SSL 证书有效期将缩短为 45 天

最近全球互联网安全界的热点之一是苹果公司 10 月 10 日提出的缩短 SSL 证书有效期为 45 天的国际标准提案，笔者当时本想写篇文章说一说这事，但是最终还是决定等等，看看业界的反应后再讲这事。两个月过去了，这事在国外反映强烈，还在持续热议中。但是，国内好像一点反应都没有，甚至我同客户当面交流说起这事时，都没有什么大的反应，估计还是“狼还没有来”的心态。所以，笔者认为还是有必要写篇文章讲一讲这事。

一、 缩短 SSL 证书有效期已成定局，国际业界严阵以待

笔者在此之前写过两篇相关的文章《对策研究 | 谷歌要革全球 CA 的命，怎么办？》、《90 天 SSL 证书倒计时开始，您准备好了？》，重复的话今天就不讲了，大家可以参考阅读这两篇文章。

本文讲一下最新的情况，缩短 SSL 证书有效期为 90 天是谷歌去年 3 月份提出的，一年半后，苹果公司提出的方案是 45 天！这是一个阶梯式的缩短过程，计划花两年多的时间把现在的证书有效期的不超过 398 天逐渐缩短到 45 天，具体计划是：

(1) 2025 年 9 月 15 日 至 2026 年 9 月 14 日，证书有效期缩短为 200 天

(2) 2026 年 9 月 15 日 至 2027 年 4 月 14 日，证书有效期缩短为 100 天

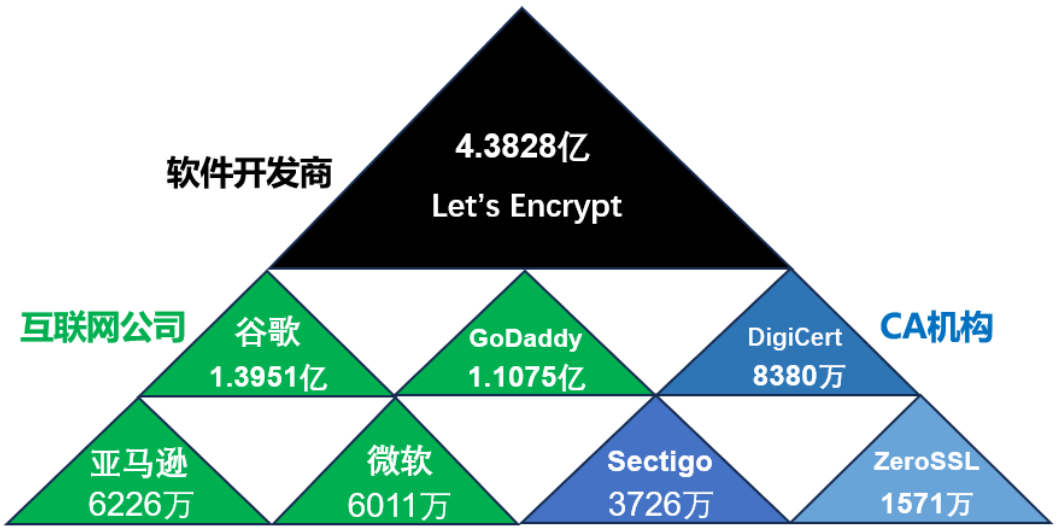
(3) 2027 年 4 月 15 日起，证书有效期缩短为 45 天

此提案比谷歌提出的一下子从 398 天缩短到 90 天稍微温和一点，有一个逐渐缩短的过程，但最终有效期比谷歌提出的 90 天还要少一半。45 天有效期是什么概念？现在是一年申请和安装一次证书，如果缩短为 45 天，则是每个月都要申请和安装一次证书！估计到时候运维工程师就只能天天安装证书了，这就是为何全球 IT 运维工程师们都出来骂人的原因，有人质问苹果：In this proposal: Tell me you've never worked in IT without telling me you've never worked in IT. 这是网上流行的来自 IT 工程师的幽默语，笔者就不翻译了，大家自己体会吧。

也就是说，手动申请和安装 SSL 证书的时代将于明年 9 月 15 彻底终结！因为证书有效期缩短到 200 天，也就是每年至少要折腾两次，即使也只有少数网站已经无法手动完成了，也就是只剩下自动化这一条路了。即使有人说半年安装一次也能接受，则后年的 9 月 15 只能签发 100 天的证书了，每年至少要折腾 4 次，每个季度安装一次证书，则一定是不可能的了。是时候提前做好自动化证书管理的准备了。

