真正实用的 CLM 应该是什么样的？

2026 年 3 月 2 日

随着全球数字化转型的深入与网络安全的严峻化，SSL/TLS 证书已从“可选项”转变为“必选项”。无论是网站、API 接口、物联网设备，还是云原生架构中的微服务，HTTPS 加密已成为保障数据传输安全的基础安全保障措施。而**证书生命周期管理（Certificate Lifecycle Management, CLM）**作为自动化管理 SSL 证书全流程的技术体系，正在成为企业尤其是关键信息基础设施（简称“关基”）运营单位不可或缺的安全保障能力。

值得特别关注的是，从 3 月 15 日起，全球 CA 机构只能签发 6 个月有效期的 SSL 证书，2029 年 3 月 15 日缩短为一个半月(47 天)！这一变化并非单纯的技术调整，而是应对日益增长的证书滥用、中间人攻击与量子计算威胁的主动防御策略。短有效期证书虽提升了安全性，却极大地增加了人工管理的复杂性与出错风险。在此背景下，CLM 从“值得拥有”变为“必须拥有”，而一个真正实用的 CLM 方案，远不止是 SSL 证书“自动续期”那么简单。

本文将从 CLM 的本质、当前关基用户的真实困境、市场现有方案的局限出发，结合零信技术的证书自动化实践与思考，系统阐述一个真正实用、面向未来的 CLM 应具备的核心特质与能力框架，旨在为关基运营单位在选型与建设过程中提供清晰的决策参考。

一、什么是 CLM？为何现在急需 CLM？

CLM，即证书生命周期管理，指的是一套覆盖 SSL 证书从申请、验证、签发、部署、监控、续期到吊销、归档的全流程自动化管理体系。其核心目标是实现 SSL 证书管理的“无人值守”与“零失误”，确保 SSL 证书始终处于有效、合规、安全的状态。

为什么 CLM 在今天变得如此紧迫？主要有以下 4 个原因：

(1) **万物互联皆需 HTTPS，规模化管理成为刚需**

从传统的 Web 服务器到移动 App 后端、API 网关、物联网、车联网、云上容器、边缘节点，甚至工业控制网络中的通信组件，每一个端点都需要 HTTPS 加密传输。一家中型企业可能管理数百张证书，大型集团或关基单位则往往面临数千甚至数万张证书的分布式管理。纯人工台账、表格记录、手工续期的模式早已不堪重负，漏续、误配导致的业务中断事件频发。

(2) **47 天有效期将成为新常态，运维压力指数级上升**

证书有效期将缩短至 47 天，意味着每月都需要完成证书续期操作。对于证书存量庞大的关基单位，这几乎意味着每天都有证书临近过期。自动化续期不再是“效率提升工具”，而是“业务连续性保障”的核心环节。

(3) **合规与审计要求日益严格**

《网络安全法》、《数据安全法》、《密码法》、《关键信息基础设施安全保护条例》等法规均对加密通信提出明确要求。等保 2.0、ISO 27001、PCI DSS 等标准也要求对证书资产进行清点、监控与策略管理。CLM 系统提供完整的证书清单、状态跟踪、策略执行报告与审计日志，是满足合规审计的必备能力。

(4) **应对未来量子计算安全威胁**

量子计算机的发展对未来公钥密码体系构成潜在威胁，并且现在已经存在“先收集后解密”安全威胁。全球业界正在向后量子密码（PQC）迁移。这意味着未来几年，关基单位面临传统 RSA/ECC/SM2 证书与 PQC 证书并存、混合部署、逐步迁移的复杂场景。CLM 系统必须具备算法敏捷性，能够平滑支持新旧算法的证书生命周期管理，否则未来迁移将代价高昂。

