国密 SSL 证书有效期到底应该有多长？

有用户反映，零信浏览器升级到 114 版本后原先 97 版本正常显示国密加密 **m** 标识的中国银行网银网站显示为“不安全”了，在线咨询客服怎么回事，笔者作为零信浏览器的总设计师特撰文讲一讲这个问题，这个问题与 114 版本无关，这是一个关于国密 SSL 证书有效期到底应该有多长的技术问题，也是一个零信技术参与制定的相关国密标准中的待定的问题，笔者认为有必要好好讲一讲这个问题的历史与未来，以期不仅能解答用户的问题，而且能给制定国密 SSL 证书标准中的证书有效期讨论抛砖引玉，有利于业界达成共识。

如下左图所示，这是零信浏览器在内核升级之前显示的中国银行网银系统用户界面，而右图为升级到 Chromium 114 内核后显示的界面，由绿色地址栏变成了“不安全”，其实这与内核版本升级没有任何关系，只是与这次升级改变了 UI 显示规则有关。这个由正常显示变成了“不安全”显示是由于这张国密 SSL 证书有效期为 3 年，2025 年 7 月 12 日到期，而零信浏览器这次升级修订了关于国密 SSL 证书有效期的验证规则，把原先允许国密 SSL 证书有效期超过 1 年改为遵循国际标准的不能超过 13 个月，这样大家就在新版本零信浏览器看到了“ERR_CERT_VALIDITY_TOO_LONG”(证书有效期太长)的安全警告，这是 Chromium 默认的显示为“不安全”规则，只是原先的 97 版本在处理国密 SSL 证书时做了特殊处理，而升级后的 114 版本不再保留这个特殊处理。

那么，为何国际标准要把 SSL 证书有效期确定为不超过 13 个月？为何谷歌又开始推动把证书有效期缩短为 90 天？这是本文重点要讲的问题。

笔者在 2004 年开始代理销售 GeoTrust SSL 证书之时 SSL 证书是可以签发 10 年有效期的，

后来不记得从那一年开始只能签发 5 年有效期了，再后来就是：

- 从 2015 年 4 月 1 日起，只能签发 3 年(39 个月)有效期的 SSL 证书
- 从 2018 年 3 月 1 日起，只能签发 2 年(27 个月)有效期的 SSL 证书
- 从 2020 年 9 月 1 日起，只能签发 1 年(13 个月)有效期的 SSL 证书

2023 年 3 月 3 日，谷歌宣布推动 SSL 证书有效期缩短到 90 天，笔者预计正式生效时间点会在 2024 年的下半年的某一天。大家可以看出，从允许 3 年到 2 年用了 3 年时间，从 2 年变成 1 年用了 2 年半时间，而从 1 年变成三个月(90 天)估计用时 4 年，到了 90 天后，一定还会在某一天缩短到 96 小时(4 天)(短期证书)。

为何国际标准一直在不断地缩短 SSL 证书的有效期？这与 SSL 证书的使用场景和全球算力的不断提升有关，SSL 证书的公钥是公开可见的，任何人或组织都有可能利用其强大的算力试图破解 SSL 证书的密码算法反推出证书私钥，从而达到破解 HTTPS 加密流量的目的。而有效期越短，则给攻击者暴力破解的时间就越短，证书密钥就越安全。为此，虽然用户都希望获得有效期很长的证书，以简化 SSL 证书的管理，但是为了保证证书密钥安全，国际标准组织 CA/浏览器论坛成员单位还是在不断地推动缩短 SSL 证书有效期，因为全球算力在不断增长中，特别是现在的云计算和量子计算发展非常迅猛。

不断缩短 SSL 证书有效期，主要有两大好处：

(1) 更快地实现技术升级 - 更长的生命周期意味着需要更长的时间来有效地推动技术升级。一个真实的例子是证书签名算法从 SHA1 升级到 SHA2 。如果证书有效期是 5 年甚至 10 年的话，除非吊销一大堆证书并强制要求用户重新颁发，否则可能需要数年时间才能替换所有旧证书。SHA1 升级花了 3 年时间，这会产生各种潜在的风险。

