From ACME to ACLM: The Ultimate Path to Automatic Certificate Management

March 16, 2026

March 15, 2026, is a day that will forever be etched into the history of internet security. From this day forward, the 32-year-old annual validity period for SSL certificates will be changed to a semi-annual validity period. This means that the "annual renewal" of certificates we were accustomed to will now be "semi-annual renewal". And this is just the beginning. According to the established timeline, the validity period will be shortened to 100 days in 2027, and it will be finally fixed to 47 days in 2029. When the certificate renewal frequency drops drastically from "annual" to "monthly," any traditional management model relying on Excel spreadsheets and manual renewal will instantly collapse. It is at this historic turning point that we need to re-examine the evolution of automatic certificate management: from **ACME** as the technological foundation to **ACLM** as the ultimate enterprise-level management solution.

1. What is ACME? What is ACLM?

ACME is an abbreviation for Automatic Certificate Management Environment**.** It's both an international standard defined by RFC 8555 and an English word meaning "summit" or "ultimate." In the SSL certificate field, the emergence of the ACME protocol is indeed a revolutionary summit. Its core value lies in solving the problem of certificate automation from scratch: by defining a standardized protocol, web servers can automatically initiate certificate requests to CAs, complete domain name validation, download and install certificates. With certificate validity periods constantly shortening, the importance of ACME is increasingly evident. Without ACME, the short lifespan of each certificate (from six months to one month) would force maintenance personnel into endless manual operations, leading to inefficiency and business interruptions due to any renewal delays. It is estimated that service interruptions caused by expired certificates could result in losses of millions or even tens of millions of dollars for large enterprises. Therefore, the ACME protocol, as the technological cornerstone of automation, ensures that a single website's SSL certificate can be "self-sufficient" in the short term, serving as the first line of defense against the challenge of short-lived certificates.

However, for large and medium-sized organizations with hundreds or thousands of websites, systems, devices, and cloud services, ACME alone is far from sufficient. This leads to **ACLM — A**utomatic **C**ertificate **L**ifecycle **M**anagement. Unlike ACME, which focuses on certificate application and renewal solutions for individual websites, ACLM's core lies in "unified management". It no longer focuses solely on "how to get certificates", but rather on the overall picture: How many certificates are there in the organization's digital assets? Where are they deployed? Which is about to expire? Are there any "ghost certificates" that are no longer valid but are still active? ACLM is a comprehensive certificate management system that integrates certificate discovery, centralized monitoring, automatic application, automatic deployment, compliance auditing, and risk alerts. Its importance lies in its ability to upgrade the fragmented, siloed ACME certificates into a unified, automatic management system covering the entire organization, ensuring that SSL certificates on physical servers, virtualization platforms, container environments, or cloud services can be automatically managed throughout their entire lifecycle on a single platform.

In simple terms, the fundamental difference between ACME and ACLM lies in their different dimensions. ACME is the technical foundation at the "point", solving the technical challenge of "how to automatically apply certificates", serving as a tool for automation. ACLM, on the other hand, is the management and implementation at the "surface", solving the governance challenge of "how to automatically manage all certificates in an organization", providing a security foundation for digital transformation. ACME is the building block of ACLM, while ACLM is the solid fortress built from these building blocks.

2. What should an excellent ACLM solution look like?

A good ACLM solution should not simply be a matter of installing ACME clients in bulk. It should be a future-oriented, intelligent security management hub with the following core characteristics:

First, **comprehensive automation capabilities are fundamental**. An excellent ACLM not only automates certificate application and renewal via the ACME protocol, but more importantly, it automates "discovery" and "deployment". It can search and scan for already applied and deployed SSL certificates by domain name and IP address, automatically building a complete certificate inventory. During deployment, it needs to seamlessly connect to various web servers, traditional SSL gateways,

load balancers, WAFs, and CDNs through pre-built plugins or APIs, automatically pushing issued SSL certificates to the target location and activating them. Simultaneously, it must support the automatic generation of various statistical reports and possess real-time alerting capabilities for automatic deployment failures, transforming operations personnel from "firefighters" to "strategy makers".

Second, **it is essential to embrace heterogeneous environments and hybrid algorithms**. Real-world IT environments are complex, and not all certificates are suitable for automatic application via ACME. For example, OV (Organization Validation) and EV (Extended Validation) SSL certificates, which require strict validation, typically still require manual review processes. A good ACLM should support manual certificate application processes and manage these manually applied certificates centrally, enabling automatic deployment and renewal reminders. More importantly, in the ongoing SM2 cryptographic transformation, it must simultaneously support the automatic management of both RSA/ECC and SM2 SSL certificates, achieving smooth scheduling of dual algorithms and dual certificates to meet the dual requirements of SM2 cryptographic compliance and global trust. Furthermore, to address the existing "harvest now, decrypt later" security threat, the ACLM must detect whether the website system with deployed certificates supports post-quantum cryptography (PQC), rather than simply automating certificate delivery.

