ZoTrus, the Leader in Dual-Algorithm SSL Certificate Automation

February 4, 2026

Yesterday, ZoTrus Technology launched a sound product for certificate automation — the free SM2 ACME Public Service and the open-source SM2 ACME client, which received a lot of attention immediately after going live. With this, ZoTrus has officially completed the full series of dual-algorithm SSL certificate automation products, a project that took over four years to develop. This article explains how these products were created, which user groups they serve, and their unique features. It is highly recommended reading for users currently evaluating dual-algorithm SSL certificate automation solutions.

1. The successful experience of ACME is well worth learning from and emulating.

The path to SSL certificate automation management began in late 2015 with the Let's Encrypt (LE) free SSL certificate automation public service initiated by Mozilla. After the release of the RFC 8555 ACME standard in March 2019, it became widely supported by major cloud companies, especially CDN provider - Cloudflare, which was the first to provide default free SSL certificate automation configuration.

This is the development history of SSL certificate automation, and a successful experience in the path of SSL certificate automation, which is well worth learning from and emulating. More specifically, it can be summarized in the following three points:

(1) There is a leading company, a leader, and this leader is the browser.

Only in this way can everyone be convinced that this can succeed, and only then can more likeminded people be attracted to participate, because the usability of an SSL certificate depends on whether the browser trusts it; the browser is the ultimate authority. The international leader in SSL certificate automation is Mozilla, the owner of the Firefox browser, which established an independent non-profit organization, ISRG, specifically for this project. Subsequently, Google strongly supported it and also launched its own free SSL certificate automation public service – GTS.

Why was certificate automation initiated by browser, rather than CA? Firstly, this was a revolution against CAs, and it's impossible for CAs to initiate it; few are willing to revolutionize themselves. Secondly, browsers, as SSL certificate consumers, have long been dissatisfied with the inaction of CAs. The launch of Let's Encrypt and GTS was precisely aimed at revolutionizing CAs, and they succeeded, achieving the first and second positions in the global SSL certificate market, with market shares of 49% and 14% respectively.

(2) There is a standard, the standard-setting organization must naturally be the leader.

Since launching its free SSL certificate automation service at the end of 2015, LE has become the world's largest Certificate Authority (CA) by 2018, demonstrating how much users appreciate certificate automation and free SSL certificates. Users worldwide have suffered from manual certificate management for far too long — over 20 years. Once someone offers certificate automation services, it's like a spark igniting a prairie fire!

What's admirable is that while LE has achieved the largest market share globally, it hasn't exclusively enjoyed this success nor applied for patent protection. Instead, based on its extensive experience in certificate automation, it collaborated with relevant organizations to develop the RFC8555 ACME standard, allowing the global industry to adopt this standard for widespread SSL certificate automation. The development of this standard is fundamental to the global adoption of SSL certificate automation, resulting in over 90% of SSL certificates now being issued and deployed automatically. The standard's development has been indispensable!

(3) Ecosystem support requires the joint participation of all parties in the SSL certificate ecosystem.

With standards in place, SSL certificates for various cloud services can be automated. Major cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, as well as CDN providers like Cloudflare, Akamai, and Fastly, and cybersecurity companies like Cisco, F5, and Citrix, were among the first to support automatic SSL certificate management. Interestingly, the world's first, second, and third largest Certificate Authorities (CAs) did not actively participate, and even actively opposed the implementation of standards for shortening SSL certificate validity periods. This caused the CAs' market share to drop from 1st and 2nd to 5th and 8th place, respectively.

In other words, all parties involved in the SSL certificate application ecosystem work together to provide users with automatic certificate management services for various cloud services and network devices based on the standard. This is how the number of SSL certificates has grown from over 200 million in 2016 to over 1.3 billion today, with LE increasing from zero at the end of 2015 to over 600 million today. This demonstrates the power of full ecosystem support for certificate automation.

2. China path to SSL certificate automation is destined to differ from the international path.

China path to SSL certificate automation must certainly learn from international approaches, but there are also differences. While both require the same three implementation paths, the key difference lies in the necessity of automating dual-algorithm SSL certificates simultaneously, and the web server must be modified to support SM2 algorithms. This can be summarized in the following three points:

(1) Similarly, there must be a lead organization, which could be a browser, a CA, or a cloud platform.

In contrast to the international path of SSL certificate automation, which was spearheaded by browser, the path to automation of SM2 SSL certificates also began with browser vendor ZoTrus, which first proposed dual-algorithm SSL certificate automation products and solutions. Given China's unique market situation, it might be easier to popularize SM2 SSL certificate automation if it were led by a CA or cloud platform.

