What should a truly practical CLM look like?

March 2, 2026

With the deepening of global digital transformation and the increasing severity of cybersecurity, SSL/TLS certificates have transformed from "optional" to "mandatory". Whether for websites, API interfaces, IoT devices, or microservices in cloud-native architectures, HTTPS encryption has become a fundamental security measure to ensure secure data transmission. **Certificate Lifecycle Management (CLM),** as a technology system for automating the entire SSL certificate management process, is becoming an indispensable security capability for enterprises, especially operators of critical information infrastructure (CII).

Of note is that, starting March 15, global Certificate Authorities (CAs) can only issue SSL certificates with a validity period of 6 months, shortening to one and a half months (47 days) by March 15th, 2029. This change is not merely a technical adjustment, but a proactive defense strategy against the increasing prevalence of certificate abuse, man-in-the-middle attacks, and quantum computing threats. While shorter-validity certificates improve security, they significantly increase the complexity and error risk of manual management. Against this backdrop, CLM has shifted from being "worth having" to being "essential", and a truly practical CLM solution goes far beyond simply providing "automatic renewal" of SSL certificates.

This article starts with the essence of CLM, the real dilemmas of current critical information infrastructure operators, and the limitations of existing solutions in the market. Combining ZoTrus Technology's automatic certificate management practices and reflections, it will systematically elaborate on the core characteristics and capability framework that a truly practical and future-oriented CLM should possess. The aim is to provide critical information infrastructure operators with clear decision-making references in the selection and construction process.

1. What is CLM? Why is CLM so urgently needed now?

CLM, or Certificate Lifecycle Management, refers to an automatic management system covering the entire process of SSL certificate management, from application, validation, issuance, deployment, monitoring, renewal to revocation and archiving. Its core objective is to achieve "unattended" and "zero-error" SSL certificate management, ensuring that SSL certificates are always in a valid, compliant, and secure state.

Why has CLM become so urgent today? There are four main reasons:

(1) **The Internet of Things (IoT) necessitates HTTPS, making large-scale management a necessity.**

From traditional web servers to mobile app backends, API gateways, IoT, connected vehicles, cloud containers, edge nodes, and even communication components in industrial control networks, every endpoint requires HTTPS encrypted transmission. A medium-sized enterprise may manage hundreds of certificates, while large groups or CII operators often face the distributed management of thousands or even tens of thousands of certificates. The purely manual ledger, table record, and manual renewal model is already overwhelmed, leading to frequent business interruptions due to missed renewals and misconfigurations.

(2) **The 47-day validity period will become the new normal, leading to an exponential increase in operational pressure.**

The shortened certificate validity period to 47 days means monthly certificate renewals are necessary. For CII operators with a large number of certificates, this translates to almost daily certificate expiration. Automated renewal is no longer just an "efficiency improvement tool," but a core component of "business continuity assurance".

(3) **With increasingly stringent compliance and auditing requirements.**

The Cybersecurity Law, Data Security Law, Cryptography Law, and the Regulations on the Security Protection of Critical Information Infrastructure all impose explicit requirements on encrypted communications. Standards such as Cybersecurity Classified Protection 2.0, ISO 27001, and PCI DSS also require the inventory, monitoring, and policy management of certificate assets. A CLM system provides a complete certificate inventory, status tracking,

policy enforcement reports, and audit logs, making it an essential capability for compliance auditing.

(4) **Addressing Future Security Threats in Quantum Computing.**

The development of quantum computers poses a potential threat to future public-key cryptography systems, and the "harvest now, decrypt later" security threat already exists. The global industry is migrating to post-quantum cryptography (PQC). This means that in the coming years, CII operators will face a complex scenario where traditional RSA/ECC/SM2 SSL certificates coexist with PQC SSL certificates, are deployed in a hybrid manner, and are gradually migrated. CLM systems must possess algorithmic agility and be able to smoothly support the certificate lifecycle management of both old and new algorithms; otherwise, future migration will be extremely costly.

The urgency of implementing CLM stems from the combined pressures of scale, frequency, compliance, and future security. It is no longer an optional tool, but a crucial automatic platform that bridges the gap in modern enterprise security architecture, and is therefore a necessity.