Looking at the CLM solutions of leading international vendors such as Sectigo and DigiCert, these trends are evident. Sectigo Certificate Manager (SCM) emphasizes its cloud-native architecture and CA independence, enabling automatic management of certificates from any CA and providing integration with over 50 mainstream technology stacks. User reviews highlight its core value as "centralized lifecycle management, powerful automation options, and clear visibility", replacing the previous chaotic reliance on email and Excel. DigiCert, through its DigiCert ONE platform, emphasizes that automation has shifted from "optional" to "essential" in the context of shortened certificate lifecycles, highlighting its preparation for post-quantum cryptography migration. It aims to help organizations achieve agile upgrades of encryption algorithms through an automatic platform when facing quantum computing threats. DigiCert also demonstrates its ability to integrate with upstream and downstream ecosystems via APIs, enabling policy enforcement, unified views, and granular reporting. These distinctive services all point in the same direction: CLM is no longer just a tool, but a central command system for enterprise cryptographic application strategies. Unfortunately,

these solutions cannot meet our need, because they can only solve the problem of automatic management of RSA/ECC SSL certificates, but cannot address the special need for automatic certificate lifecycle management in China, which requires both RSA/ECC SSL certificates and SM2 SSL certificates.

3. What are the features of ZoTrus ACLM solution?

Since its inception, ZoTrus Technology has been dedicated to providing automatic SSL certificate management solutions using dual algorithms. It has completed a full range of products, from ACME clients to ACME cloud services and ACME hardware gateways, as well as an integrated client-to-cloud automatic certificate management solution. However, these solutions were broken down into more than a dozen different products, addressing only the specific ACME application challenges in different scenarios, but not solving the problem of centralized and unified management for large and medium-sized security service providers. Therefore, these ACME solutions have now evolved into the ACLM solution.

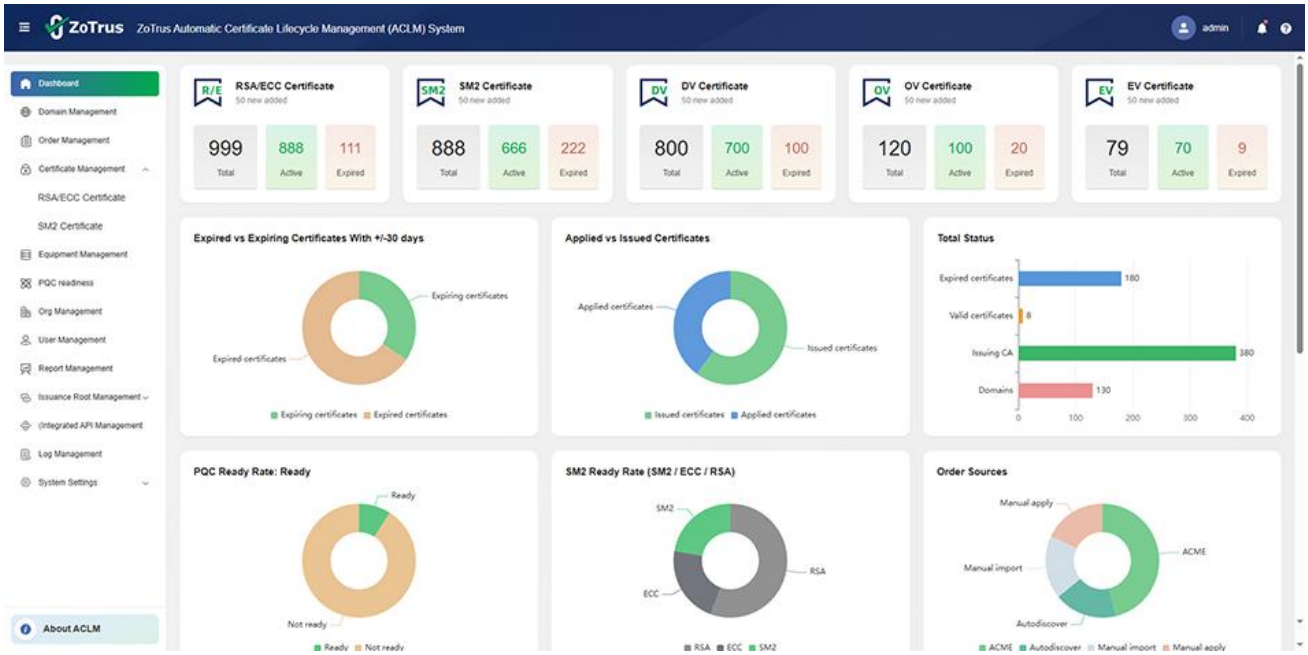
ZoTrus Technology has built a unique ACLM solution matrix, aiming to provide critical information infrastructure operators with an "out-of-the-box" and "self-controllable" centralized and unified automatic certificate management experience. ZoTrus ACLM solution adopts a dual-drive model of "cloud-ground collaboration, edge-cloud integration, and hardware-software integration" to meet the needs of different security levels and deployment environments.