(2) Similarly, there must be a standard, and the standard-setting organization must naturally be the leader.

The successful experience of SSL certificate automation lies in the development of standard, but the ACME standard can only solve the automation problem of RSA/ECC algorithm SSL certificates, and it cannot solve the problem of automating dual algorithm (SM2+RSA) SSL certificates in China. Fortunately, in 2023, the National Cryptography Industry Standardization Technical Committee approved the project led by ZoTrus, in conjunction with several CAs and Internet companies, to develop the cryptography industry standard GM/T, "Automatic Certificate Management Specification". It is estimated that the standard will be completed and released this year.

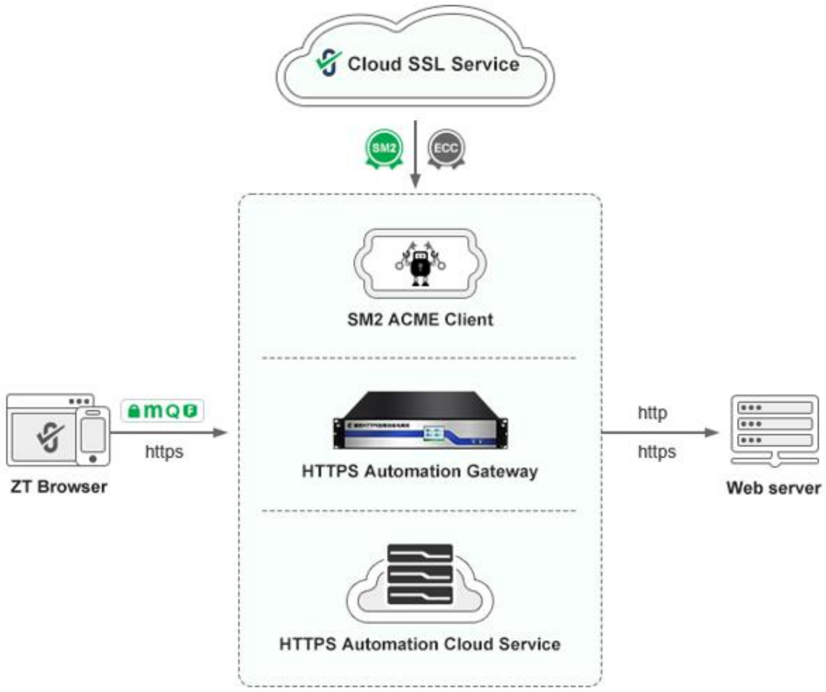
(3) Similarly, ecosystem support and the joint participation of all parties in the SM2 SSL certificate ecosystem are essential.

In contrast to the successful experience of SSL certificate automation, which relies on the active participation of all relevant vendors in the ecosystem, the automation of SM2 SSL certificates has not been so fortunate. Although a draft of the SM2 ACME standard was released long ago with reference to the RFC ACME standard, and only ZoTrus' entire product line supports it so far. This is the biggest problem in popularizing the automation of SM2 SSL certificates in China — the lack of full ecosystem support.

China should learn from the international SSL certificate automation ecosystem. Major cloud platforms, CDN service providers, CAs, and cybersecurity vendors should actively participate in building a SM2 SSL certificate automation ecosystem to provide users with automatic dual-algorithm SSL certificate services. Only in this way can SM2 SSL certificates be truly popularized to safeguard cyberspace security in China.