实施 CLM 的紧迫性源于规模、频率、合规与未来安全四重压力的叠加。它不再是可选的工具，而是现代企业安全架构中承上启下的关键自动化中台，是必选项。

二、仅有 CLM，能解决关基用户的难题吗？

显然**不能**。对于政府、金融、能源、交通、电信等关基运营单位而言，证书管理自动化只是其庞大安全改造与升级工程中的一个基础环节。关基用户面临的是一个“安全复合型难题”，包括但不限于：

(1) **国密合规和全球信任**

根据相关法律法规要求，关基系统需采用国产密码算法（SM2/SM3/SM4）进行加密与签名。这意味着需要同时管理国际算法（RSA/ECC）与国密算法（SM2）的双证书体系，并确保其能够同时服务于相同或不同的业务场景（如浏览器自适应兼容），同时满足国密合规和全球信任的应用需求。

(2) **后量子密码迁移**

PQC 迁移不仅是一个持续数年、分阶段实施的战略工程，而且是必须现在就开始的紧迫工程。关基单位需要一套能够同时管理国际证书、国密证书及未来 PQC 证书的统一平台，并具备灰度发布、流量调度等高级能力。而且还需要有从混合 PQC 算法到纯 PQC 算法的平滑迁移能力。

(3) **一体化安全防护**

HTTPS 加密解决了传输层安全，但应用层威胁如 OWASP Top 10 攻击、SQL 注入、API 滥用、恶意爬虫等仍需 Web 应用防火墙（WAF）等防护，并且是 HTTPS 加密流量的 WAF 防护，而不是明文 HTTP 流量的防护。这就要求 WAF 设备也必须集成证书自动化能力。

(4) **混合 IT 架构**

关基单位的 IT 资产往往横跨传统数据中心、私有云、公有云、CDN、边缘节点。SSL 证书需要被部署到物理服务器、负载均衡器、云 WAF、CDN 服务商等多个位置。缺乏统一管控会导致“证书孤岛”与安全盲区。

