密改新思路—密码敏捷原则

笔者从美国国家标准技术研究院(NIST)最近发布的网络安全白皮书《实现密码敏捷性的注意事项：策略和实践》悟到了一个密改新思路—密码敏捷原则，特撰文分享，以供密码主管部门、关基运营单位、密改从业者和密评单位等决策参考。同时该话题非常值得我国密码业界深入探讨并形成共识，以实现我国后量子密码迁移的“后来者居上”。

一、 什么是密码敏捷性？

根据 NIST 白皮书的定义，密码敏捷性（Crypto Agility）是指在确保安全性和持续运营的同时，替换和调整协议、应用程序、软件、硬件、固件和基础设施中的密码算法所需的能力，这是能够快速、平滑地切换密码算法的架构能力。

密码敏捷性是一种面向未来的应对变化的策略。它要求密码学家、开发人员、实施人员和从业人员之间进行沟通，以应对不断变化的安全性、性能和互操作性挑战。追求密码敏捷能力需要探索新技术和新方案，并且必须针对每种环境制定新的密码敏捷要求。协议、系统和应用程序的安全分析和评估必须包含过渡机制。当过渡机制不可用时，应制定计划实施补偿控制，以缓解密码算法漏洞和不断演变的威胁。

密码敏捷性应作为项目立项、安全架构、安全基线、协议规范和应用程序设计的重要评估项。NIST 建议可以像 IETF RFC 标准有“安全注意事项”部分一样加上“密码敏捷注意事项”部分，以便广泛应用“密码敏捷性”。笔者把这个要求定义为“**密码敏捷原则**”。

二、 密改不能“头痛医头”，应遵循“密码敏捷原则”

我国关键信息基础设施运营单位是强制要求密改单位，所谓“密改”就是采用商用密码来改造现有信息系统，确保其密码应用符合国家有关法规要求。“密评”是商用密码应用安全性评估的简称，是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性等进行评估。密改要求实现“三同步一评估”，即密码应用于系统建设同步规划、同步建设、同步运行，并实现安全性评估。

具体来讲，密改就是一次密码算法迁移工作，从现在的 RSA 密码体系迁移到 SM2 密码体

(C) 2025 零信技术（深圳）有限公司

系，在过去的 50 年里，全球经历了多次密码算法迁移工作，并且每次都经历了漫长的过渡期。如 1977 年启用 DES 算法，2001 正式启用更加安全的 AES 算法，直到 2024 年才禁用 3DES 算法，历时 23 年完成了算法迁移。当然，这些 RSA 密码体系的迁移在我国都是被动接受，并且因为起步晚也许感受不到迁移的痛苦，而商用密码算法的迁移则需要我们自己更新所有系统，这个迁移工作量是巨大了，这就是大家常说的“国密改造难”。

可是，时间不等人，SM2 密码算法改造工作还没有完成，但是参考 NIST 弃用和禁用 RSA/ECC 密码体系的时间表，SM2 密码也必须在 2030 年弃用和 2035 年禁用。这是因为量子科技发展迅速，传统密码算法可以被量子计算机秒破，这就有了现在已经存在的“先收集后解密”安全威胁，先收集现在的已加密的机密信息流量，等量子计算机可用时解密。所以，现在就必须开始实施后量子密码 HTTPS 加密改造，以保证机密数据在量子时代的始终安全。

所以，我国正在如火如荼进行中的商用密码改造同时已经面临紧迫的后量子密码改造工作，这就要求现在的密改不能“头痛医头”（商用密码改造），也不能“脚痛医脚”（后量子密码改造），必须依据密改的要求做好同一规划工作，把商用密码改造和后量子密码改造一并规划，一并建设，一并运行，一并评估，这就是“密码敏捷原则”的具体行动，两次都是密码算法迁移，不如一次统一搞定！这个“敏捷”思路一定能使得我国比欧美更快完成后量子密码迁移工作，因为后量子密码迁移变成了商用密码改造的顺带一同完成的工作，基本上不会再增加太多的改造成本。

