对策研究 | 谷歌要革全球 CA 的命，怎么办？

谷歌在 3 月 3 日发布了最新的可信根认证计划相关的政策，在其“Move Forward, Together”(一起面向未来)栏目发布了将来的计划，其中最重要的一件是：

In a future policy update or CA/Browser Forum Ballot Proposal, we intend to introduce:

- **a maximum validity period for subordinate CAs.** Much like how introducing a term limit for root CAs will allow the ecosystem to take advantage of continuous improvement efforts made by the Web PKI community, the same is true for subordinate CAs. Promoting agility in the ecosystem with shorter subordinate CA lifetimes will encourage more robust operational practices, reduce ecosystem reliance on specific subordinate CA certificates that might represent single points of failure, and discourage potentially harmful practices like key-pinning. Currently, our proposed maximum subordinate CA certificate validity is three (3) years.
- **a reduction of TLS server authentication subscriber certificate maximum validity from 398 days to 90 days.** Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on “broken” revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.

在未来的政策更新或 CA/浏览器论坛投票提案中，我们打算引入：

- *从属 CA（中级根证书)的最大有效期。就像为根 CA 引入任期限制将允许生态系统利用 Web PKI 社区所做的持续改进工作一样，从属 CA 也是如此。 通过较短的从属 CA 生命周期促进生态系统的敏捷性将鼓励更健壮的操作实践，减少生态系统对可能代表单点故障的特定从属 CA 证书的依赖，并阻止潜在的有害实践，如密钥固定。 目前，我们建议的最长从属 CA 证书有效期为 3 年。*
- *将 TLS 服务器身份验证用户证书的最长有效期从 398 天减少到 **90 天**。 缩短证书生命周期鼓励自动化部署实践，这些实践将推动生态系统摆脱巴洛克式(繁琐的)、耗时且容易出错的颁发流程。这些变化将允许更快地采用新兴的安全功能和最佳实践，并提高将生态系统快速过渡到抗量子算法所需的敏捷性。缩短证书生命周期还将减少生态系统对“破烂不堪的”吊销检查解决方案的依赖，这些解决方案无法解决故障，进而提供不完整的保护。 此外，较短生命周期的证书将减少意外的证书透明日志系统被禁用的影响。*

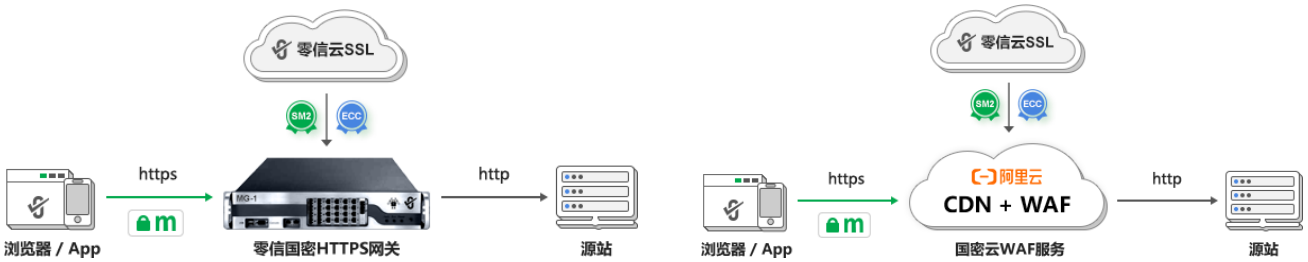
SSL 证书有效期从以前 10 年、5 年降到 3 年、2 年，再降到 1 年(2020 年 9 月 1 日)，也就是 3 年时间内就要从 1 年有效期降到 3 个月有效期。Sectigo 在 3 月 7 日的网络讨论会说估计年内会落实实施，这绝对是一个重磅炸弹！我国用户做好只能申请 90 天有效期的 SSL 证书的准备了？答案是没有！

