200 天！100 天！47 天！

今天，国际标准组织-CA/浏览器论坛正式批准了 SC-081v3 提案--缩短 SSL 证书有效期和验证数据重用期。全球信任的 SSL 证书有效期从明年 3 月 15 日起分三个阶段由现在一年有效期分别缩短为 200 天、100 天和 47 天，计划最终将缩短为 10 天！本文讲一讲这个巨变对各利益相关方意味着什么，是危机还是机遇？可以说都是，就看大家如何理解和应对这个巨变了。

一、 为何 SSL 证书有效期一直在不断缩短？对整个数字安全行业有何影响？

SSL 证书从早期的 5 年有效期相继缩短到 3 年、2 年，再到 1 年，这个不断的缩短有效期的核心诉求是为了保证 HTTPS 加密的安全，缩短证书有效期就是缩短私钥的存活期，也就是缩短了攻击者的攻击时间和攻击窗口，从而最大程度减少潜在威胁的风险，确保全球网络安全基础设施保持最新状态。

谷歌在两年前(2023 年 3 月 3 日)首次提出了要推动 SSL 证书有效期从现在的一年缩短为 90 天，意在促进生态系统敏捷性和轻松过渡到抗量子算法。于是，国际标准组织-CA/浏览器论坛开始了漫长的提案讨论，而苹果公司于 2024 年 10 月 10 日又提出了缩短 SSL 证书有效期为 47 天的更新提案，并给出了一个分阶段实施的方案：2025 年 9 月 15 日缩短为 200 天，2026 年 9 月 15 日缩短为 100 天，2027 年 4 月 15 日缩短为 47 天。这个缩短证书有效期的提案在谷歌首次提出的两年后的 2026 年 4 月 13 日获得通过，通过的提案比苹果的提案又推迟了半年施行，推迟两年施行 47 天有效期：2026 年 3 月 15 日缩短为 200 天，2027 年 3 月 15 日缩短为 100 天，2029 年 3 月 15 日缩短为 47 天。这是一个各利益相关方妥协的方案，但无论如何，喊了两年的靴子终于落下了！有用户说终于“狼来了”。

对于数字安全行业来说，这一标准的制定代表着一个重大的转折点，那就是在网络威胁快速发展的时代，一年有效期的静态安全措施已不再足够，敏捷性和主动风险管理必须成为现代安全策略的核心。CA 机构、单位安全团队和 IT 管理员都必须重新考虑这个核心点，确保关键信息基础设施能够处理增加的证书续订节奏，保持运营效率和不影响业务系统正常运转。

除了技术影响之外，这种转变还反映了各行各业正在朝着安全优先的思维方向迈进。不愿意缩短证书有效期的观点植根于便利性，但便利性不再是安全决策的主要驱动力。47 天有效期 SSL 证书政策的落地，不仅仅是一项技术标准的制定，而是数字安全发展的方向标，它标志

着对降低风险、提高敏捷性和促进更具弹性的互联网安全至关重要。虽然挑战很大，但这一政策落地的长期利益将远远超过现在的挑战，强化了在万物互联和 AI 时代必须始终将安全放在首位的原则。

二、 200 天、100 天、47 天证书政策对用户意味着什么？应该如何应对？

200 天对于网站主，也就是 SSL 证书用户来讲，意味着从 2026 年 3 月 15 日起，如果仍然采用手动申请证书和部署证书方式的话，每年必须折腾两次！一个网站尚可接受，10 个、100 个、1000 个乃至 1 万个网站还受得了吗？

100 天对于 SSL 证书用户来讲，意味着从 2027 年 3 月 15 日起，如果仍然采用手动申请证书和部署证书方式的话，每年必须折腾 4 次！一个网站都已经比较困难了，更不说 10 个、100 个、1000 个乃至 1 万个网站了，必须实现自动化证书管理！

47 天对于 SSL 证书用户来讲，意味着 4 年后必须完成所有网站系统的 SSL 证书自动化管理，无论多少个网站，即使只管理一个网站，也不可能一年折腾 10 次！完成了 SSL 证书自动化管理，到时候就可以从容应对后续实施的 10 天有效期政策了。

所以，所有网站主必须从现在开始着手准备实施 SSL 证书自动化管理，必须开始方案规划、方案调研和做好采购预算，必须在明年 3 月 15 日之前搞定双算法 SSL 证书自动化管理，只有这样才能确保网站系统的不间断可靠运行，满足等保、密评和相关法律法规的合规要求。