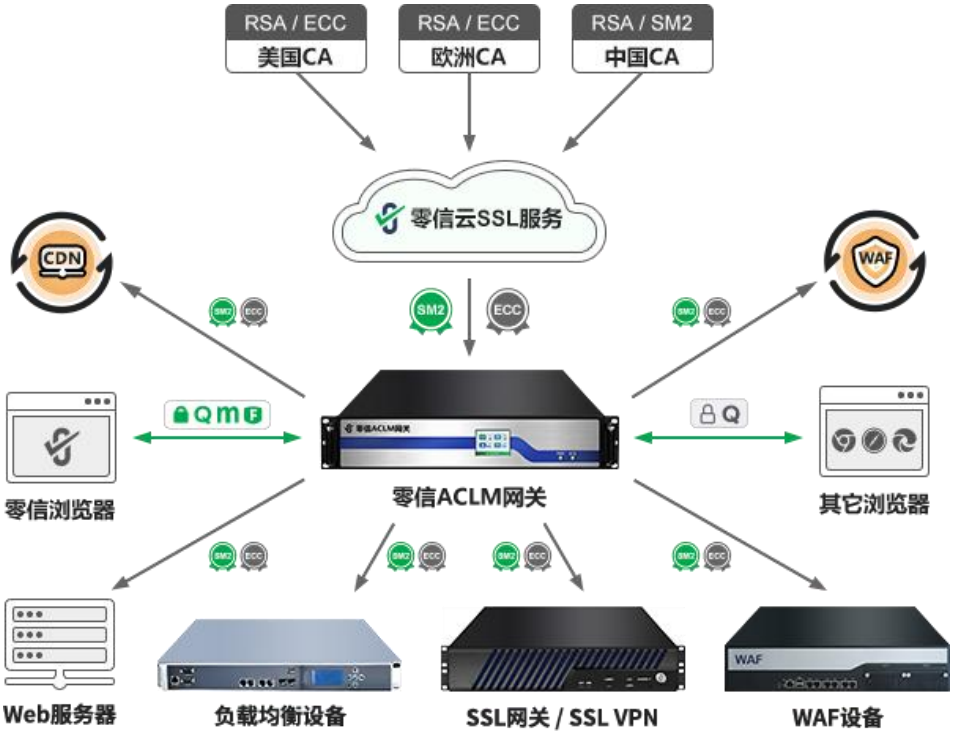
(5) **高可用性与高性能要求**

关基业务系统中断影响重大。证书签发、部署、更新流程必须高可用、低延迟，且不应成为性能瓶颈，尤其在高并发场景下。

因此，关基用户需要的不是一个独立的 CLM 软件系统，而是一个能够深度融合密码能力、安全防护与统一管控的一体化安全基础设施。

三、零信技术 CLM 方案的核心优势：从软件到硬件，从管理到防护

基于对关基用户深层需求的深刻理解，零信技术推出了创新的 CLM 解决方案——集成证书生命周期管理功能的硬件产品—**零信 ACLM 网关**。这不是一个简单的证书管理软件，而是一次从架构理念到交付形式的全面升级，从繁琐复杂的软件部署升级为即插即用的硬件部署，从简单管理升级为综合防护。



零信 CLM 方案具有如下 4 大核心优势：

1. 软硬一体交付，打造安全可信的自动化中台

零信 CLM 方案将 CLM 从“软件方案”升级为“硬件解决方案”，采用了软硬件一体化的集成在 HTTPS 加密自动化网关上的一个功能模块。这样做带来的根本性好处有如下 3 点：

(1) **高可靠与高性能：** 高性能网安硬件提供稳定的计算环境，内置国密与国际密码算法的硬件加速卡，实现 SSL/TLS 握手与加解密的高性能处理。远超纯软件方案的仅提供证书管理服务，是可以自己下场干活(HTTPS 加密)，可用于替代不支持证书自动化管理的传统 SSL 网关的创新产品。

(2) **边界清晰与易于部署：** 作为物理网关设备部署在网络边界或核心区域，无需在每台服务器安装代理软件，原 Web 服务器零改造，不侵入业务系统，不中断现有业务运行，简化架构，无缝部署，大大降低运维复杂度。

(3) **自成安全域：** 网关设备基于高端网安硬件平台，本身具备高强度安全加固，提供内置通过商密产品认证的密码卡，可保障 ACME 密钥和 SSL 证书私钥的安全管理。所有 SSL 证书私钥不出网关硬件，杜绝证书私钥泄露风险，安全级别远远高于传统人工管理证书私钥的多人多途径交接方式。

2. 双算法与后量子密码的“平滑迁移引擎”

零信 CLM 方案内嵌 “双算法证书自动化引擎” ，自动对接零信云 SSL 服务系统，实现多 CA 签发通道自动切换的双算法 RSA/ECC 与 SM2 SSL 证书的申请、验证、签发取回部署、续期等，实现与浏览器自动协商最优算法。更重要的是，这是一个兼容传统密码算法和后量子密码算法的双密码体系就绪架构：

(1) **混合 PQC 算法**：马上实施关键核心业务系统同时支持国际混合 PQC 混合算法 X25519MLKEM768 和国密混合 PQC 算法 SM2MLKEM768 的 HTTPS 加密，优先采用 PQC 算法，并与零信浏览器紧密配合优先采用 SM2MLKEM768 算法，同时满足我国关基用户的国密合规和后量子密码迁移需求。

(2) **纯 PQC 算法**：当 PQC 算法 SSL 证书得到 CA 和浏览器的全面支持后，可通过免费系统升级，无缝增加 PQC 算法 SSL 证书管理能力和纯 PQC 算法 HTTPS 加密能力。

(3) **传统 SM2/ECC/RSA 算法**：不仅支持混合 PQC 算法，而且对于不支持 PQC 算法的国密浏览器优先采用 SM2 算法，而对于不支持 PQC 算法的其他浏览器，则兼容传统 RSA/ECC 算法。