该提案目前已经列入讨论日程中，提案通过的可能性有多大呢？那就要看苹果的决心有多大了。2020 年谷歌、苹果和 LE 共同提议把 SSL 证书有效期从当时的 825 天(2 年 3 个月)缩短为现在的 398 天(1 年 1 个月)，CA/浏览器论坛投票结果是提案没通过，因为大多数 CA 都投反对票。但是，苹果单方面决定只信任一年期证书，其他浏览器也跟进，使得这事即使投票没有通过也得到了执行，实现了 SSL 证书有效期从 2 年缩短到了现在的 1 年。所以，大家还是应该相信此事一定会到来，不是缩短为 90 天，而是最终缩短为 45 天！

为了对应这件大事，国际 CA 和国际领先的云服务提供商都已经行动起来了，DigiCert 和 Sectigo 都推出了自己的 SSL 证书生命周期管理解决方案，DigiCert 官网列出的 SSL 证书价格是按每域名每月多少钱，而 Sectigo 则是计划按域名每年收费，而不再是按张证书每年收费。全球领先的云服务提供商都已经全部支持 ACME 自动化配置 SSL 证书。最新的全球前八大 SSL 证书提供商排名和证书签发量如下图所示，全球有效的 SSL 证书数量为 9.7541 亿张，超过 90%的 SSL 证书已经实现了自动化管理，这就是苹果和谷歌推动缩短 SSL 证书有效期的底气，至于有效期为 90 天还是 45 天就不是个问题了，只要实现了自动化，就可以实现任何有效期的自动化签发和部署了。



全球前八大SSL证书提供商排名和证书签发量(2024.12.6统计)

二、 我国 IT 业界应高度重视，提前做好应对准备

鉴于目前我国在 SSL 证书标准方面没有话语权，并且目前 99.99%的网站还是严重依赖于国际 SSL 证书，所以，我国必须高度重视这个影响到所有政府网站、网银系统、各种关键信息基础设施是否能正常运行的 SSL 证书的国际标准的变化，提前做好应对之策，以避免到时导致这些重要的网站系统无法访问。

也许有人说：我国不是在推广普及国密 SSL 证书吗？如果普及了国密 SSL 证书是不是就

没有这个问题了？不是的，为了保证国密 HTTPS 加密安全，国密 SSL 证书也应该同国际标准同步实施相应的证书有效期政策。

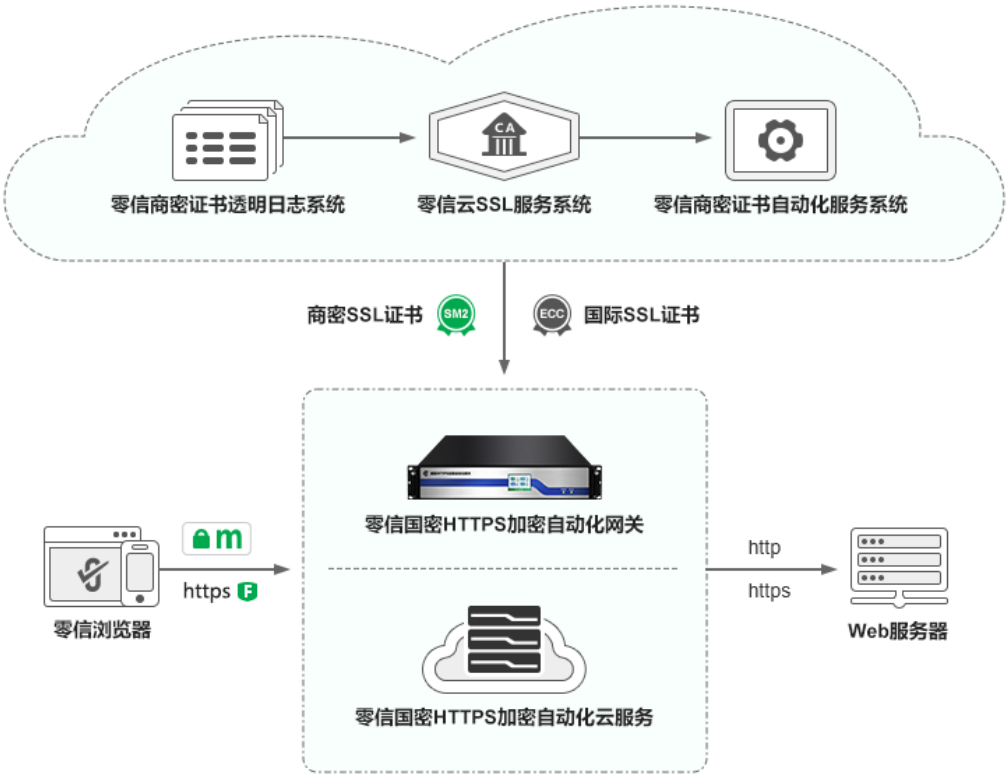
缩短 SSL 证书有效期是为了进一步提升 HTTPS 加密的安全，并为过渡到抗量子算法提前做好准备。唯一可行的解决方案是彻底放弃人工申请和部署 SSL 证书的传统方案，全面实现 SSL 证书的自动化申请和部署。对于我国正在推广的国密 HTTPS 加密改造，必须同时推动国密 SSL 证书的自动化申请和部署，建议所有国密改造方案都是直接一步到位的先进方案，自动化实现国密 HTTPS 加密，而不再采用传统的人工部署国密 SSL 证书和安装国密模块的方案。