On one hand, ZoTrus offers **ACLM Cloud Service**, a multi-tenant SaaS platform that allows users to easily manage all SSL certificates through a cloud-based web interface. The core highlight of this service is its diverse ACME service capabilities:

- **Standard ACME Service**: Not only does it adhere to international ACME standards and the SM2 ACME standard, but it also offers the world's first free SM2 ACME Public Service. Users only need to deploy the open-source SM2 ACME client software (SM2cerBot) to automatically obtain both a 90-day valid SM2 SSL certificate and an ECC SSL certificate, achieving "one-time deployment, dual-certificate automation". This perfectly solves the "last mile" problem of automating SM2 SSL certificates, a problem that international CLM

solutions cannot address.

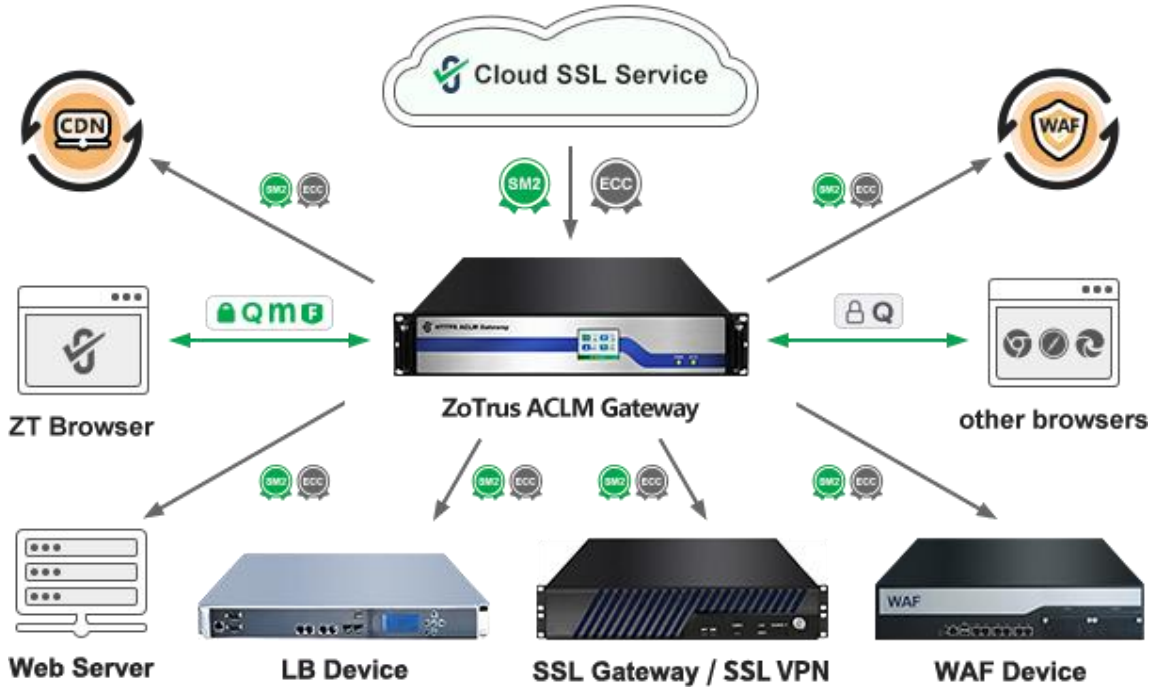
- **The CDN-based ACME service:** offers a deeply integrated ACME solution for users already using CDN service. Certificate application and renewal are automatically completed at the CDN edge nodes, requiring no modifications to the original Web server, allowing users to enjoy global acceleration and automatic dual-algorithm HTTPS encryption. This "CDN + cloud SSL service " model extends automation from the original server to the network edge, greatly simplifying user operations.
- **Support manual certificate application:** For users who need to apply for SSL certificates manually, a traditional manual certificate application service is also provided, including the application for OV SSL certificates and EV SSL certificates. These manually applied and manually deployed SSL certificates are also incorporated into unified management, providing certificate expiration renewal notification services and post-deployment security monitoring services.