(2) 更短的域名验证间隔 - 用于验证身份的信息应该保持信任多长时间？身份验证间隔时间越长，风险越大。谷歌曾表示，在理想的情况下，每隔六个小时就应该重新验证域名控制权。

如果 SSL 证书有效期从现在的 1 年改为 90 天，则传统的手动申请和部署 SSL 证书已经成为不可能，必须实现 SSL 证书自动化管理，自动化申请和部署 SSL 证书。谷歌在推动缩短 SSL 证书有效期为 90 天也是意在推动 SSL 证书的自动化管理，谷歌浏览器在其根认证计划中列出了实施自动化证书管理的六大好处：

(1) 促进敏捷，对于整个生态系统

(2) 增强弹性，对于 CA 机构和网站主

(3) 应对挑战，帮助网站管理员有效应对证书部署规模的不断扩大和部署环境的越来越复

杂

(4) 推动创新，通过对开放社区的持续加强支持

(5) 轻松过渡，到抗量子算法

(6) 管理风险，更好地定位 PKI 生态系统

其实，早在 2015 年谷歌就在 CA/浏览器论坛发起了一个短期证书(4 天有效期)的提案而被否决。但是，最近由谷歌、微软和 Sectigo 发起的弃用 OCSP 的提案已经获得通过，其中有一条就是短期证书中可以没有 CRL 和 OCSP 网址，这也是短期证书的优势之一，包括：

(1) 浏览器不再需要费时去查询 CA 提供的可能访问速度非常慢的 CRL/OCSP 服务，能更快地实现 https 加密和显示加密锁标识，更快的展示网站内容，更好的用户体验。

(2) 证书在 4 天内过期，限制了攻击者获得证书私钥后的使用时间，更有利于保护网站安全。

(3) 大大减少了全球互联网的 CRL/OCSP 查询流量，这也是为何国际标准弃用 OCSP 的原因之一，不仅仅是为了保护用户隐私。

上面讲了这么多缩短 SSL 证书有效期的好处，当然这对网站管理员来讲的确不是一个好消息，网站管理员需要省时省事，当然是希望拿到的证书有效期越长越好，但是对于网站安全来讲，证书有效期就是越短越安全，特别是在后量子时代。这就需要掌握一个平衡点，大家也能从 SSL 证书有效期的不断缩短时间线也能看出这种平衡，是慢慢不断向短推进的过程。所有网站管理员应该做的事情是尽快为 90 天有效期的到来做好充分的准备，这就是为何零信技术投入巨大研发力量研发了国密 HTTPS 加密自动化管理三大解决方案的原因，在 90 天证书有效期到来之前做好技术准备，为用户提供三个可选的解决方案，让用户可以比现在的一年安装一次证书更省事和更省心，只有这样才能让用户能接受不断缩短的证书有效期，做到省事和安全两不误。

那么，国密 SSL 证书有效期到底应该有多长呢？零信浏览器对超过 1 年有效期的国密 SSL 证书给出了“不安全”警示就是我们给出的答案。零信浏览器会参考国际标准同步对不符合国际标准对 SSL 证书有效期的要求的国密 SSL 证书采用一样的处理方式，以保证国密 https 加密的安全，保障部署了国密 SSL 证书的网站安全。

最后讲一下用于内网的 SSL 证书的有效期问题，前面讲过 SSL 证书有效期的不断缩短时间线是一个平衡密钥安全和使用便利的过程，而考虑到内网是同互联网隔离的，很难实现证书自动化管理。所以，笔者认为：用于内网 HTTPS 加密用的 SSL 证书可以适当放宽证书有效期，

因为内网不是公网，其公钥证书遭遇暴力破解的可能性大大降低，适当放宽证书有效期可以在保证密钥相对安全的情况下方便了内网 SSL 证书的部署使用，使得原先明文传输的内网能实现更加安全的内网流量 https 加密，从而有效保障内网流量安全。

王高华

2023 年 8 月 8 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。