2. Can CLM alone solve the problems of CII operators?

Obviously **not**. For critical infrastructure operators such as governments, financial institutions, energy companies, transportation companies, and telecommunications companies, automatic certificate management is merely a fundamental component of their massive security transformation and upgrade projects. CII operators face a "complex security challenge", including but not limited to:

(1) Cryptographic compliance and global trust

In accordance with relevant laws and regulations, CII systems must use SM2 algorithms for encryption and signing. This means that it is necessary to manage a dual-algorithm certificate system that simultaneously supports international algorithms (RSA/ECC) and the Chinese cryptographic algorithm (SM2), and ensure that it can serve the same or different business scenarios (such as browser adaptive compatibility), while meeting the application requirements of both cryptographic compliance and global trust.

(2) **Post-quantum cryptography migration**

PQC migration is not only a strategic project that will last for several years and be implemented in stages, but also an urgent project that must begin now. CII operators need a unified platform capable of simultaneously managing RSA/ECC certificates, SM2 certificates, and future PQC certificates, with advanced capabilities such as canary releases and traffic scheduling. Furthermore, it needs the ability to smoothly migrate from hybrid PQC algorithms to pure PQC algorithms.

(3) **Integrated security protection**

HTTPS encryption only solves transport layer security, but application layer threats such as OWASP Top 10 attacks, SQL injection, API abuse, and malicious crawlers still require protection from Web Application Firewall (WAF). Specifically, this protection should be for HTTPS encrypted traffic, not plaintext HTTP traffic. This necessitates that WAF devices also integrate automatic certificate management capabilities.

(4) **Hybrid IT architectures**

CII operators' IT assets often span traditional data centers, private clouds, public clouds, CDNs, and edge nodes. SSL certificates need to be deployed across multiple locations, including physical servers, load balancers, cloud WAFs, and CDN service providers. A lack of unified management can lead to "certificate silos" and security blind spots.

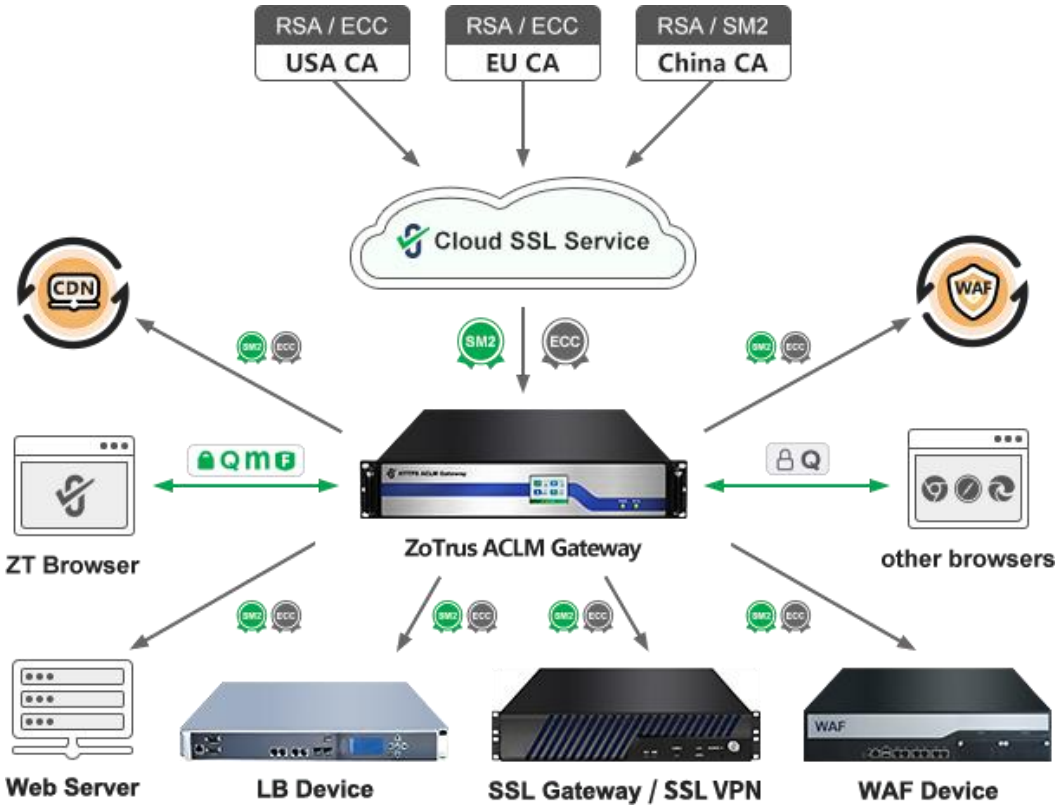
(5) **High availability and high performance requirements**

Disruption of critical information infrastructure has a major impact. Certificate issuance, deployment, and renewal processes must be highly available and have low latency, and should not become a performance bottleneck, especially in high-concurrency scenarios.