三、 自动化是实现密码敏捷必须的技术措施

“密码敏捷原则”的核心有两点：一是密码改造不能影响现有业务系统的**持续运营**，二是密码改造必须确保现有业务系统的**持续安全**。也就是两个“持续”，这是 NIST 提出“密码敏捷性”的核心要求，这是一种能够快速、平滑地切换密码算法的核心竞争力。

要实现两个“持续”，关键在于“自动化”，这是核心。对于 HTTPS 加密，“密码敏捷”能力的顺利实施关键在于是否具备以下两个方面的自动化能力：

1. SSL 证书自动化管理能力

实现 HTTPS 加密必需 SSL 证书，这是基础，而为了缩短传统算力和量子算力破解密钥的窗口，唯一解决方案是缩短证书有效期，这就是谷歌、苹果等业界巨头一直在全力推动缩短 SSL 证书有效期的根本原因，经各方妥协终于达成 2029 年 3 月 15 日缩短 SSL 证书有效期为 47 天的共识，而传统密码算法的弃用时限是 2029 年 12 月 31 日，可以看出这是一个不能再推迟的极限时间。

谷歌提出缩短 SSL 证书有效期的主要理由是促进敏捷性，轻松过渡到后量子密码算法。

(C) 2025 零信技术（深圳）有限公司

这就要求 HTTPS 加密服务具备 SSL 证书自动化管理能力，我国则是双算法(RSA/SM2)SSL 证书，不仅能不断缩短 SSL 证书有效期实现自动化更新证书，而且能自动化更新签发 SSL 证书的密码算法，以便实现无缝切换到纯后量子密码算法 SSL 证书，从而实现纯 PQC 算法的 HTTPS 加密。

2. 密码套件的自动化更新能力

实现 HTTPS 加密的核心是客户端和服务端协商一个安全的密码套件及 TLS 支持协议，每个密码套件和支持协议都有一个 IANA 分配的标识 ID，设计这种机制的目的就是为实现密码敏捷性，方便增加新的密码套件及 TLS 支持协议后能优先采用新的密码算法。这就是“密码敏捷原则”要求的保证业务系统的持续安全。

而要想实现客户端和服务端都能及时支持新的密码套件，客户端浏览器有日常升级更新机制，只需用户允许浏览器自动升级即可。对于服务端，Web 服务器要像实现密码套件的升级需要人工处理，一定会影响正在运行的业务系统。最理想的方案是采用前置网关的方案，Web 服务器无需改造，只要网关支持升级密码算法即可。这也是“密码敏捷原则”要求的保证业务系统的持续运行。

四、 零信技术是“密码敏捷原则”的实践者和领导者

传统的商用密码 HTTPS 加密改造方案是要改造 Web 服务器支持商用密码算法，人工申请国密 SSL 证书并人工部署国密 SSL 证书，这一定会影响业务系统的正常运行，这就不是好方案，不符合“密码敏捷原则”要求的持续运行。零信技术的创新解决方案就是原 Web 服务器零改造的方案，不会影响现有系统的正常运行，先并联行接入零信国密 HTTPS 加密自动化网关，实现双算法 SSL 证书的自动化管理，自动化实现自适应密码算法的 HTTPS 加密，兼容国际算法，优先采用商用密码算法。待零信自动化网关这条新通道部署完成后，就可以停用原先不支持证书自动化的通道，这就满足了“密码敏捷原则”的“持续运营”和“持续安全”的两个核心要求，这就是一个优选的商用密码迁移方案。

对于后量子密码 HTTPS 加密改造，目前国内出现的改造方案是新建设一套量子网络，或者让用户像商密改造一样再买一套支持后量子密码的密码设备，再建一套支持后量子密码的系统，这些都是商密改造走过的弯路，在后量子密码改造绝对不能重滔覆辙的犯同样的错误技术路线！笔者在此特别提醒关键信息基础设施运营单位防止这个技术陷阱，特别是已经开始规划后量子密码改造的银行机构。