On the other hand, for high security requirements and strict demands for 'zero disruption' to existing network services, ZoTrus Technology launched **a locally deployed edition— the ACLM Gateway**. This is not merely a hardware gateway integrating an ACME client, but a comprehensive security device integrating Certificate Lifecycle Management (CLM), certificate automation, SM2 cryptographic transformation, post-quantum cryptography migration, and WAF protection. Its core

innovation lies in the "hardware-based CLM" concept: integrating the CLM module, ACME service, SM2 cryptographic module, post-quantum cryptography module, and WAF engine into a single device deployed in front of the user's business servers. This not only provides automatic certificate management for the connected web servers but also empowers other systems and network devices in the organization's network architecture that do not support certificate automation, achieving unified and centralized management of dual-algorithm SSL certificates for all websites, systems, devices, and cloud services within the organization. This architecture brings revolutionary advantages:

- **Zero impact on business systems**: No software needs to be installed on the user's original server, and no need to stop or modify the existing web server. All HTTPS traffic can be taken over, completely solving the problem of not being able to install ACME client software on old or critical systems.
- **One-stop SM2 transformation**: The gateway has a built-in SM2 algorithm module, automatically providing backend business systems with SM2 HTTPS encryption capabilities, while also being compatible with RSA/ECC algorithms. It acts like a "translator", instantly enabling older systems that do not support SM2 standards to achieve SM2 cryptographic compliance, solving the historical problem of e-government, online banking, and other systems needing to build multiple platforms to cope with different visitors.
- **Post-quantum cryptography migration**: The gateway has a built-in post-quantum cryptography algorithm module, which is the only one in the world to simultaneously support two hybrid PQC algorithms: X25519MLKEM768 and SM2MLKEM768. It works closely with ZT Browser to prioritize the use of SM2MLKEM768 to achieve quantum-resistant SM2 algorithm HTTPS encryption, while meeting the SM2 cryptographic transformation and post-quantum migration needs, effectively ensuring the continued security of critical system data in the present and future quantum era.
- **Integrated security capabilities**: In addition to automatic certificate management, the gateway also integrates WAF functionality to clean decrypted traffic and intercept malicious attacks, truly achieving the integration of "encryption" and "protection" and solving the problem that traditional WAF devices do not support automatic certificate management.



4. ACLM is the ultimate solution for automatic certificate management.

Looking back at the development of the entire industry, from the birth of the ACME protocol in 2019 to the management changes triggered by the shortening of validity periods, we can see a clear evolutionary path: when the number of certificates is small and the validity period is long, manual management or single-point automation can still cope; but when certificates become ubiquitous "digital identities" and must be changed rapidly on a monthly basis, decentralized and unmanaged automation will only bring new chaos.

For large and medium-sized organizations with multiple websites, systems, devices, and cloud services, the need is not just for ACME, but for unified management and scheduling of ACME – that is, ACLM. ACME solves the "how to do it" problem, while ACLM solves the "how to manage it well" problem. An excellent ACLM platform can integrate all ACME services into a unified view, orchestrate manually applied certificates with automatically applied certificates, seamlessly integrate support for RSA/ECC and SM2 algorithms, support the mixed application of traditional cryptographic algorithms and post-quantum cryptographic algorithms and support seamless migration, and present the certificate lifecycle status to administrators in real time in the form of reports and alerts.

From Let's Encrypt promotion of ACME, to giants like Sectigo and DigiCert building CLM ecosystems, and ZoTrus innovatively launch a dual-mode ACLM solution combining cloud services and local gateways, an industry consensus has emerged: **ACLM is the ultimate solution for automatic certificate management**. Before the 47-day validity period arrives in 2029, and with the ever-increasing threat of quantum computing, widespread adoption of ACLM is not only a means to improve operational efficiency but also a strategic choice to ensure the uninterrupted and reliable operation of critical information infrastructure systems. Let us embrace ACLM and evolve from passively managing certificates to proactively and automatically building a cryptographically agile digital trust infrastructure.

Richard Wang

March 16, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 118 articles in English (more than 163K words) and 266 articles in Chinese (more than 783K characters in total).