其实，这个政策对于网站管理员和安全管理员来讲，实在是一个大利好，只要推动 SSL 证书自动化管理改造落地实施，则自己将更加轻松，无需再为每年为大量 Web 服务器更新 SSL 证书而烦恼了。特别是需要完成国密 HTTPS 加密改造的用户，一劳永逸的解决方案就是微改造，只需在现有 Web 服务器前面部署国密 HTTPS 加密自动化网关即可，一次投资，一次部署两台网关，可以为多达 255 个网站系统自动化实现国密 HTTPS 加密和 WAF 防护，免费自动化配置提前满足 2027 年规定的 100 天有效期双算法 SSL 证书，并且是网关硬件系统和 SSL 证书都包用 5 年，5 年安全无忧，不再需要关心申请 SSL 证书和部署 SSL 证书了。当然，更多网站和更大流量的网站系统需要部署更多台国密 HTTPS 加密自动化网关。

三、 200 天、100 天、47 天证书政策对数字安全服务提供商意味着什么？应该如何抓住机遇？

对于数字安全服务提供商，包括系统集成商、云服务提供商、CA 机构等等，这是一个巨大的新商机，这不再是一个销售几千元的 SSL 证书的小生意，而是一个几十万、几百万、几千

万甚至上亿元的大生意！因为所有用户都需要完成这个升级改造，这个产业将是一个上千亿元的大产业。特别是叠加我国必须完成的国密改造和 IPv6 改造强制要求，这是一个难得的一举两得的技术改造市场机会。

对于系统集成商，这个市场机会有两种业务模式，一是代理销售国密 HTTPS 加密自动化网关，帮助用户轻松完成国密 HTTPS 加密改造，完成 WAF 防护改造，完成 IPv6 改造。对于省级或者国家级政务云平台，除了销售 HTTPS 加密自动化网关外，还可以销售政务云 SSL 服务系统，帮助政府用户实现自动化从政务专用 SSL 中级根证书签发政务系统用双算法 SSL 证书，所有政务系统限定部署政务专用 SSL 证书，彻底杜绝各种 SSL 中间人攻击和不受 CA 机构的断供影响。

另一种系统集成商商业模式是为用户提供 SSL 证书自动化管理服务，自己投资采购国密 HTTPS 加密自动化网关，部署在用户机房，按启用的网站数量和按年收费，收费标准可以参考现在的双算法 SSL 证书收费标准。据粗略估算，这个服务模式的投资收益率大大超过销售网关硬件的收益率。这个商业模式是一个双赢方案，政务云平台无需购置国密 HTTPS 加密自动化网关，仍然按现在的每个网站购买双算法 SSL 证书的费用支付给服务商，开通多少网站支付多少钱，前期投入少。而服务提供商的投入不仅得到了高回报，而且无需工程师去给用户安装 SSL 证书，只需点击鼠标为用户开通国密 HTTPS 加密和 WAF 防护服务即可。

对于商业云平台商，必须学习谷歌云、亚马逊云、微软云等国际大厂的成功经验，只需自建云 SSL 服务系统或直接对接零信云 SSL 服务系统，就可以快速为所有云主机用户、CDN 用户、WAF 用户提供双算法 SSL 证书自动化管理服务，可以在云端部署多台国密 HTTPS 加密自动化网关为用户提供国密 HTTPS 加密自动化云服务。