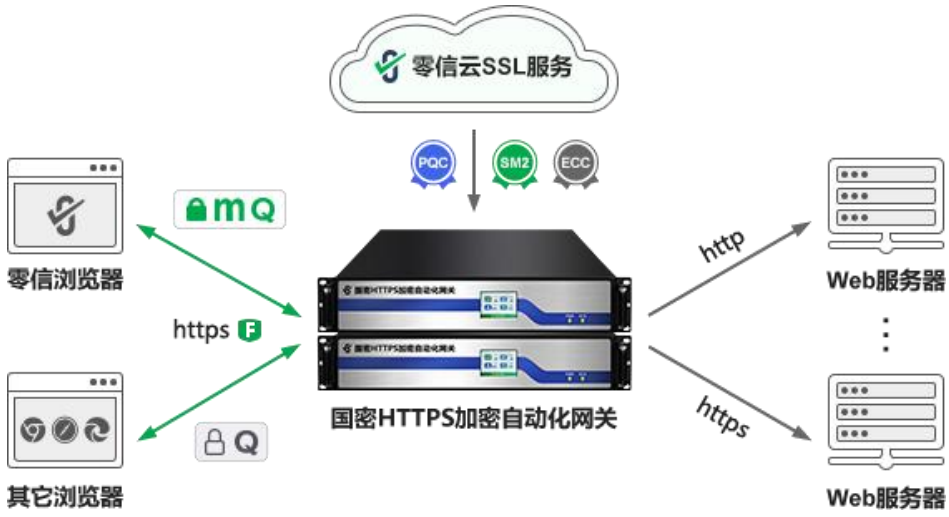
目前国际上的后量子密码 HTTPS 加密迁移方案是完全满足“密码敏捷原则”的两个核心要

(C) 2025 零信技术（深圳）有限公司

求的，首先是后量子密码算法如何使用，那就现在大家已经看到的采用混合密钥封装协议(X25519+MLKEM786)，传统密码算法和后量子密码算法同时使用，这就确保了持续安全。其次是要保证持续运行，这就是 Cloudflare 的方案，直接为用户免费升级 CDN/WAF 服务支持后量子密码混合协议实现 HTTPS 加密，仅用于回源的原 Web 服务器零改造，用户也无需更换正在使用的 SSL 证书，也无需用户申请和配置 SSL 证书，实现无感无缝完成后量子密码迁移，保证了业务系统的持续运营。

零信技术的商用密码 HTTPS 加密改造方案同 Cloudflare 方案有异曲同工之妙，一样是原 Web 服务器零改造，用户无需申请 SSL 证书，无需安装 SSL 证书，也无需安装 ACME 客户端软件，只需部署零信国密 HTTPS 加密自动化网关，就可以无感无缝完成商密 HTTPS 加密改造，完美地从 RSA 密码迁移到商用密码，同时确保了业务系统的持续安全运营，满足“密码敏捷原则”要求。

零信技术即将提供的后量子密码 HTTPS 加密改造方案也是一样的无缝无感完成，只要用户已经部署了零信国密 HTTPS 加密自动化网关，就完全免费完成后量子密码 HTTPS 加密改造，不增加一分钟开支！当然，用户必须使用支持后量子密码的浏览器才能实现后量子密码 HTTPS 加密，首选完全免费的、同时支持商用密码和后量子密码的零信浏览器。这就是遵循“密码敏捷原则”的最佳方案，完美地实现从传统密码到后量子密码的迁移。



零信技术的商密 HTTPS 加密改造方案之所以受到广大用户的厚爱，也正是遵循了 NIST 倡导的“密码敏捷原则”，因为商用密码 HTTPS 加密改造也是一次密码算法迁移。零信技术正在沿着这个创新思路助力用户一样可以顺利完成后量子密码 HTTPS 加密迁移工作，并且是无需增加额外费用。

正如 NIST 白皮书所讲，追求密码敏捷能力需要探索新技术和新方案，零信技术的解决方

(C) 2025 零信技术（深圳）有限公司

案就是针对我国的特定环境所设计的支持密码敏捷要求的创新解决方案，能切实解决我国面临的商用密码和后量子密码迁移难题，一次改造完成两次密码算法的迁移工作，助力我国关键信息基础设施早日完成后量子密码迁移工作，切实保障我国关基系统在现在和量子时代的持续安全。

王高华

2025 年 9 月 8 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 227 篇(共 67 万 7 千多字)和英文 99 篇(13 万 4 千多单词)。

(C) 2025 零信技术（深圳）有限公司