密改升级：双证书+双混合PQC，一步改造就位

——面向密改决策者的技术白皮书

数字认证　2026年5月

当前，我国关键信息基础设施的密码应用改造（密改）已进入深水区。从2017年试点到2020年《密码法》实施，再到2024年的《互联网政务应用安全管理规定》的强制执行，还有2025年的《关键信息基础设施商用密码使用管理规定》的重磅发布，各级政府、银行、能源、卫生等关基单位已投入大量密改经费，完成了或正在完成“双证书模式”的部署（同时配置国密SSL证书和国际SSL证书），实现国密合规与全球兼容。

然而，双证书模式只是密改的起点，而非终点。面对量子计算的现实威胁和SSL证书有效期的断崖式缩短，密改必须从“双证书”升级到“双证书+双混合PQC”，并且实现全自动化管理。否则，今天的密改投资将在三年内失效，数据面临“先收集后解密”的风险，运维成本和可靠性也将全面失控。

本文面向密改决策者，阐述密改升级的必要性、技术路径及数字认证的一步到位解决方案，帮助您将密改经费用在刀刃上，一次改造，长期受益。

一　密改现状：双证书模式已广泛部署，但存在三大短板

双证书模式是指Web服务器同时部署国密SSL证书（SM2）和国际SSL证书（RSA），通过自适应算法实现HTTPS加密。这一模式成功解决了国密算法“用起来”的兼容性问题，是当前密改的主流方案。

然而，决策者需要清醒认识到，双证书模式存在三大固有短板：

短板	客户痛点	具体表现
不抗量子	国密SM2与国际RSA均属于传统公钥算法，量子计算机可破解	当前加密的政务、金融数据面临“先收集后解密”风险，未来批量泄露
手工管理	每个网站需同时管理3张证书，申请、验证、部署、续期全人工	证书有效期缩短后，运维成本指数级上升，业务中断风险剧增
无自动化	缺乏多CA签发自动切换能力，依赖单一CA签发	一旦CA断供（如俄乌冲突地缘政治原因、技术故障），所有网站证书失效，业务瘫痪

结论：仅靠双证书模式，既无法应对证书有效期缩短和证书断供的运维危机，也无法保障数据在量子时代的长期安全。密改必须升级。

二　密改升级方向：双证书 + 双混合PQC + 全自动化

2.1 什么是双混合PQC?

双混合PQC是指在密钥交换阶段，同时使用传统密码算法(RSA/ECC/SM2)与后量子密码算法（PQC）进行混合密钥封装。具体包括：

- **国际混合PQC：**X25519 + MLKEM768（即X25519MLKEM768，IANA国际编号4588）
- **国密混合PQC：**SM2 + MLKEM768（即SM2MLKEM768，IANA国际编号4590）

在双混合PQC模式下，Web服务器仍然保留传统密码算法双证书（国密+国际），但密钥交换升级为“传统算法+PQC算法”的混合模式。即使未来量子计算机破解了传统算法，由于PQC部分无法被破解，历史加密数据依然安全。

2.1 什么是双混合PQC?

双混合PQC是指在密钥交换阶段，同时使用传统密码算法(RSA/ECC/SM2)与后量子密码算法（PQC）进行混合密钥封装。具体包括：

◆ **国际混合PQC：**X25519 + MLKEM768（即X25519MLKEM768，IANA国际编号4588）
◆ **国密混合PQC：**SM2 + MLKEM768（即SM2MLKEM768，IANA国际编号4590）

在双混合PQC模式下，Web服务器仍然保留传统密码算法双证书（国密+国际），但密钥交换升级为“传统算法+PQC算法”的混合模式。即使未来量子计算机破解了传统算法，由于PQC部分无法被破解，历史加密数据依然安全。

2.2 为什么必须同时实现全自动化?