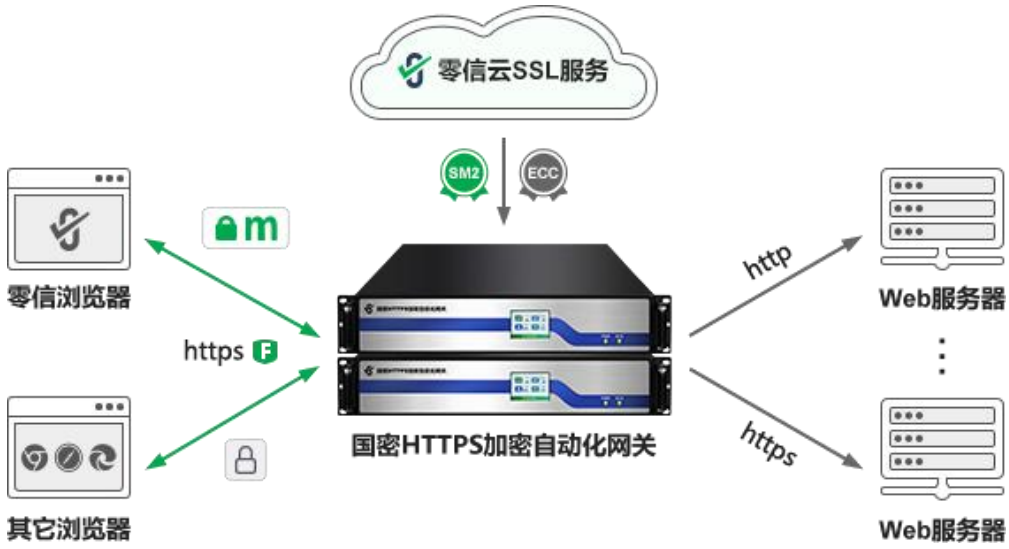
对于 CA 机构，则需要抓紧具备双算法 SSL 证书的自动化签发能力和自动化部署能力，不仅可以为自己的国密 HTTPS 加密自动化网关自动化配置双算法 SSL 证书，还可以为其他网关厂商提供双算法 SSL 证书自动化管理服务，而不再是销售 SSL 证书给用户，而是销售 SSL 证书自动化管理解决方案。零信技术历时 4 年打造了双算法 SSL 证书签发系统和自动化管理解决方案，能助力 CA 机构快速具备这两个核心能力，以最快的方式切入 SSL 证书自动化管理大市场。

对于相关网安厂商和密码厂商，如果其相关网安设备和密码设备(如网关和 WAF)需要 SSL 证书，是时候拥抱 SSL 证书自动化了，为用户提供基于国密 ACME 标准的双算法 SSL 证书自动化管理服务。零信技术作为国密 ACME 标准制定牵头单位，能助力网安厂商和密码厂商快速实现其网安设备和密码设备具备双算法 SSL 证书的自动化管理能力，多通道可靠地为用户签发全球信任的国际 SSL 证书和国密 SSL 证书，以最快的方式切入 SSL 证书自动化管理大市

场。

四、 零信技术早已做好准备，支持每 1 天自动化更新双算法 SSL 证书

零信技术早在 2021 年成立之时就已经认准 SSL 证书自动化管理这个发展趋势大方向，大投入研发国密 SSL 证书自动化管理生态产品，并牵头制定《自动化证书管理规范》密码行业标准，于 2023 年 11 月在第二十五届中国国际高新技术成果交易会上推出了端云一体的 SSL 证书自动化管理解决方案，核心产品是零信国密 HTTPS 加密自动化网关，国内首个通过商用密码产品认证的国密 HTTPS 加密自动化网关，最多支持 255 个网站的双算法 SSL 证书的自动化申请和部署，同时集成高性能的 WAF 防护系统，为用户提供自动化 HTTPS 加密和 WAF 防护服务。而完全免费的国密浏览器—零信浏览器是国密 SSL 证书自动化管理的配套产品，优先采用国密算法实现 HTTPS 加密，支持国密证书透明。



目前已有多家政府机构、高校和银行等单位部署零信国密 HTTPS 加密自动化网关实现了 SSL 证书自动化管理，默认自动化配置的是 90 天有效期的国际 DV SSL 证书和国密 OV SSL 证书，满足用户的全球信任和国密合规应用需求。不仅提前满足了 2027 年 3 月 15 日开始的 100 天证书有效期政策，并且自动化支持 SSL 证书有效期变更的要求，即在 2029 年 3 月 15 日之前会自动化为用户配置 47 天有效期的双算法 SSL 证书而无需用户设置。

更加值得一赞的是：零信云 SSL 服务系统支持多通道签发国际 SSL 证书和国密 SSL 证书，切实保障了无论 CA 机构将来出现什么问题或由于国际形势变化导致的断供事件都不会影响零信云 SSL 服务系统为国密 HTTPS 加密自动化网关自动化配置双算法 SSL 证书。这是零信技术全球独家创新提供的 SSL 证书供应链安全保障措施，彻底解决了单一 CA 供应链而无法保

障 SSL 证书供应安全的难题，从而切实保障了用户网站系统的 HTTPS 加密的永不间断服务。这一点非常值得用户在评估和选择 SSL 证书自动化管理服务商时高度重视。

王高华

2025 年 5 月 16 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 213 篇(共 63 万 2 千多字)和英文 92 篇(12 万 3 千多单词)。