

对“谷歌不再信任台湾省中华电信 CA”的深思

谷歌于 2025 年 5 月 30 日在其官方安全博客中宣布：7 月 31 日之后谷歌浏览器 139 版本不再信任台湾省中华电信 CA 的两个根证书(ePKI 和 HiPKI)和匈牙利 CA-Netlock 的根证书签发的 SSL 证书。笔者本不想公开讨论这么晦气的事情，但是这事并没有引起国内业界的关注，这不是好事，所以，笔者决定写篇文章讲讲这事，所有 CA 机构必须居安思危，准备可行的灾备应对之策，而不仅仅是坚信自己严格遵守相关国际标准就不会有问题。更重要的是，所有 SSL 证书用户也都应该在选购 SSL 证书时谨慎选择 SSL 证书提供商，特别是政府和银行等运行关键信息基础设施系统的用户，本文将提供决策指南供参考。

一、SSL 证书的供应链存在很多不稳定的因素

谷歌在公告中写道：“我们建议受影响的网站运营者尽快合理地过渡到新的公众信任的 CA 机构。为避免对网站用户产生不利影响，必须在 2025 年 7 月 31 日之前完成证书替换工作”。目前来讲，这也是用户必须也只能这样做了。但发生这样的事情，最大的受害者是 SSL 证书用户，这对于 SSL 证书用户来讲是非常不公平的事情，但又是非常无奈的事情。其实，SSL 证书用户还可以有避免此类 SSL 证书断供事件发生的更好选择！

笔者不想在此评论这件事情的是非曲直，只是想一想中华电信 CA 为台湾省政务网站和银行网站签发了 3 万多张有效期内的 SSL 证书，这些用户都要重新向其他 CA 申请新的 SSL 证书重新在几万台服务器上部署 SSL 证书，这给这些关基用户带来了多大的痛苦，笔者感同身受。相信国内所有银行 IT 人员也仍然对 2017 年赛门铁克 SSL 证书不被信任时挑灯夜战重新部署 DigiCert SSL 证书时的困难记忆犹新，而那次事件受影响是全球两百多万个网站，几乎全球所有银行网站和许多政府网站部署的都是赛门铁克 SSL 证书，也就是赛门铁克花了 12.8 亿美元收购的 VeriSign 品牌 SSL 证书。这些已经发生的安全事件引起了笔者深思 SSL 证书供应链安全问题。

大家千万不要以为这是小概率事件而不重视，去年 11 月份，谷歌决定不再信任曾经是全球第二大 CA 的 Entrust CA 包括旗下 AffirmTrust 的所有根证书，也使得全球近 60 万用户包括许多银行和政府机构都不得不重新向接手用户的其他 CA 申请和重新安装 SSL 证书！两次不信任案件仅相差半年时间，谁也不知道何时下一个遭遇不信任的是哪个倒霉的 CA 机构，所以，

全球 CA 机构和所有 SSL 证书用户都应该高度重视和思考这个 SSL 证书供应链安全问题。

不仅由于技术层面导致了 SSL 证书供应的不稳定，而且地缘政治一样会导致 SSL 证书供应链断裂问题。3 年前的俄乌冲突发生后，几乎所有俄罗斯政府网站和银行网站的 SSL 证书被吊销和被断供，这当然是极少发生的极端安全事件，但结果也是一个 SSL 证书供应链不安全的问题。

SSL 证书是一个重要的 IT 产品，一个密码产品，一个有多家供应商可以供货的产品。既然是产品就有供应链安全问题，而 SSL 证书作为一个很重要的离不开的安全产品，其供应链存在很多不确定的因素，存在一个如果原供应商无法供货时，用户很难马上选择新的供应商给补上的问题。因为一旦 SSL 证书被吊销，则网站马上就无法正常访问了。即使原 SSL 证书不会被吊销，但被断供，则需要更换供应商，需要重新向新的供应商申请 SSL 证书，拿到证书后还要重新部署到 Web 服务器上去。一个网站还能应付，集约化管理的政务云平台要管理几百个、几千个甚至几万个网站怎么办？这些都是网站管理员必须考虑的问题，特别是有很多网站系统的大型机构，因为所有业务系统都需要一刻也不能中断的 HTTPS 加密服务。