这是一个关系到整个 IT 产业的大事，各种需要 SSL 证书实现 HTTPS 加密的应用都需要升级改造支持自动化证书管理，包括政务系统、网银系统、其他所有关键信息系统、SSL VPN 设备、WAF 设备、WAF 云服务、CDN 服务、电子邮件服务、各种物联网设备、各种网关设备等等，否则到时候就会出现大量的系统由于 SSL 证书到期没有续期而导致中断服务，这件大事必须得到高度重视，并提前做好相应的充分的技术准备。

三、 零信技术提供双算法 SSL 证书自动化管理解决方案

零信技术专注于双算法 SSL 证书自动化管理解决方案，为用户提供完整的全线的国密 HTTPS 加密自动化产品，不仅实现了国际算法 SSL 证书的自动化管理，而且实现了国密算法 SSL 证书的自动化管理，实现了原 Web 服务器零改造、自适应加密算法的 HTTPS 加密自动化。

零信 HTTPS 加密自动化解决方案是一个基于零信云密码基础设施的端云一体的密码应用自动化解决方案。其核心产品是零信国密 HTTPS 加密自动化网关，同国际上的证书自动化管理解决方案不同的是：不要求用户在 Web 服务器上安装 ACME 客户端软件，这个要求在重要的政务系统、网银系统和其他关键信息系统不现实。用户原 Web 服务器零改造，不用安装国密算法支持模块，不用安装 SSL 证书，更不用向 CA 购买和申请 SSL 证书，只需在原 Web 服务器前部署零信国密网关即可，由零信网关自动对接零信云 SSL 服务系统完成双算法 SSL 证书的申请和取回部署，零信云 SSL 服务系统对接国际 CA 和国内 CA 获取全球信任的 ECC 算法 SSL 证书和国密合规的 SM2 算法 SSL 证书，实现双 SSL 证书部署，自动化实现 HTTPS 加密和 WAF 防护。



第二个核心产品是零信浏览器，这是目前全球唯一一个完全免费的、支持国密算法、国密 SSL 证书、国密证书透明的、基于 Chromium 内核的高性能通用浏览器，是零信网关的免费配套产品，这两个核心产品使得所有网站都可以零改造实现国密 HTTPS 加密。

零信国密 HTTPS 加密自动化网关最多支持 255 个网站的双 SSL 证书(国密 OV SSL 证书+国际 DV SSL 证书)免费自动配置，已经实现每 80 天自动化更新密钥和签发 90 天有效期证书，支持每天更新密钥和证书，也就是说已经支持缩短 SSL 证书有效期为 2 天，而不只是 45 天！

对于只有少量网站需要实现证书自动化的用户，可以选购零信国密 HTTPS 加密自动化云服务，这是一个把零信国密 HTTPS 加密自动化网关部署在云上共享给最多 255 个网站使用的创新云服务，用户无需购买和部署网关硬件，只需做两次域名解析，自动化实现自适应加密算法的 HTTPS 加密和 WAF 防护，一样自动化为每个网站配置每 80 天自动更新的双算法 90 天有效期 SSL 证书。

45 天新政即将到来，这并不可怕，因为零信技术已经做好的充分的技术准备，可以充足供应零信网关产品来实现 HTTPS 加密自动化，同时自动化实现 HTTPS 方式的 WAF 防护。对于政府网站、银行网站和所有关键信息系统运营单位，必须提前未雨绸缪，提前规划和准备，借国密改造之机，直接采用证书自动化管理解决方案，一步到位实现国密 HTTPS 加密自动化

和 WAF 防护自动化。只有这样才不至于到时被动应对局面，不至于由于 SSL 证书到期而影响重要信息系统的可靠运行和不间断服务。45 天新政不可怕，提前准备是关键。选对技术方案，零改造实现证书管理自动化。

王高华

2024 年 12 月 9 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 195 篇(共 55 万 9 千多字)和英文 82 篇(10 万 5 千多单词)。