零信浏览器优先采用 PQC 算法实现 HTTPS 加密

2025 年 10 月 20 日

零信浏览器更新到 137 版本后，实现 HTTPS 加密的密码算法从优先采用国密 SM2 算法更改为优先采用后量子密码(PQC)算法，这引起有些用户的不解，本文专门讲一讲这个改变的缘由。

一、 零信浏览器为何优先采用 SM2 算法？

零信浏览器定位为一个完全免费的、干净无广告的、支持国密算法和国密证书透明的通用浏览器，虽然用户把零信浏览器定位为一个免费的国密浏览器，那是因为其他国密浏览器都是收费的。零信技术始终认为：我国要想普及国密算法 HTTPS 加密应用，必须有完全免费的浏览器支持国密算法，这个使命当然不能靠一直是完全免费的国外四大浏览器，必须由国产浏览器来承担，这就是零信浏览器承诺永久免费支持国产密码算法的根本原因。

既然零信浏览器定位为一个承担普及国密 HTTPS 加密重任的浏览器，当然是优先采用国密算法实现 HTTPS 加密，并且创新地在地址栏增加显示 m 标识，以便用户一眼就知道网站是否商密合规。

这个优先采用 SM2 算法实现 HTTPS 加密的策略导致了一些未正确部署国密 SSL 证书的网站显示为“不安全”，零信浏览器 114 版本会自动改用 RSA 算法实现 HTTPS 加密，这样用户就看不到“不安全”提示了，但这就违背了优先采用国密算法的原则。所以，137 版本就不再自动改用 RSA 算法了，仍然用 SM2 算法实现 HTTPS 加密，但由于证书链部署不完整或者由于根证书不受信任等问题无法验证证书是否可信，就只能显示为“不安全”，以便用户提醒网站主及时修正部署错误，让商用密码算法真正发挥网站安全保障作用。

二、 零信浏览器现在为何优先采用 PQC 算法？

最新发布的 137 版本，零信浏览器仍然是优先采用国密算法实现 HTTPS 加密，这是针对网站同时支持 RSA/ECC 和 SM2 算法，但不支持后量子密码算法的情况。

如果网站已经支持 PQC 算法，无论网站部署的 SSL 证书是 RSA/ECC 还是 SM2 算法，都会优先采用 PQC 算法实现 HTTPS 加密，这是因为传统密码算法(RSA/ECC/SM2)实现的 HTTPS 加密流量在量子时代是不安全的。攻击者现在就已经开始收集已加密的流量，待量子计算机可用时就可以解密这些已加密的机密信息，这就是“先收集后解密”安全威胁。

为了保障用户提交到网站的机密数据在现在和量子时代的持续安全，如果网站支持 PQC 算法，无论网站部署的 SSL 证书是国际 SSL 证书还是国密 SSL 证书，零信浏览器都会优先采用 PQC 算法实现 HTTPS 加密，并创新地在地址栏显示“Q”标识，明确告诉用户这个网站能保障机密数据在量子时代的持续安全-“量子安全”。

三、 零信浏览器的密码算法优先原则是什么？

零信浏览器支持传统密码算法(RSA/ECC/SM2)实现 HTTPS 加密，同时支持混合后量子密码算法，将来支持纯后量子密码算法，其密码算法优先顺序是：纯国产 PQC 算法(CPQC)、纯国际 PQC 算法、SM2+CPQC 混合算法、SM2+PQC 混合算法、ECC+PQC 混合算法、RSA+PQC 混合算法、SM2 算法、ECC 算法、RSA 算法。

可以看出，零信浏览器是优先采用纯 PQC 算法，再就是混合 PQC 算法，再就是传统密码算法，这三个不同发展阶段仍然是国产密码算法优先，这是零信浏览器的使命和定位，不会变。欢迎 下载 使用全球唯一一个同时支持商用密码和后量子密码的、完全免费的、干净无广告的国产浏览器—零信浏览器。

王高华

2025 年 10 月 20 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 234 篇(共 69 万 5 千多字)和英文 100 篇(13 万 6 千多单词)。