解读 Sectigo 2024 年预测七：证书有效期将缩短，所有组织都应积极应对挑战

零信技术国际 SSL 证书战略合作伙伴 Sectigo 本月在其官网博客栏目发布了 2024 年数字安全领域的七大预测，笔者利用周末时间翻译并解读了这七大预测。

今天解读预测七：证书有效期将缩短，所有组织都应积极应对挑战。

正如 Sectigo 这篇文章所讲，90 天有效期的 SSL 证书一定会到来，但是会在 2024 年的哪一天到来，现在还未知，浏览器厂商和 CA 界还在博弈，我们不能心存侥幸而不提前为此做好准备。未雨绸缪才能从容应对将来的变化，因为业务系统的可靠不间断运行是企业的生命线，这不能不高度重视。

业界到底该如何应对这个挑战，Sectigo 并没有提出更多的解决方案，只是简单提了一下其 SCM 系统，这并不能解决我国所面临的问题—普及商用密码来实现 HTTPS 加密。我国应该如何应对缩短数字证书有效期的挑战，推荐读者朋友读一读笔者先前写的四篇博客文章-《90 天 SSL 证书对策一：政务篇》、《90 天 SSL 证书对策二：企业篇》、《90 天 SSL 证书对策三：云平台篇》和《90 天 SSL 证书对策四：CA 篇》，这 4 篇文章针对不同的行业提供详细的解决方案。

这里再在这里总结一下零信技术提出的应对缩短 SSL 证书有效期挑战的解决方案，那就是三个字-自动化，只有自动化才能彻底解决问题，手动申请证书和部署证书将成为不可能。而国际上在服务器上安装一个 ACME 客户端软件的自动化解决不了我国面临的难题，我国需要普及商密 HTTPS 加密，唯一解决方案只有两个：部署国密 HTTPS 加密自动化网关和启用国密 HTTPS 加密自动化云服务，由网关或云服务来自动对接零信云 SSL 系统，自动化为网站配置双算法 SSL 证书，自动化实现自适应加密算法的 HTTPS 加密，满足用户国密合规和全球信任的应用需求。这是唯一可行的解决方案，不是方案之一。

为了应对 2024 年可能到来的 SSL 证书有效期缩短为 90 天，所有网站业主能做的是年底做好投资预算，在明年这个政策正式实施之前一定会给大家一个足够完成改造的过渡期，这时候有钱就好办事，只需到时及时采购网关或云服务即可完成所有网站和业务系统的自动化实现 HTTPS 加密，切实保障重要的网站和业务系统不会因为无法应对 90 天证书而影响业务系统的可靠持续运行。

危机也是机遇，也是商机，为即将到来的 90 天证书危机提供正确的解决方案，也是 CA 机构、云平台厂商赢得市场的机遇。所以，无论组织规模大小，都应该通过采取积极主动的行动

来应对这些挑战并变得更强大，确保网站和业务系统不会因为无法正常实现 HTTPS 加密而受影响，确保在数字时代实现安全的持续增长。

岁末将至，新年来临，零信技术愿携手所有合作伙伴和用户共同迎接即将到来的 2024 年的各种挑战，特别是 90 天 SSL 证书的挑战，这是保障互联网服务和数据流通传输安全的最大挑战。

<下面请读者朋友仔细阅读原文译文>

数字证书的寿命将继续缩短。随着领先的浏览器厂商继续推动缩短数字证书的寿命，企业在更新数字证书方面将面临一个令人头疼的问题。企业必须做好准备，对长期徘徊在阴影中的安全基本面游戏规则改变进行重新评估。

企业正在为 2024 年的巨变做准备，该巨变有可能破坏其数字安全协议的基础。各种数字证书的最大有效期正在缩短，随着业界领先机构越来越相信短期证书从根本上讲更加安全，这一趋势将继续下去。在未来的一年里，企业将在自动化解决方案上进行大量投资，以便他们能够为即将到来的缩短证书有效期做好准备。随着支持所有数字流程和应用环境的数字证书的有效期的不断缩短，企业将面临的重大挑战是无法跟上所需的新的证书更新节奏。

一项即将采取的行动是：主流根认证计划厂商将缩短 TLS/SSL 证书有效期到 90 天。谷歌浏览器在其*“携手共进”(Moving Forward, Together)*网站上明确指出了其强制缩短证书有效期这一举措的计划。组织将面临升级其流程和系统以适应这些新的、短期证书的挑战。即将到来的向更短的证书有效期的转变需要一种积极主动的自动化方法，迫使企业重新评估和调整其安全基础，以应对持续转型的应用环境。

