，所有消极思维的人都会抵制所有革命，所以才会做出突击采购一年期 SSL 证书的错误决策，这是消极应对，下下策！

唯一正确的决策是：马上规划和实施 SSL 证书自动化管理解决方案，这才是上上策！对于我国政务系统和网银系统这些关键信息基础设施运营单位，必须规划和实施双算法(SM2/RSA)SSL 证书自动化管理解决方案，同时把国密 HTTPS 加密改造问题一起解决，因为传统的密改方案还是让用户去采购国密 SSL 证书手动部署到网关或者改造 Web 服务器支持国密算法并手动安装国密 SSL 证书。

上上策就是采购能免费自动配置双算法 SSL 证书的国密 HTTPS 加密自动化网关，一次采购和部署，就能管 5 年最多 255 个网站的 HTTPS 加密自动化和 WAF 防护，无需再花钱采购 SSL 证书，无需费力安装 SSL 证书，无需费力安装 ACME 客户端软件，Web 服务器也无需升级改造支持国密算法，原 Web 服务器零改造，业务零中断，这才是一劳永逸的最佳解放方案，上上策。

三、 对比分析“突击批量采购 SSL 证书”和“采购 HTTPS 加密自动化网关”的优劣

对于少量国际 SSL 证书用户，最佳方式是直接采用市场上现成的 SSL 证书自动化解决方案—在 Web 服务器上一次安装 ACME 客户端软件，这是一劳永逸的解决方案。而对于已经采

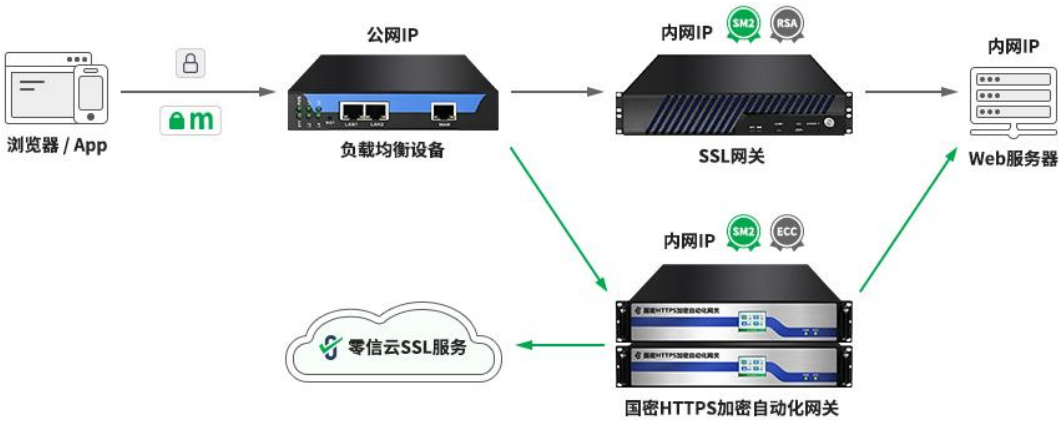
购了大量 SSL 证书用户和需要国密改造的用户，意味着有大量的网站系统需要实现证书自动化，不推荐人工去每台服务器安装 ACME 客户端软件和为每个网站配置自动化服务，工作量巨大不说，还会影响现有系统的正常运行，因为在现有系统中安装一个第三方软件，一定会影响现有系统的正常运行。怎么办？必须采用微改造的方案—部署国密 HTTPS 加密自动化网关。

为了对比“突击批量采购 SSL 证书”和采购“HTTPS 加密自动化网关”的优劣，以某大型国有银行为例，目前每年都采购了七百多张全球最贵的国际 SSL 证书，证书采购费用一定超过 700 万元，这还只是国际 SSL 证书的采购费用，不包括国密 SSL 证书的采购费用，因为国密 SSL 证书还都不支持证书透明，所以无法从证书透明日志数据库中查到采购数量，暂按 300 万元估算。这样，双算法 SSL 证书合计每年 SSL 证书采购费用为 1000 万元，实际采购金额一定大于这个数字，笔者引用此大致数据只是为了对比说明突击采购 SSL 证书的决策是何等严重的错误决策。

正确的决策是：不采购 SSL 证书，而是把每年采购国际 SSL 证书和国密 SSL 证书的 1000 万元用于采购零信国密 HTTPS 加密自动化网关，可以采购 20 台网关，这 20 台可以分为 5 组，每组 4 台网关，每组最多支持 255 个网站，合计支持 **1275** 个网站，这应该能满足此银行目前的业务和将来 5 年的发展需要。由于零信网关不仅硬件包用 5 年而且含 5 年的双算法 SSL 证书，也就是说只需花一年采购 SSL 证书的钱，就可以管 5 年的 1275 个网站的 HTTPS 加密自动化和 WAF 防护自动化，并且是双算法 SM2/ECC 支持，同时自动化完成了所有网站系统的国密改造和 IPv6 改造。这绝对是一个非常超值的产品升级换代采购方案，这才是上上策的方案，不仅节省了 4 年的证书采购费用 4000 万元，而且省事(无需申请和部署 SSL 证书)，更安全(证书私钥不出网关，不再需要多人经手处理)，更可靠(再也不会因为忘记证书续期而导致业务中断)。

这就印证了一句古话“不比不知道，一比吓一跳”，两个采购决策的优劣是如此之大，相信这个对比一定能惊醒所有决定突击采购 SSL 证书的决策者。但是，为何这些用户会想到突击采购的决策呢？一个原因当然是用户可能不知道还有更好的省钱的自动化解决方案，这就是笔者决定写这篇文章的原因，要让正在寻求解决方案的用户了解市场上已经有了比突击采购 SSL 证书更优的方案。另一个原因则是对新技术和新事物的抵触，不敢尝试打破传统的创新方案，这个决策的确需要一点魄力。其实，用户完全没有必要担心新方案的可靠性，零信技术提出的是并联接入方式，用户可以在保留现有架构的情况下，并联接入零信国密 HTTPS 加密自动化网关，先平行运行一段时间直到现有网关系统的 SSL 证书过期后就可以自然淘汰不支持证书自动化的老网关了，这就可以平稳地从人工管理证书过渡到自动化管理证书，证书过期后就不再需要继续采购 SSL 证书了，所以，用户必须在现有证书到期前半年部署零信国密 HTTPS 加

密自动化网关，以便有时间考验新方案的可靠性，也就可以放心地顺利地完成 SSL 证书自动化管理技术改造了。



四、 一次技改完成两次 HTTPS 加密技术革命，上上上策

通过以上的两个采购方案的对比，大家一定也会认可采购国密 HTTPS 加密自动化网关是上上策，而传统方案采购 SSL 证书则是下下策。其实，零信技术的创新解决方案还有一个更吸引人的承诺。由于实现了双算法 SSL 证书的自动化管理，为下一个 HTTPS 加密技术革命—“从传统密码到抗量子密码”打下了技术基础，这个技术革命的到来时间是 2029 年 12 月 31 日，零信技术正在打造后量子密码 HTTPS 加密全生态产品，一旦产品成熟，用户只需免费自动升级零信浏览器和零信国密 HTTPS 加密自动化网关，即可无缝无感地升级到后量子密码 HTTPS 加密，轻松完成后量子密码的迁移，有力保障了重要业务数据在后量子密码时代的始终不间断安全。

零信技术的创新解决方案能让用户只需一次技术改造就可以完成 HTTPS 加密即将来临的两次技术革命，这才真正是上上上策。

王高华

2025 年 8 月 4 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 222 篇(共 66 万 4 千多字)和英文 97 篇(13 万 2 千多单词)。