SSL证书有效期现在是200天，明年3月15日将缩短至100天，2029年缩短至47天。在双证书模式下，每个网站每年需处理4次、8次、16次证书更新（两张证书）。一个管理着1000个网站的政务云平台，到2029年每年需要完成超过3万次证书操作，这根本不可能靠人工完成。

因此，密改升级必须同时实现双证书自动化：自动申请、自动验证、自动部署、自动续期、多CA自动切换。

2.3 密改升级后的技术架构对比

能力维度	传统双证书模式	升级后：双证书+双混合PQC+自动化
国密合规	✅ 满足	✅ 满足
全球兼容	✅ 满足	✅ 满足
抗量子攻击	❌ 不满足	✅ 满足（双混合PQC）
证书自动化	❌ 手工管理	✅ 全自动，多CA切换
应对证书有效期缩短	❌ 越短越难	✅ 越短价值越大
未来PQC标准演进	❌ 需二次改造	✅ 免费在线升级

三 数字认证一步到位方案：SSL自动化网关

数字认证最新推出的数字认证SSL自动化网关是专门为密改升级打造的软硬一体化设备，帮助关基用户以“一次改造”同时完成双证书自动化、双混合PQC就绪，从容应对证书有效期缩短和量子威胁。

3.1 核心能力

能力	技术实现	客户价值
双证书自动化	对接多家国际CA和国密CA，故障自动切换； 证书自动申请、验证、部署、续期	5年零运维，彻底消除证书过期风险
国密合规增强	率先支持TLS 1.3国密算法，实现前向安全； 默认配置国密OV证书	满足密评最高要求，身份可验证
双混合PQC	独家支持SM2MLKEM768（国密混合）和 X25519MLKEM768（国际混合）	同步抗量子，防御“先收集后解密”
平滑演进	未来我国PQC标准发布后，免费在线升级	保护投资，无需二次改造
内置A级WAF	一体化架构Web安全防护，先HTTPS加密卸载后 流量清洗，真阳率98.06%	免费赠送Web应用防护，等保合规

3.2 部署方式

- ◆ 旁路部署：不改变现有网络架构，原Web服务器零改造
- ◆ 即插即用：1小时内完成部署，即刻双证书自动化生效
- ◆ 规模弹性：推荐双网关负载均衡部署，支持100-255个网站，可集群扩展

3.3 投资回报

以100个网站为例，5年总拥有成本对比：

成本项	传统手工双证书方案	数字认证自动化网关一体化方案
双证书采购（5年）	100张×4888元/年×5 = 244.4万元	**已包含**
人力成本（2人专职）	180万元	**0元**
独立WAF采购	30万元	**已包含**
后量子密码模块	市场无成熟产品，报价50万元	**已包含**
总计	**约504.4万元**	**网关采购价（约50万元）**

小结：节省超过90%的5年总成本，且获得抗量子能力。

四 为什么现在是密改升级的最佳时机？

1. **政策窗口期：**相关法律法规已施行，密评每年一次，不升级将面临合规风险。

2. **技术窗口期：2027年3月15日起，SSL证书有效期将缩短至100天**，2029年将进一步缩至47天。在双证书模式下，每个网站每年需处理8次、20次证书更新（两张证书）。若继续依赖人工管理，一个管理着1000个网站的政务云平台，到2029年每年需要完成超过2万次证书操作！这根本不可能靠人工完成。不实现证书自动化，业务中断将不可避免。

3. **经费窗口期：**密改专项经费仍在预算周期内，将经费用于一劳永逸的升级方案，远比未来二次改造更经济，更省心。

4. **安全窗口期：“先收集后解密”攻击已经在发生**，攻击者现在就已经大量收集加密数据，等待未来量子计算机成熟后批量破解。政务数据、金融数据的保密期长达数十年，早一天实现混合PQC，这些数据就早一天得到抗量子保护；每延迟一天，数据泄露的风险就增加一分。全球已有超过67%的互联网流量实现了后量子密码加密，而我国尚属空白。若不尽快行动，我国关基数据将成为攻击者的“优先目标”。

五 密改经费，投向未来

密改不是一次性任务，而是持续的安全能力建设。将密改经费投入到“双证书+双混合PQC+自动化”的一步到位方案，不仅是应对当前合规的明智选择，更是对未来数据安全的战略投资。

数字认证 SSL自动化网关，已为关基用户准备好这条进化路径。欢迎联系我们的技术团队，获取定制化密改升级方案。

一步改造，同步完成国密改造、证书自动化改造和抗量子就绪；一次投资，五年无忧。