新动向：2026 年 5 月 13 日支持缩短 SSL 证书为 45 天

2025 年 12 月 8 日

相信广大读者已经了解了 SSL 证书有效期将于明年 **3 月 15 日**缩短为 200 天，但是新的方向标是 Let's Encrypt 计划明年 **5 月 13 日**正式支持自动化签发 45 天有效期证书，比国际标准要求的 2029 年 3 月 15 日签发 47 天证书提前了两年十个月！这是绝对是一个方向标，笔者大胆预测国际标准也许会更改缩短 SSL 证书有效期时间表，本文讲一讲这个关系到所有 SSL 证书用户的大事。

一、 解读 Let's Encrypt 发布的新计划

Let's Encrypt 是 SSL 证书自动化的发起厂商，也是国际标准 RFC 8555 (自动化证书管理环境，ACME) 的制定牵头单位，同时也是占领全球 SSL 证书市场接近 **50%**市场份额的免费 CA 机构，位于第二位的谷歌信任服务(GTS)市场份额为 14%。Let's Encrypt 于 12 月 2 日在其官网发布了"提前缩短 SSL 证书有效期为 45 天"的计划，具体有：

(1) **2026 年 5 月 13 日：**将支持签发 **45** 天有效期 SSL 证书，用户只需使用其 tlsserver ACME 配置文件即可。该配置文件为自愿使用。

(2) **2027 年 2 月 10 日：**将默认 ACME 配置文件改为签发 **64** 天有效期 SSL 证书。

(3) **2028 年 2 月 16 日：**将默认 ACME 配置文件改为签发 **45** 天有效期 SSL 证书。

请读者朋友再对齐一下国际标准制定的时间表：

(1) **2026 年 3 月 15 日：**缩短 SSL 证书有效期为 200 天。Let's Encrypt 从 2015 年就一直免费签发 90 天有效期证书，而本次发布的早鸟计划直接改为 45 天，而不是等到 2029 年 3 月 15 日。

(2) **2027 年 3 月 15 日：**缩短 SSL 证书有效期为 100 天。Let's Encrypt 则是从 2027 年 2 月 10 日起签发 64 天有效期证书，提前一个多月，证书有效期缩短了 34 天。

(3) **2029 年 3 月 15 日：**缩短 SSL 证书有效期为 47 天。Let's Encrypt 则是提前了一年多签发 45 天有效期证书。

请注意：谷歌是在 2023 年 3 月 3 日首次提出了缩短 SSL 证书有效期为 90 天的标准提案，那个时候 Let's Encrypt 和谷歌 GTS 就一直在免费提供 90 天有效期 SSL 证书，并且 Let's Encrypt

市场份额已经是第一位(接近 50%)，谷歌 GTS 为第 4 位，现在谷歌 GTS 已经是第二位。如果 Let's Encrypt (火狐浏览器背景)、谷歌(谷歌浏览器)和苹果(Safari 浏览器)再次联手的话，则极有可能会修改国际标准提前实现 47 天！

二、 为何需要提前缩短 SSL 证书有效期？

我把这个问题分别问了一下 Grok 和 DeepSeek，都印证了笔者想到的理由，总结一下主要有如下两点：

1. 作为证书自动化领导者，必须给业界做出表率和制定新的方向标。

Let's Encrypt 本来就一直在提供 90 天有效期证书，而国际标准的妥协方案是先缩短为 200 天再缩短为 100 天，Let's Encrypt 已经有了 10 年的自动化证书签发经验，作为行业领导者不能满足于仅满足国际标准的要求，而应该提前缩短证书有效期，给业界做一个表率和制定一个方向标，实现其根本目标：构建一个更安全、自动化程度更高的全球互联网安全基础环境。

2. 量子计算机临近实用，可能需要提前做好后量子密码迁移准备工作。

Let's Encrypt 科研团队和主要赞助商包括谷歌、亚马逊、思科等应该已经评估到量子计算机可能会提前到来，可破解当前密码算法的量子计算机临近实用，更短的证书生命周期意味着全球互联网可以更快地强制切换到新的、抗量子攻击的密码算法。量子计算是推动缩短证书有效期这一行业趋势的 "终极压力"和长期驱动因素。Let's Encrypt 的提前调整，不仅是为了应对眼下的威胁，更是为即将到来的密码范式转变铺平道路，确保互联网基础安全能够平滑、快速地过渡到后量子密码时代。

三、 不再观望，越早行动损失越小！早行动早收益！

SSL 证书自动化管理是非常成熟的技术。从 2019 年成为 RFC8555 国际标准到现在已经成熟运行 6 年多，自动化签发的全球信任的 SSL 证书超过 100 亿张，目前全球超过 90%的 SSL 证书都是自动化签发的，很遗憾，这么成熟的技术在我国没有得到普及应用，直到最后三个月了大多数用户还在计划抢购最后一批一年期证书，这真的是很不理智的采购行为。

既然 SSL 证书自动化是必须的，为何不早点采用呢？早点采用不仅可以省掉不必要的采购证书费用，而且可以早点不再为多个系统部署 SSL 证书操心，选择零信技术双算法 SSL 证书自动化管理解决方案可以实现一次微改造完成五大技改目标：

(1) 轻松完成双算法(SM2/ECC) SSL 证书自动化管理改造，从此再也不用花钱买证书了，再也不用安装 SSL 证书了；

(2) 自动化完成所有系统的国密 HTTPS 加密合规改造，保证顺利通过密评；

(3) 自动化完成商密算法和后量子密码混合算法的 HTTPS 加密，即刻保障宝贵数据资产在现在和量子时代的持续安全；

(4) 自动化完成 WAF 防护改造，解决原采购的 WAF 设备不支持证书自动化的难题；

(5) 自动化完成 IPv6 改造，原 Web 服务器无需支持 IPv6。

鉴于 Let's Encrypt 具备主导制定国际标准的能力，由于自身已经提前缩短了 SSL 证书有效期，证明了继续缩短 SSL 证书有效期是可行的。所以，为了避免国际标准提前缩短证书有效期而急于应对，不如现在就行动起来，马上实施 SSL 证书自动化，同时完成后量子密码迁移，真正采用切实可行的技术方案来保障关键信息基础设施系统的机密数据的持续安全，切实保障组织的持续健康发展。早行动，早收益，少损失。

王高华

2025 年 12 月 8 日于深圳