(4) **公网和内网 SSL 证书**：不仅支持自动化管理公网 SSL 证书，而且还可以自动化管理内网 SSL 证书(绑定内网 IP 地址)，实现内外网业务系统的统一管理和统一安全基线。

3. 不止于 CLM，融合 WAF 与统一管控能力

零信 CLM 方案超越了传统 CLM 的范畴，深度融合了关基系统必须具备的以下安全防护能力：

(1) **集成 WAF 防护：** 在提供 HTTPS 加密的同时，对解密后的 HTTP 流量进行实时应用层安全检测与防护，防御 SQL 注入、XSS、CC 攻击等常见 Web 威胁，一举两得，彻底解决用户部署的 WAF 设备不支持证书自动化的难题。

(2) **集群化统一管控：** 通过一个中央管理平台，可统一管理成百上千台分布式部署的服务器和网关设备，以及这些设备所服务的所有 Web 站点、负载均衡器、云 CDN/WAF 服务的证书状态。实现最安全的“一站一密钥一证书”部署管理，彻底杜绝了传统人工证书管理的一张通配证书和一份私钥到处共享使用的不安全部署方式。

(3) **全生命周期可视化：** 提供驾驶舱式可视化大屏，全局展示证书资产地图、到期热力

图、合规状态、算法分布，并提供预警、报表与审计日志。

4. 灵活的部署与服务模式

零信 CLM 方案不仅可以作为独立 SSL 网关替代传统不支持证书自动化的 SSL 网关和 WAF 设备，而且还可以作为现有运行的网关设备的备用网关设备，并为现有设备提供双算法 SSL 证书自动化管理服务。不仅支持为本地设备提供 CLM 服务，而且支持为不在本地机房的云端 Web 应用提供 CLM 服务。

(1) **独立网关模式：** 直接作为 Web 服务器前置网关，提供 HTTPS 加速与卸载、双证书自动化与 WAF 防护。

(2) **证书管理中台模式：** 为现有网络架构（如负载均衡设备、Web 集群）或 CDN/WAF 云服务提供统一的证书供给与更新服务，无需改变现有网络拓扑。

(3) **混合云支持：** 支持在物理机房、私有云、公有云中部署，即插即用，统一管理 Web 服务节点与边缘网关，适应复杂的混合 IT 架构。

四、CLM 硬件化——通往全方位安全防护的必由之路

综上所述，在证书有效期缩短、国密改造深化、量子威胁逼近的“三重刚需”下，一个真正实用的 CLM 方案，必须具备以下特征：

(1) **自动化与智能化：** 全流程自动化，具备智能预警、策略自愈能力。

(2) **密码算法敏捷性：** 原生支持传统密码国际与国密双算法，并同时支持后量子密码算法，优先采用国密混合 PQC 算法，实现平滑 PQC 迁移。

(3) **架构融合性：** 能与常用 CDN/WAF 服务实现无缝集成，形成协同防御。

(4) **企业级可靠性：** 满足关基业务对高可用、高性能、可审计的严苛要求。

(5) **混合环境适应性：** 能够无缝管理云、地、边、端的多形态证书应用资产。

零信技术提出的 **“CLM 硬件化”** 路径，正是对这些需求的集中回应。它通过将 CLM 与密码加速、安全防护、统一管控能力固化于专用的安全硬件中台，不仅彻底解决了证书自动化管理的运维难题，更是一站式解决了关基用户急需完成的国密改造、后量子密码迁移、HTTPS 流量安全防护三大关键防护任务。

未来已来，安全防护体系的升级不再是单点补强，而是面向整体安全能力的架构重塑。选择一款真正实用的 CLM 方案，就是为关基单位的数字业务打造一个既坚固又智能、既能应对当下又能面向未来的安全基石。

零信 CLM 方案—**零信 ACLM 网关**，正是为承担这一使命而生。

王高华

2026 年 3 月 2 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 264 篇(共 77 万 4 千多字)和英文 117 篇(16 万 1 千多单词)。