也许有读者朋友会说，必须选购大品牌。赛门铁克当时就是全球第一品牌(承接 VeriSign / GeoTrust / Thawte 等品牌)，一样被“一锅端”。Entrust 曾经是全球第二大 CA，是仅比 VeriSign 晚了 4 年的 CA 机构，一样被“一锅端”。选择第一大品牌也不一定可靠，无辜的用户该怎么办？是否有更好的选择？连全球第一大 CA 也难逃被浏览器不信任的厄运，全球所有 CA 机构是否都应该做好应急灾备工作呢？

二、SSL 证书自动化管理能大大减轻 SSL 证书供应不稳定带来的影响

为了保证 HTTPS 加密安全，国际标准已于 5 月 16 日发布了逐步缩短 SSL 证书有效期的时间表，明年 3 月 15 日缩短为 200 天，2027 年 3 月 15 日起为 100 天，2029 年 3 月 15 日起为 47 天。也就是说，从现在开始，用户在选购 SSL 证书时还需要增加一个考量，必须选择能提供 SSL 证书自动化管理解决方案的供应商，因为手动申请和部署 SSL 证书即将成为不可能。

目前，全球 SSL 证书中超过 80% 以上的 SSL 证书都已经实现了自动化管理，各大云服务提供商和 CA 机构都已经提供了 SSL 证书自动化管理服务(ACME)。试想一下，如果台湾省中华电信 CA 的用户实现了 SSL 证书自动化管理，则只需在服务器上修改 ACME 服务提供商的服务网址即可继续享受 SSL 证书自动化服务，这些用户是影响最小的，这就是实施 SSL 证书自动化管理的好处。

也即是说，SSL 证书自动化管理能大大减轻 SSL 证书供应不稳定带来的影响。如果出现 SSL 证书提供商无法供货或故意断供的情况，传统的人工申请 SSL 证书和部署 SSL 证书的用

户是最痛苦的，而已经实现了 SSL 证书自动化管理的用户就轻松多了，受影响的程度也是比较轻的。这也是谷歌在 2023 年 3 月提出的推动 90 天有效期 SSL 证书自动化时强调的理由之一：提升敏捷性和增强弹性。

作为 SSL 证书用户，不要只关心证书品牌，因为选择大品牌一样也有可能遭遇断供，用户应该关心的是 SSL 证书提供商是否能提供 SSL 证书自动化管理解决方案，并加紧实施 SSL 证书自动化管理，这不仅能大大减轻 SSL 证书管理负担，更重要的是能大大降低如果自己网站部署的 SSL 证书被无奈断供需要重新部署新证书的工作难度，因为谁也不能保证自己正在使用的 SSL 证书什么时候会被断供，SSL 证书的供应链非常脆弱！积极拥抱 SSL 证书自动化才是明智选择，也已经成为必须选择的技术路线。

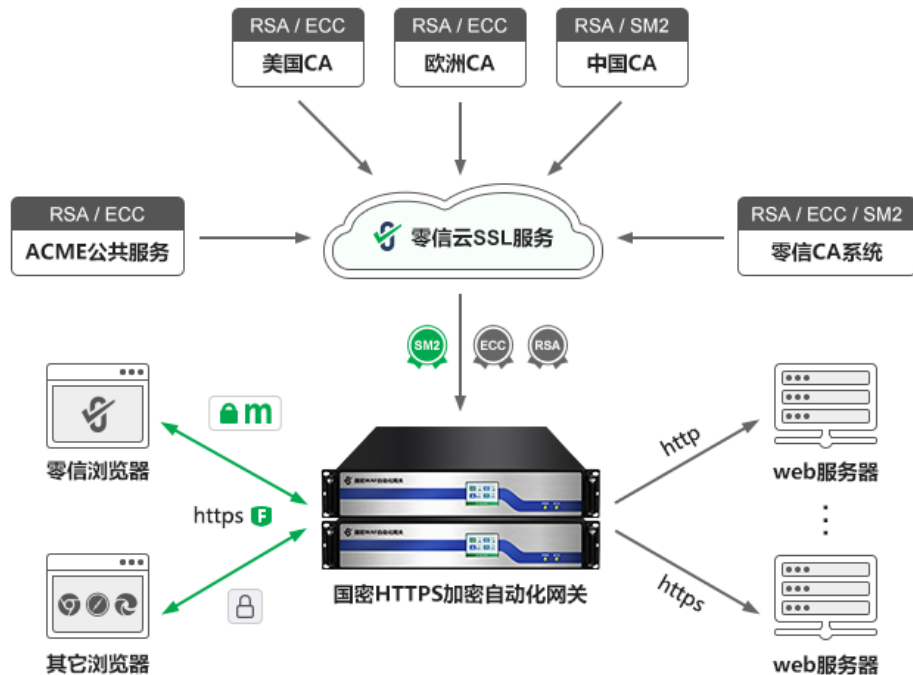
三、 只有实现 SSL 证书自动化管理+多通道签发，才能真正解决 SSL 证书供应链不稳定难题

