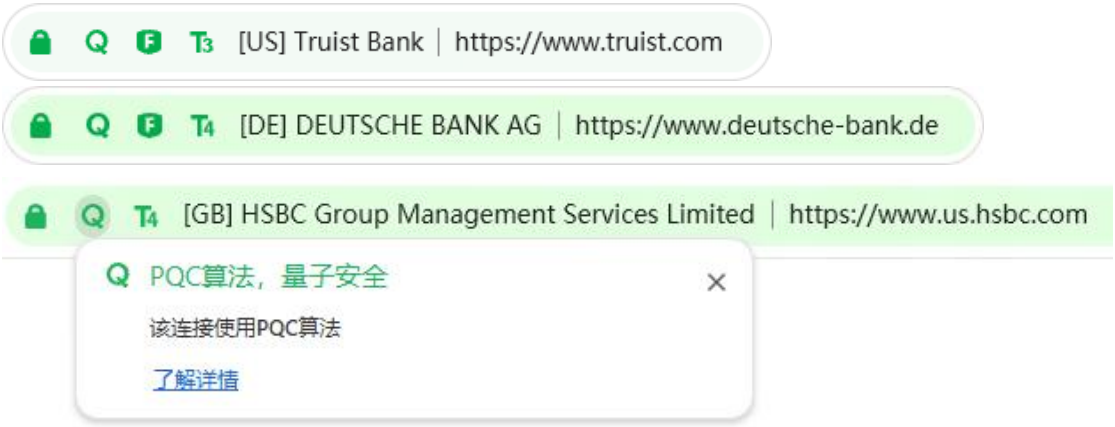
# 美欧网银系统纷纷启用后量子密码 HTTPS 加密

笔者在上上周发表的文章《美英法政府门户网站已启用后量子密码 HTTPS 加密》提到了全球著名支付公司 Visa 官网已经启用了后量子密码 HTTPS 加密，这引起了我国多家银行机构主管们对网银系统实施后量子密码 HTTPS 加密的浓厚兴趣，纷纷私信笔者咨询有关情况，特别是想了解美欧同行的情况。本文就结合他们提出的相关问题再写一个专题文章，以供国家金融主管部门和各个金融机构高管决策参考。

## 一、 美欧银行网银系统纷纷启用后量子密码 HTTPS 加密

笔者在撰写美英法政府网站已启用后量子密码 HTTPS 加密博文时并没有去查询美欧银行官网，只是以笔者了解的 Visa 为例说明金融机构也已经纷纷启用。撰写本文时使用零信浏览器访问了美国前 20 大银行，发现了只有排名靠后的 Truist 银行、汇丰银行北美、第一国民银行(FNBA)、硅谷银行(第一公民银行)等四个银行官网启用了后量子密码 HTTPS 加密，这符合银行越大新技术采用速度越慢的规律。欧洲银行中笔者只发现了德意志银行启用了后量子密码 HTTPS 加密，如下图所示。




## 二、 我国网银系统没有一家启用后量子密码 HTTPS 加密

全球十大银行排名中，我国占了前四大、第 8 和 9 大，这的确是令人欣慰的事情。但是，很遗憾的是，这些大银行的网银系统并没有启用后量子密码 HTTPS 加密。笔者也没有发现其他银行启用，这非常值得我国银行机构反思并尽快采取行动，也非常值得我国金融主管部门高度关注。

为何网银系统必须尽快实现后量子密码 HTTPS 加密呢？因为网银系统的流量都是非常重要的金融机密信息，包括网银账户信息、登录口令、交易口令、交易数据等等，这些机密数据虽然都已经采用 RSA 或 SM2 密码算法实现了 HTTPS 加密保护，但是，现在已经存在“先收集后解密”的安全威胁，攻击者现在收集这些加密的银行数据，等量子计算机可用时就解密这些机密数据，而这些机密的金融数据如交易记录是需要保存多年的，这些机密数据一旦被破解就会给银行和用户带来巨大的财产损失，这个时间点并不遥远，预计是 2030 年，不到 5 年时间了。

所以，为了保障金融数据安全，所有网银系统即使已经实现了 RSA 或 SM2 算法 HTTPS 加密，都必须马上实现后量子密码 HTTPS 加密，早一天实现就早一天保护用户的银行数据在将来的安全，否则将来的后果很严重，也许是灾难性的大批量巨额金钱损失，甚至可能会导致金融系统崩溃。这个极端情况必须现在开始未雨绸缪，防患于未然。

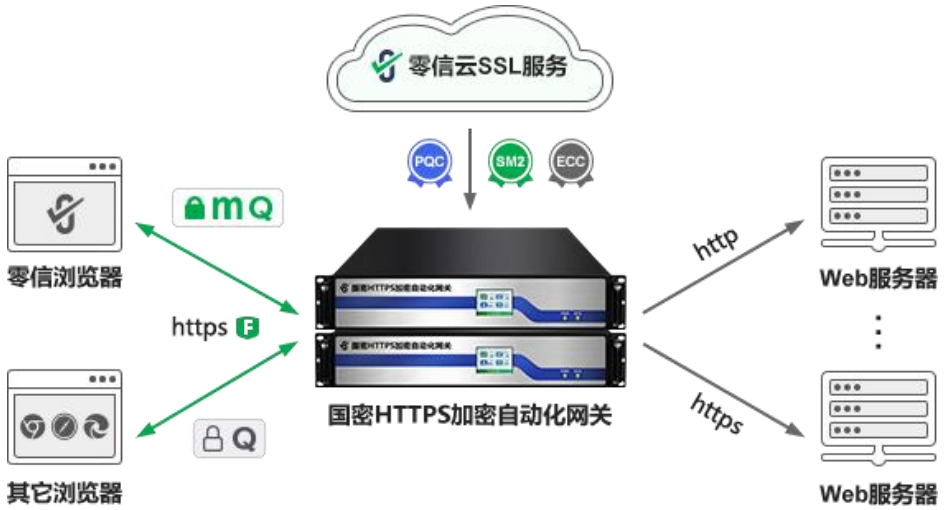
## 三、 一次技改同时完成证书自动化改造、商用密码改造和后量子密码改造，上上策

