三次国密改造，为何必须一次完成？

2026 年 4 月 28 日

本文的“国密”是指国产密码算法，“国密改造”是指采用国产密码算法改造信息网络系统，本文特指 HTTPS 加密国密改造。我国关基用户面临三次国密改造工作，而不是一次国密改造。但如果用户打算分三次来做的话，不仅浪费钱，更会让关基数据在未来几年内持续暴露于风险之中。一次完成，才是唯一正确的选择。

一、现状：三次必须做的国密改造，一次都不能少

我国从 2012 年启动国密改造，至今已逾 14 年。但很多人没有意识到的是，国密改造并不是“一次过关”的事情，而是至少需要经历三次算法或协议的强制性升级改造。

第一次改造：支持国密 TLCP（国标 TLCP）

这是最基础的强制必须完成的改造，目的是满足《密码法》和密评的基本要求。通过在 Web 服务器上部署国密 SSL 证书和升级支持国密算法实现，或者通过部署国密 SSL 网关实现，让业务系统支持国密 SM2/SM3/SM4 算法 HTTPS 加密。目前已完成的国密改造和通过密评的系统都是停留在这个阶段，甚至还有很多关基系统包括政府官网和政务服务系统、银行官网和网银系统连这一步都还没有完成。

第二次改造：支持基于 TLS 1.3 的新国密标准

TLCP 协议（对标 TLS 1.2）存在一个致命缺陷：**不支持前向安全**。这意味着，一旦证书私钥泄露（而随着证书有效期不断缩短，泄露风险正在急剧上升），攻击者就可以解密所有历史加密数据，政务数据、金融交易数据、客户订单、商业合同、技术图纸、个人隐私，全部暴露。几乎所有单位都在用共享一个私钥的通配证书，因为私钥经过多人多渠道传递，并部署在多台 Web 服务器上，所以极容易导致私钥泄露。更可怕的是：这个私钥泄露很不容易被发现，除非被人在互联网上曝光。

为此，密码行业标准化技术委员会已经正式立项，启动基于 TLS 1.3 的国密协议修订工作，新标准将强制支持前向安全。预计该标准最快于 2027 年底发布。届时，所有已完成 TLCP 国密改造的系统，必须再次升级，否则无法通过密评。

也就是说，**第二次国密改造也是强制的，不是可选项**。

那么，在官方新标准发布之前，我们能不能提前获得前向安全？**当然可以**。国际互联网工程任务组（IETF）已于 2021 年发布 RFC 8998，正式将国密算法纳入 TLS 1.3。关基用户可以先基于 RFC 8998 完成国密 TLS 1.3 改造，提前守护数据安全。**早一天支持前向安全，早一天保护加密数据不被批量解密**。

第三次改造：支持国产后量子密码算法（PQC）

无论国密 SM2 还是国际 RSA/ECC，在量子计算机面前都不堪一击。“先收集后解密”攻击已经真实发生，攻击者现在就在大量收集加密流量，等待量子计算机成熟后批量破解。政务数据、金融交易数据、医疗数据、企业商业机密、个人隐私数据的保密期长达数十年，今天不保护，未来就是裸奔，这将是灾难性的。这就是为何全球迅速实现了互联网流量的 68%已经支持混合 PQC 算法 HTTPS 加密的根本原因。

我国商用密码标准研究院已于 2025 年 2 月启动新一代商用密码算法全球征集（NGCC），也就是国产 PQC 算法标准正在紧锣密鼓制定中。一旦标准发布，所有使用传统公钥算法的系统都**必须**完成第三次改造，迁移到纯国产 PQC 算法。

也就是说，**第三次改造也是强制的，不是可选项**。

这三次改造，每一次都是刚性强制要求，绕不开、躲不过。如果你打算分三次做，每次招标、每次采购、每次停业务改造，不仅总成本高昂，**更致命的是**：在等待第二次、第三次改造的窗口期，你的宝贵数据一直处于风险之中。