SSL 证书在我国网站的普及率本来就很低(少于 20%)，一方面是不重视网站机密信息的加

密保护，另一方面则是申请和安装 SSL 证书很麻烦。现在，每 90 天就要去重新申请一张新的证书，重新安装证书，这简直是要了网管的命！这一变化一定会进一步打击用户部署 SSL 证书的积极性，可能会导致大量的网站在 SSL 证书过期后不再费力去申请和安装 SSL 证书！怎么办？我国的 CA 产业界、网络安全产业界和云服务提供商必须为此拿出对策！

其实，谷歌在发布这个政策计划时已经为用户指明了方向，那就是马上尽快采用 ACME 客户端实现证书自动化管理，只有这样才能避免 SSL 证书繁琐的人工申请和人工部署和人工续期。但是，ACME 服务不支持国密 SSL 证书，所幸的是，零信技术已于 1 月 6 日推出了国密 ACME 服务，包括国密 ACME 客户端软件—SM2cerBot 和国密 ACME 服务系统，能帮助用户实现自动化申请和部署双算法双 SSL 证书(ECC SSL 证书和 SM2 SSL 证书)。但遗憾的是，由于安装国密 ACME 客户端软件的同时必须先卸载原 Nginx Web 服务器系统，必须重新安装改造后的支持国密算法 Nginx 系统，这样才能使得 Web 服务器支持国密算法和国密 SSL 证书，但这对用户的业务系统伤害很大，所以，笔者认为 ACME 也不是用户所需要的解决方案！

怎么办？零信技术已经为用户提供了两个可行的解决方案：部署国密 HTTPS 网关或启用国密云 WAF 服务，实现现有 Web 服务器零改造，自动化配置双算法双 SSL 证书，这就不怕谷歌或者国际标准要求只能签发 90 天证书了，90 天内由网关或云服务自动化对接零信云 SSL 系统实现自动化申请新的 SSL 证书并自动化部署好。有了零改造的自动化部署方案，哪怕是将来的某一天证书有效期缩短为 1 天，都可以妥妥的应对！



笔者在阿里云在线访谈节目-云谷创新谈和在深圳商密协会讲座上都在强调实现 SSL 证书

自动化部署的重要性，现在看来，这个自动化部署不再是需要推广的方案，而是必须执行的方案了！这值得各大网站管理员、各个云服务提供商高度重视，值得 SSL 证书相关的各方高度重视，各种云服务提供商必须尽快提供自动化证书申请和部署服务，各个用户网站必须尽快决定采用何种解决方案来解决这个即将带来的“革命”，因为每 90 天去手动申请证书和部署证书已经成为不可操作的事情了，一定会发生由于证书到期而忘了续费的事件，这样一定会影响业务系统的正常运行。

以上都是看得见的问题，但是还有一个大家可能看不到的问题，那就是这件事对 CA 业务的冲击也许比对用户的影响更大，试想一下，现在支持 ACME 自动化部署的免费 90 天 SSL 证书已经高达 80%，如果收费 SSL 证书也必须是 90 天有效期，那还会有用户愿意花钱去购买收费 SSL 证书？这不是要革了 CA 的命吗？哪里是要“一起面向未来”哦！谷歌真会讲故事！由谷歌和火狐浏览器领头的 90 天免费 SSL 证书已经占领了全球超过 60%以上的市场份额，而谷歌这一次的强势要求缩短 SSL 证书有效期，必将进一步加速他们的市场占有率，传统 CA 机构的前景堪忧，必须好好思考该往哪个方向走了。

笔者在多个会议上给出的建议是 CA 机构必须改变观念，改变以前只是销售 SSL 证书的传统观念，因为用户需要的是 https 加密，而不是 SSL 证书！应对即将到来的 90 天证书有效期政策的唯一解决方案是为用户提供自动化部署 SSL 证书解决方案，而不是销售 SSL 证书！零信技术在一年前就开始探索这个解决方案，并且已经找到了唯一可行的方案，欢迎广大 CA 机构合作共同应对“90 天证书革命”。

王高华

2023 年 3 月 14 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。