SSL 证书自动化管理非常重要，也是必选之路。当 SSL 证书提供出现断供时，用户只需切换到其他能提供 SSL 证书自动化管理的 SSL 证书提供商即可，但需要人工手动修改每个网站的 ACME 服务网址和其他参数，需要重启 ACME 服务和重启 Web 服务器，这个对于有成百上千上万个网站需要管理的政务平台、云平台和大机构来讲，这还是一个很大的挑战，而且可能对正在运行的业务有短暂中断。怎么办？

也就是说，要想保障网站系统的不间断可靠运行，仅有自动化还是不够的，特别是有大量网站系统需要管理的大型机构，还需要能自动化切换到其他 SSL 证书签发通道的解决方案。也就是说，仅有自动化证书管理也会由于 SSL 证书供应链的脆弱而变成了半自动化！全球通行的 SSL 证书自动化管理解决方案也其实都只是实现了半自动化，还是有可能因为 SSL 证书供应的脆弱仍然需要人工介入解决 SSL 证书出现断供的事情。怎么办？最佳解决方案就是多通道签发证书+自动化切换通道+自动化证书管理，就是有多个 SSL 证书供应商可以为用户网站自动化签发 SSL 证书，并且有自动化切换签发通道系统，彻底解决 SSL 证书供应链不稳定的难题。

对于我国用户来讲，不仅仅是要解决双算法 SSL 证书的自动化管理难题，还要加上多通道签发和自动化切换签发通道，还要解决 Web 服务器不支持国密算法的难题，特别是，如果 Web 服务器不允许安装 ACME 客户端软件怎么办？这些都是我国网站，特别是政务网站、银行网站等有大量网站系统需要部署 SSL 证书和需要完成国密改造所遇到的技术难题，是否有更好的解决方案呢？

零信技术的创新解决方案是把原先由 Web 服务器承担的 HTTPS 加密任务剥离出来，由零信国密 HTTPS 加密自动化网关来承担自动化证书管理工作，原 Web 服务器零改造，实现 HTTPS 加密的双算法 SSL 证书由零信国密 HTTPS 加密自动化网关负责自动化对接零信云 SSL 服务系统自动化签发和自动化部署，而零信云 SSL 服务系统已经对接了多家国际 CA 和国密 CA，同时还对接了国际 ACME 公共服务系统和零信 CA 系统，实现自动化切换证书签发通道地为用户网站提供双算法 SSL 证书，用户既不需要手动申请和部署 SSL 证书，也不需要担心某个 SSL 证书提供商无法签发 SSL 证书或断供，确保万无一失地保证用户网站系统 HTTPS 加密的不间断可靠运行。



四、SSL 证书供应链稳定，保障网络服务不断

SSL 证书就像所有产品一样都存在供应链安全问题，在当前不稳定的国际环境下，必须高度重视这个问题。所幸的是 SSL 证书是数字产品，已有 SSL 证书自动化管理解决方案，再加上多通道签发和多通道自动化切换，只有这样才能彻底解决 SSL 证书供应链不稳定难题，所有 SSL 证书用户都应该正确选择 SSL 证书自动化提供商，为业务系统提供可靠的自动化证书管理解决方案，从而确保业务系统的不间断的 HTTPS 加密安全运行，保障网络服务的不中断，从而保证国家的长治久安。

王高华

2025 年 7 月 7 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 218 篇(共 64 万 8 千多字)和英文 95 篇(12 万 9 千多单词)。