我国网银系统是最早实现并基本完成商密改造的，所有网银系统都实现了 HTTPS 加密，大多数也都支持商用密码算法 HTTPS 加密。但是，新情况来了，今年 5 月 16 日国际标准制定了不断缩短 SSL 证书有效期的时间表，2026 年 3 月 15 日缩短为 200 天，2027 年 3 月 15 日为 100 天，2029 年 3 月 15 日为 47 天，使得原先人工申请和部署 SSL 证书不再可能，所有网银系统面临 SSL 证书自动化改造问题，必须实现双算法 SSL 证书的自动化管理(自动化申请和自动化部署)，包括国密 SSL 证书和国际 SSL 证书。这是银行目前面临的必须在明年 3 月 15 日之前完成的技术改造之一，也就是说，原先已经完成的商密改造也得重新改造支持双算法 SSL 证书自动化管理，因为原先的改造方案是人工申请 SSL 证书和人工部署 SSL 证书，但是现在不行了，还得继续改造，改造支持国密 SSL 证书自动化管理，以继续必须完成的商用密码 HTTPS 加密改造工作，这是多个法律法规的合规要求。

第二个即将到来的技术改造是后量子密码 HTTPS 加密改造，虽然我国还没有出台相关的法规，但是这是量子科技倒逼出来的刚需，必须马上着手实施，因为早一天完成改造就能早一天保障网银机密数据在量子时代的安全。但是，必须指出的是，这个改造不能走商密改造的弯路，不能又采购一批支持后量子密码的设备再建设一套系统，应该在规划商密 SSL 证书自动化管理改造时，同时考虑后量子密码改造工作，把两次密码算法改造同证书自动化改造一起统一规划和统一实施，这才是上上策。

## 四、 零信技术微改造方案，助力银行轻松完成双密码算法改造

既然 SSL 证书自动化改造、商用密码改造和后量子密码改造都是必须的，零信技术的创新解决方案是一次微改造完成三个必须的改造，这是一个端云一体的、原 Web 服务器零改造的解决方案，只需在原 Web 服务器前面部署零信国密 HTTPS 加密自动化网关，由网关自动化对接零信云 SSL 服务系统，自动化完成双算法 SSL 证书申请、域名验证和证书部署，实现自适应密码算法的 HTTPS 加密和 WAF 防护，让银行可以轻松完成双算法 SSL 证书自动化管理改造，同时轻松完成商密 HTTPS 加密改造。零信浏览器优先采用商密算法实现 HTTPS 加密，同时支持其他不支持商密算法的浏览器采用 ECC 算法实现 HTTPS 加密。




对于必须尽快完成的后量子密码 HTTPS 加密改造，零信技术的创新解决方案是只要用户完成了上述的双算法 SSL 证书自动化改造，部署了零信国密 HTTPS 加密自动化网关，那就自动化实现了基于 ECC 算法 SSL 证书采用 ECC+PQC 混合算法(X25519+MLKEM768)的后量子密码 HTTPS 加密，不会增加一分钱费用，无需再做任何改造。零信技术正在研发实现基于 SM2 算法 SSL 证书采用 SM2+PQC 混合算法(SM2DH+MLKEM768)的后量子密码 HTTPS 加密，预计今年年底上线，到时只需升级零信国密 HTTPS 加密自动化网关即可。零信浏览器下周发布的版本就已经支持 ECC+PQC 混合算法(X25519+MLKEM768)的后量子密码 HTTPS 加密，等零信国密 HTTPS 加密自动化网关支持 SM2+PQC 混合协议 HTTPS 加密后，零信浏览器会发布升级版本实现商用密码算法+后量子密码算法的混合后量子密码 HTTPS 加密。后续待纯后量子密码算法成熟可行时，也只需免费升级零信国密 HTTPS 加密自动化网关和零信浏览器即可，免费升级支持纯后量子密码 HTTPS 加密，帮助银行轻松完成后量子密码 HTTPS 加密迁移工作。

**五、借商密改造东风，领先完成后量子密码改造，保障我国金融安全**

美欧银行网银系统纷纷启用后量子密码 HTTPS 加密，这给了我国银行很好的示范，我国银行界已经有了丰富的商用密码改造经验，现在还需继续努力完成 SSL 证书自动化改造和后量子密码改造，这三个密码改造工作必须统筹规划，绝对不能头痛医头，选择一次改造同时完成三个必须的改造，实现跨越式超越。

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，正是遵循了“密码敏捷原则”，保障了商用密码 HTTPS 加密改造不影响网银系统的持续运行和持续安全，实现了一次改造同时完成 SSL 证书自动化改造、商用密码改造和后量子密码改造，切实解决了我国面临的商用密码和后量子密码改造难题，助力我国金融机构快速完成商用密码改造和后量子密码迁移工作，切实保障我国网银系统和金融交易系统在现在和量子时代的持续安全。

王高华

2025 年 9 月 15 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 228 篇(共 68 万 1 千多字)和英文 99 篇(13 万 4 千多单词)。