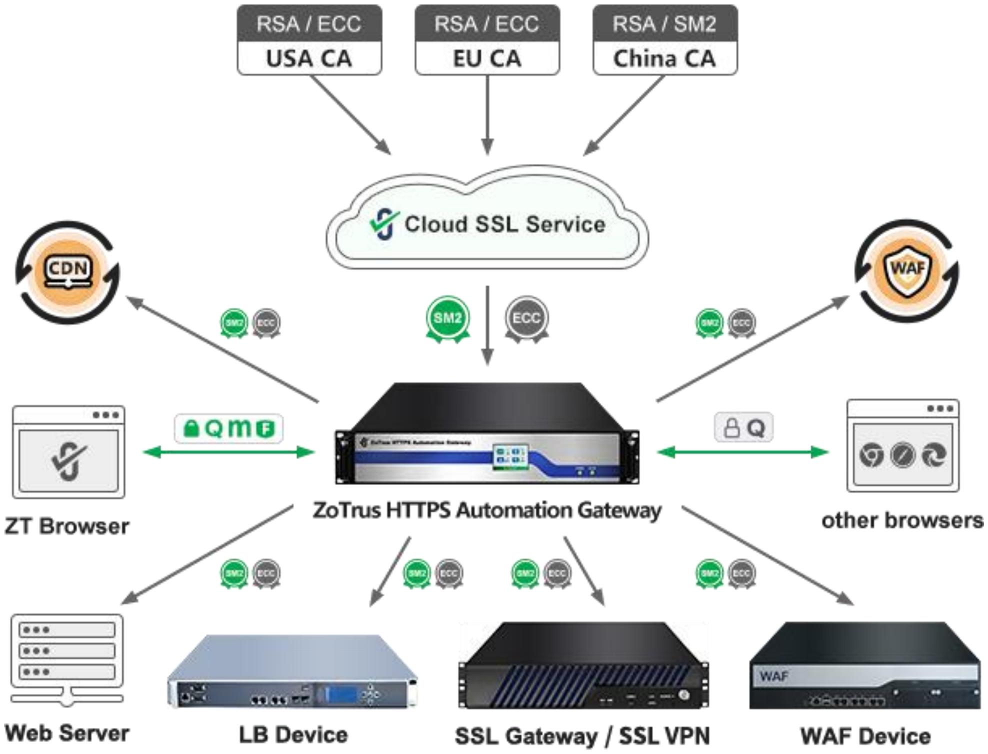
3. ZoTrus has successfully built a complete full-stack SSL certificate automation ecosystem.

Since its inception, ZoTrus has positioned itself as a provider of cryptographic application automation technology. Its first solution was a dual-algorithm SSL certificate automation solution. Over the past four years, it has successfully built a three-in-one, client-to-cloud integrated full-stack SSL certificate automation ecosystem to meet the dual-algorithm SSL certificate automation needs of different users. The first solution references international SSL certificate automation solutions, it is based on an open-source solution using the SM2 ACME client. It not only provides open-source SM2 ACME client software but also offers completely free SM2 ACME public service. This allows users to use dual-algorithm SSL certificate automation services for free, and enables users with development capabilities to automate dual-algorithm SSL certificate implementation for various business systems and devices based on the SM2 ACME public service. ZoTrus has transformed from a technology provider into a builder of the SSL certificate automation ecosystem and a promoter of standard implementation.



The second solution draws on the experience of cloud providers and CDN service providers in the international SSL certificate automation ecosystem. It offers CDN services a "patchwork" dual-algorithm SSL certificate automation service based on the CDN API, and a "native integration" solution through deep cooperation with CDN providers. This is the most economical and optimal solution for the large-scale deployment of SSL certificate automation, avoiding the need for millions of internet businesses to "reinvent the wheel" for certificate automation transformation, and turning certificate automation capabilities into a universally accessible service. ZoTrus transforms from a technology provider into an Internet security service provider selling "perpetual security status" service and a promoter of standard implementation.

The third solution draws on the experience of cybersecurity vendors in the international SSL certificate automation ecosystem, creating a hardware product — ZoTrus HTTPS Automation Gateway — for government, financial, and other critical information infrastructure entities. This integrated hardware and software SSL certificate automation management platform goes beyond simple certificate automation management, deeply integrating hardware acceleration of ECC and SM2 algorithms, smooth migration capabilities for post-quantum cryptography algorithms, WAF protection capabilities, and unified management of SSL certificates across multiple sites and devices. It not only provides dual-algorithm SSL certificate automation services for web servers but also for other network devices and cloud services requiring SSL certificates. ZoTrus is not only practicing comprehensive automation of the SSL certificate ecosystem but also participating in defining the security architecture specifications for future critical information infrastructure.



4. Only automatic certificate management can truly guarantee network security and data security.

ZoTrus has successfully implemented three technical solutions for SSL certificate automation through an integrated client-to-cloud technical approach: ACME public service and open-source ACME client empowerment, CDN service API mode and native integration, and hardware gateway with in-depth protection and management. These solutions form a solid foundation for ZoTrus leading position in SSL certificate automation.

Only through certificate automation can the SM2 transformation and the post-quantum cryptography migration to be successfully completed, truly guaranteeing China's cybersecurity and data security. ZoTrus, through its robust advancement of the "three-in-one" SSL certificate automation solution, will undoubtedly become a leader in the SSL certificate automation market in this profound cryptographic technology revolution driven by automation, and will further define and guide the era of automatic cryptographic applications. ZoTrus is leading a new digital era characterized by full-stack trust, end-to-end automation, and comprehensive intelligence.

Richard Wang

February 4, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 116 articles in English (more than 159K words)
and 261 articles in Chinese (more than 764K characters in total).