二、正确的做法：一次改造，同时完成三次合规升级

既然三次改造都不可避免，为什么不能一次完成？答案是：**完全可以**。

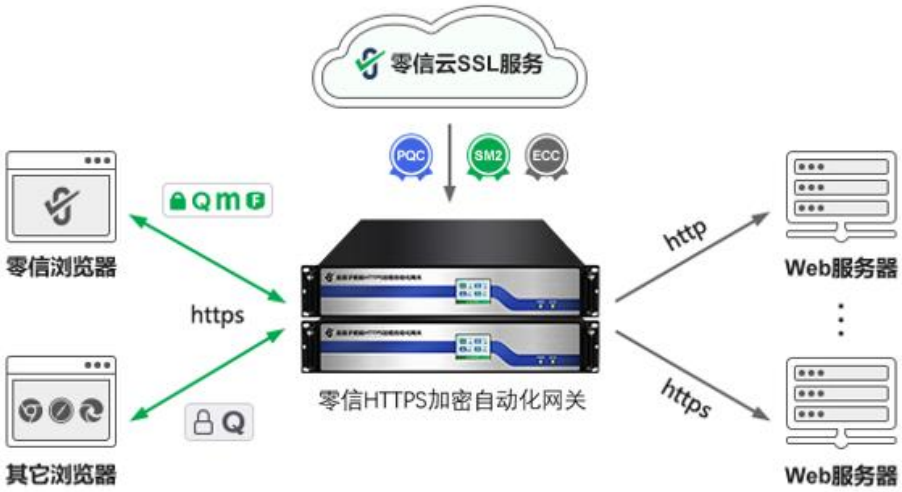
三项改造本质上是在解决同一个问题：**HTTPS 加密通道的安全强度**。差异只是协议版本和算法集的不同。**明智的思路是**：不再去改造每一台 Web 服务器，而是在业务系统前端部署一个支持密码敏捷的安全网关，由网关来承担所有算法协商、证书管理、加密卸载的工作。关基用户无需改动 Web 服务器，无需停机，无需为每次改造重复采购、重复部署。

最正确的国密改造是：一次投资，一次部署，同步实现完成第一次改造、第二次改造和第三次改造。这才是面向未来 5 年必须完成的正确投资。你不需要等到 2027 年新标准发布再改第二次，也不需要等到国产 PQC 标准发布再改第三次。**现在一次改造，可以让你比同行早三年获得前向安全和量子安全。**

三、零信技术的解决方案：一次改造，全部搞定

零信技术推出的 **HTTPS 加密自动化网关**（至少双机热备），正是为此而生。我们不做“头痛医头”的零散改造，而是提供一套能够一揽子解决三次国密改造和证书自动化的一体化硬件设备。

部署方式：自动化网关前置部署于用户数据中心，原 Web 服务器无需任何改造（仅需将域名解析改指向网关）。即使是最老旧的、无法停机的业务系统，也能无缝获得全套安全能力和三个合规要求。



一次改造，同时获得：

(1) **国密 TLCP 支持：**兼容现有国密浏览器，满足密评最低要求。

(2) **国密 TLS 1.3 + 前向安全：**基于 RFC 8998，立即获得前向安全。即使证书私钥泄露（证书有效期越来越短，泄露风险越来越高），过去的所有加密数据也无法被解密。待国标 TLS 1.3 发布后，免费在线平滑升级完成第二次改造。

(3) **国密混合 PQC：**同时支持国密混合 PQC（SM2MLKEM768）和国际混合 PQC（X25519MLKEM768），优先采用国密混合 PQC。今天部署，今天就获得量子安全，比等待国标发布早三年保护宝贵数据。待纯国产 PQC 算法发布后，免费在线平滑无感升级完成第三次改造。

(4) **双证书自动化：**这是实现无缝平滑改造的基础，也是实现 HTTPS 加密的基础。自动化完成国际 DV 和国密 OV 证书的申请、验证、部署、续期，包 5 年双证书，5 年零人工干预。多 CA 自动签发切换，杜绝单 CA 的断供风险。

(5) **内置 A 级 WAF：**一体化 WAF 防护，不会因证书过期失效，原生支持国密 TLCP 和

TLS 1.3 以及 PQC，同步满足等保 2.0 要求。

早改早安全：不要等到 2027 年国标发布才去改第二次，不要等到国产 PQC 发布才去改第三次。**现在一次改造，让你的数据立刻得到前向安全保护和量子安全保护。**

四、三次国密改造一次完成，才是上上策

三次国密改造，不是要不要做的问题，而是什么时候做、怎么做的问题。被动作法：等标准发布再改，宝贵数据在等待中暴露；**明智选择**：立即一次改造，同时覆盖三次要求。

证书有效期越来越短，私钥泄露风险越来越高；量子计算机正在逼近，“先收集后解密”正在发生。你还有时间等第二次、第三次改造吗？

立即行动，一次改造，五年无忧。

王高华

2026 年 4 月 28 日于深圳