Therefore, what CII operators need is not a standalone CLM software system, but an integrated security infrastructure that can deeply integrate cryptographic capabilities, security protection, and unified management.

3. Core Advantages of ZoTrus CLM Solution: From Software to Hardware, From Management to Protection

Based on a deep understanding of the core needs of CII operators, ZoTrus Technology has launched an innovative CLM solution — a hardware product integrating certificate lifecycle management functionality — **ZoTrus ACLM Gateway**. This is not just a simple certificate management software, but a comprehensive upgrade from architectural philosophy to delivery form, from cumbersome and complex software deployment to plug-and-play hardware deployment, and from simple management to comprehensive protection.



ZoTrus CLM solution has the following four core advantages:

3.1 Integrated hardware and software delivery to create a secure and reliable automatic middleware platform.

ZoTrus CLM solution upgrades CLM from a "software solution" to a "hardware solution", employing an integrated hardware and software module on an HTTPS Automation Gateway. This brings three fundamental benefits:

(1) **High reliability and high performance:** High-performance cybersecurity hardware provides a stable computing environment and features a built-in hardware acceleration card for both SM2 and RSA/ECC algorithms, enabling high-performance processing of SSL/TLS handshakes and encryption/decryption. This far surpasses pure software solutions that only

provide certificate management services; it can perform its own tasks (HTTPS encryption) and is an innovative product that can replace traditional SSL gateways that do not support automatic certificate management.

(2) **Clear boundaries and easy deployment:** Deployed as a physical gateway device at the network boundary or core area, it eliminates the need to install proxy software on every server, requires zero modification to the original web server, does not intrude on business systems, does not interrupt existing business operations, simplifies the architecture, enables seamless deployment, and greatly reduces the complexity of operation and maintenance.

(3) **Self-contained security domain:** The gateway device is based on a high-end cybersecurity hardware platform and features strong security reinforcement. It provides a built-in cryptographic card certified by commercial cryptographic products, ensuring secure management of ACME keys and SSL certificate private keys. All SSL certificate private keys remain within the gateway hardware, eliminating the risk of certificate private key leakage. This level of security far surpasses traditional methods of manually managing certificate private keys through multiple parties and channels.

3.2 Dual-algorithm and post-quantum cryptography's "smooth transfer engine"

ZoTrus CLM solution embeds a "dual-algorithm certificate automation engine", automatically connecting to ZoTrus Cloud SSL Service System. This enables automatic switching between multiple CA issuance channels for the application, validation, validation, issuance, retrieval, deployment, and renewal of dual-algorithm RSA/ECC and SM2 SSL certificates, and realize the automatic negotiation of the optimal algorithm with browsers. More importantly, it is a dual-cryptography-ready architecture compatible with both traditional and post-quantum cryptography algorithms.

(1) **Hybrid PQC Algorithm**: Immediately implement HTTPS encryption for critical core business systems that simultaneously support the hybrid PQC algorithm X25519MLKEM768 and SM2MLKEM768, prioritize the use of the PQC algorithm. And it works closely with ZT Browser to prioritize the use of the SM2MLKEM768 algorithm, while also meeting the cryptographic compliance and post-quantum cryptography migration needs for CII operators.

(2) **Pure PQC Algorithm**: Once PQC algorithm SSL certificates are fully supported by CAs and browsers, PQC algorithm SSL certificate management capabilities and pure PQC algorithm HTTPS encryption capabilities can be seamlessly added through free system upgrades.

(3) **Traditional SM2/ECC/RSA algorithms**: Not only do they support hybrid PQC algorithms, but they also prioritize the use of the SM2 algorithm for browsers that do not support the PQC algorithm, while being compatible with the traditional RSA/ECC algorithm for other browsers that do not support the PQC algorithm.