这个缩短证书寿命的大门已经开始徐徐打开，这是基本事实。

数字证书的演变

长期以来，SSL 数字证书一直是在线安全的基础上，以实现通过互联网进行安全通信和数据传输。此类证书由 CA 机构签发，以验证 Web 服务器的身份，并确保用户连接到合法和安全的平台。然而，形势正在迅速变化，企业必须面对这样一个现实，即随着短期证书成为新常态，其所有关键证书的寿命将大大缩短。

传统的手动证书管理会损害组织的数字状态，因为手动流程不足以处理短期证书的管理和续订。寿命较短的证书更安全，因为证书错误、密钥被盗或其他问题的风险窗口更小。他们还通过在生产中更快地循环证书来创建更多的加密敏捷系统。

但是，寿命较短的证书就需要更频繁的续订，如果这些续订未能按时正确进行，各种业务系统、应用程序或功能可能会停止工作或停止正常工作。这可能导致服务中断、收入损失、违反服务协议、违规以及降低客户满意度。

引领潮流的浏览器

这场即将到来的剧变背后的驱动力是领先的浏览器厂商为增强在线安全性而做出的共同努力。谷歌浏览器的提议是率先在行业内开展合作，以支持更严格的控制和对新出现的威胁做出更快的响应，其他主流浏览器可能会采取类似的政策。尽管这一举动无疑旨在加强网络安全，但其连锁反应将导致企业修改其整个企业范围的证书策略。

及时无缝地更换证书的需求至关重要，因为一旦新策略生效，这些安全风险的基本要素将变得越来越具有挑战性。企业可能因此而突然倒下的预测并不夸张，这是一个严峻的现实，需要立即关注和战略规划。

缩短证书寿命的推动力

除了浏览器推动更短的证书寿命外，还有其他事件表明，较短的证书已成为网络安全的广泛趋势。2023 年采用的 S/MIME(安全多用途互联网邮件扩展)证书基线要求将电子邮件证书的期限限制为两年或三年，这是有史以来第一次，预计未来的工作将所有 S/MIME 邮件证书限制在两年内，没有例外。同样，主流的可信根认证计划将根证书的有效期限制为 15 年，并计划弃用此前的更长有效期的根证书，这些可信根认证计划最终希望将根证书的最长生存期缩短到 7 年。

这反映了业界对缩短证书寿命的价值的普遍认识，并采取了积极行动来实现这些共识。

这些业界计划与缩短数字证书生命周期以应对新出现的威胁并促进更安全的在线环境的大趋势相一致，90 天证书生命周期提案将这一话题推到了每个企业的董事会面前。

不要惊慌，做好准备！

不要恐慌，开始准备。何时实施 90 天证书仍存在不确定性。但它会发生，唯一的问题是什么时候发生。当然也不用惊慌，企业一定会有足够的时间来为此做好充分的准备。

企业应采取的步骤同以前从 2 年期证书缩短到 1 年期证书的操作完全相同：

(1) 发现/可见性：了解所有 SSL 证书在网络中的位置。

(2) 自动化：通过告警、续订和配置实现整个证书生命周期的自动化。

(3) 问责制：定义证书所有权并明确证书生命周期管理的责任。

(4) 策略和流程：使用自助服务工具简化证书申请和批准的流程。

数字证书寿命的转变需要采取积极主动的方法，要求组织重新评估其网络安全战略并加强对迫在眉睫的挑战的防御。

这没有任何不确定性。完全确定。

携手共创安全未来

面对这种迫在眉睫的转变，企业、CA 机构和浏览器厂商之间的协作变得至关重要。开放的沟通渠道对于应对数字证书寿命缩短带来的挑战至关重要。建议企业积极与其 CA 机构合作，随时了解政策变化、行业最佳实践和缓解过渡的潜在解决方案。

战略规划和面向未来

战略性地应对短期证书激增的企业将能够更好地保持整个组织的网络弹性。成功的策略不仅包括制定全面的证书续期计划，还包括针对网络安全格局的进一步变化采取面向未来的安全措施。积极主动的措施，例如实施证书更新自动化和跟上新兴技术的步伐，可以帮助企业保持领先地位。

在 Sectigo，我们有一个通用平台，专门用于管理数字证书的生命周期，使各种规模的企业都能从单一界面全面了解整个证书操作。Sectigo Certificate Manager 与领先的技术提供商集成，可以发现任何组织网络中的任何公共或私有证书，从而将企业与网络攻击和服务中断隔离开来。

归根结底，你无法管理你看不见的东西，因此，随着证书寿命的缩短和后量子密码的出现，变得加密敏捷并准备采用面向未来的解决方案从未像现在这样重要。

把握增长机会

数字环境在不断发展，企业必须适应不断变化的网络安全浪潮，以保护其资产并维护客户的信任。通过采取积极主动的协作方法，企业可以应对这些挑战并变得更强大，确保不会遭遇突然倒下的威胁，而是在数字时代实现增长和弹性的机会。

王高华

2023 年 12 月 28 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。