(4) **Internet and Intranet SSL Certificates**: Not only does it support automatic management of Internet SSL certificates, but it can also automatically manage intranet SSL certificates (bound to private IP addresses), achieving unified management and a unified security baseline for internal and external network business systems.

3.3 Beyond CLM, integrating WAF and unified management capabilities

ZoTrus CLM solution goes beyond the scope of traditional CLM, deeply integrating the following security protection capabilities that CII systems must possess:

(1) **Integrated WAF protection:** While providing HTTPS encryption, it performs real-time application-layer security detection and protection on decrypted HTTP traffic, defending against common web threats such as SQL injection, XSS, and CC attacks. It achieves two goals at once and completely solves the problem that the traditional WAF devices deployed do not support certificate automation.

(2) **Clustered and unified management:** Through a central management platform, hundreds or thousands of distributed servers and gateway devices can be managed uniformly, along with the certificate status of all websites served by these devices, load balancers, and cloud CDN/WAF services. This achieves the most secure "one site, one key, one certificate" deployment management, completely eliminating the insecure deployment method of traditional manual certificate management where a single wildcard certificate and a single private key are shared everywhere.

(3) **Full lifecycle visualization:** Provides a cockpit-style visualization dashboard that displays a global map of certificate assets, expiration heatmap, compliance status, and algorithm

distribution, and provides alerts, reports, and audit logs.

3.4 Flexible deployment and service models

ZoTrus CLM solution can not only replace traditional SSL gateways and WAF devices that do not support certificate automation as a standalone SSL gateway, but also it serves as a backup gateway for existing devices, providing dual-algorithm SSL certificate automation management services. It supports CLM services not only for local devices but also for cloud-based web applications located outside the local data center.

(1) **Standalone gateway mode:** Directly acts as a front-end gateway for web servers, providing HTTPS acceleration and offloading, automatic dual SSL certificate management, and WAF protection.

(2) **Certificate management platform mode:** Provides unified certificate provisioning and update services for existing network architectures (such as load balancers, web clusters) or CDN/WAF cloud services without changing the existing network topology.

(3) **Hybrid cloud support:** Supports deployment in physical data centers, private clouds, and public clouds; plug-and-play functionality; unified management of web service nodes and edge gateways; adaptable to complex hybrid IT architectures.

4. CLM Hardwareization – The Inevitable Path to Comprehensive Security Protection

In summary, to meet the demands of shortened certificate validity periods, in-depth reconstruction of cryptographic compliance, and the looming threat of quantum mechanics, a truly practical CLM solution must possess the following characteristics:

(1) **Automation and intelligence:** Full-process automation with intelligent early warning and strategy self-healing capabilities.

(2) **Cryptographic algorithm agility:** It natively supports both traditional international and China algorithms, and also supports post-quantum cryptographic algorithms. It prioritizes the use of the SM2 hybrid PQC algorithm to achieve smooth PQC migration.

(3) **Architecture integration:** It can be seamlessly integrated with commonly used CDN/ WAF services to form a collaborative defense.

(4) **Enterprise-level reliability:** Meets the stringent requirements of critical business operations for high availability, high performance, and auditability.

(5) **Hybrid environment adaptability:** It can seamlessly manage multi-form certificate application assets across cloud, local, edge, and endpoint.

ZoTrus **"CLM Hardwareization"** approach is a concentrated response to these needs. By embedding CLM, cryptographic acceleration, security protection, and unified management capabilities into a dedicated security hardware platform, it not only completely solves the operational and maintenance challenges of automatic certificate management, but it also provides a one-stop solution for the three key protection tasks that CII operators urgently need to complete: Chinese cryptographic transformation, post-quantum cryptography migration, and HTTPS traffic security protection.

The future is here. Upgrading security systems is no longer about reinforcing individual points, but about reshaping the architecture of overall security capabilities. Choosing a truly practical CLM solution means building a robust yet intelligent security foundation for CII operators' digital businesses, capable of addressing current needs while remaining future proof.

ZoTrus CLM solution — **ZoTrus ACLM Gateway** — was created to fulfill this mission.

Richard Wang

March 2, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 117 articles in English (more than 161K words) and 264 articles in Chinese (more than 774K characters in total).