The core of Intranet SSL certificate automation is self-sufficiency

December 1, 2025

In several blog posts, the author has detailed the automatic management and automatic switching of multiple CA issuing channels for Internet SSL certificates, which is the core of automatic Internet SSL certificate management. This article will discuss the automatic management of Intranet SSL certificates, the key point is self-sufficiency.

1. Intranet traffic urgently needs HTTPS encryption, and there is an urgent need for Intranet SSL certificates and certificate automation.

Because Intranet IP addresses and Internal Names cannot be validated, international standards prohibit publicly trusted Certificate Authorities (CAs) from issuing SSL certificates for Intranet IP addresses and Internal Names. However, Intranets handle confidential information that cannot connect to the public Internet, and this confidential information requires HTTPS encryption protection. Therefore, Intranet administrators have no choice but to build their own private CA system and issue SSL certificates that browsers do not trust.

However, with the increasing number of intranet management systems and the continuously shortening validity periods of publicly trusted SSL certificates, intranet SSL certificates also need automatic management. Intranets also need to implement SM2 algorithm HTTPS encryption in China, and it also need to support post-quantum cryptography algorithms. However, the automatic SSL certificate management solutions used on the Internet cannot be used for automatic management of intranet SSL certificate management because the publicly trusted SSL certificate automatic management requires an Internet connection to the certificate issuing CA's ACME service. What can be done?

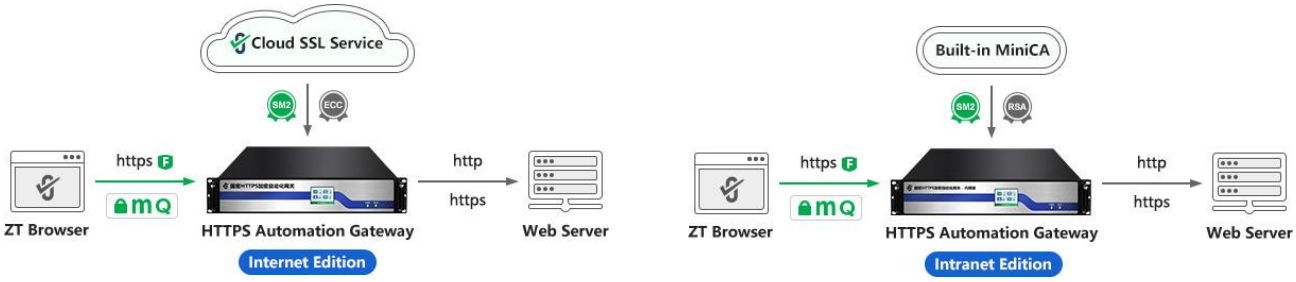
2. The core of automatic management of Intranet SSL certificates is self-sufficiency.

Because the Intranet cannot connect to the Internet, automating SSL certificate issuance requires building a self-built CA system that supports certificate automation, while also ensuring the intranet

(C) 2025 **ZoTrus Technology Limited**

web server supports it. In other words, to automate intranet SSL certificate issuance, customers would need to replicate and build a system identical to the one used for Internet SSL certificate automation. This is too costly and significantly increases internal system management workload, making it an undesirable solution.

Since intranets cannot connect to the Internet to obtain all the resources for automatic management of SSL certificates, self-sufficiency is the only viable option. However, investing in and building a complete automatic certificate management system is too expensive and complex. Recognizing these challenges, ZoTrus Technology, after completing its publicly trusted SSL certificate automatic management solution, continued to develop an intranet SSL certificate automatic management solution. This solution is derived from the Internet ACME system that integrates the client (ZT Browser), the cloud (ZoTrus Cloud SSL Service System), and the server (ZoTrus HTTPS Automation Gateway) into a unified solution (as shown in the left diagram below). This is an intranet SSL certificate automatic management solution integrating the client (ZT Browser) and the server (ZoTrus HTTPS Automation Gateway Intranet Edition + Built-in MiniCA System) (as shown in the right diagram below).



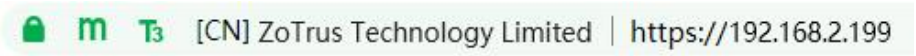
This is ZoTrus Technology's automatic intranet SSL certificate management solution, built upon its existing automatic Internet SSL certificate management. It eliminates the need to connect to an external CA system or invest in building a complex internal CA system. Instead, it integrates a MiniCA system directly on the Intranet Gateway, achieving self-sufficiency in dual-algorithm Intranet SSL certificates. This is the optimal solution.

This not only achieves self-sufficiency in intranet SSL certificates but also solves the problem of self-signed root CA certificates not trusted by browsers. ZT Browser is not only completely free, supporting both commercial cryptographic algorithms and post-quantum cryptography, but it also included and trusted the root CA certificates for issuing intranet SSL certificates by the MiniCA in the ZoTrus

(C) 2025 **ZoTrus Technology Limited**

Intranet Gateway, thus completely resolving the browser trust issue for intranet SSL certificates. ZoTrus Technology customizes two intermediate root CA certificates (SM2/RSA) trusted by ZT Browser for each intranet gateway, using customer's brand names (e.g., Abcdef), respectively for automatically issuing SM2 and RSA algorithm intranet SSL certificates. The certificate's common name is bound to a validated customer's domain by default, and it can automatically issue SSL certificates for subdomains of the bound domain, intranet IP address certificates, and internal name SSL certificates. Each intranet gateway supports up to 510 intranet websites. The automatically configured dual-algorithm SSL certificates (RSA OV SSL certificate + SM2 OV SSL certificate) are completely free. The certificate chain for the dual-algorithm SSL certificates is shown in the figure below.

ZT Browser displays the organization's name in the address bar for all intranet websites, assuring visitors that they are accessing their organization's intranet website, as shown in the left figure below. Alternatively, users can use other browsers (such as Google Chrome) to implement HTTPS encryption on the intranet using RSA algorithm. These browsers trust the RSA algorithm intranet SSL certificate issued by ZoTrus Intranet Gateway, as shown in the right figure below.



ZoTrus HTTPS Automation Gateway (Intranet Edition) has the same functions as the Internet Edition Gateway, except for automatic configuration of intranet SSL certificates. It also supports SM2 algorithms, RSA algorithms, and PQC algorithms, meeting the needs of users' intranet systems for cryptographic compliance, compatibility with RSA algorithms, and PQC migration. It is the best solution to ensure the security of intranet traffic.

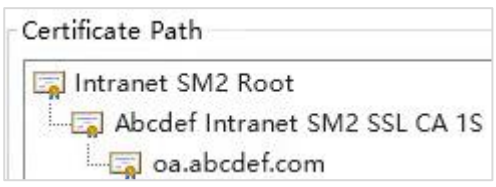
3. Configure a self-signed SSL sub-CA certificate to meet specific application needs.

To meet the special application needs of some users whose intranet uses public IP addresses, ZoTrus Intranet Gateway also sets up two other customer-branded ZT browser untrusted self-signed root CA

(C) 2025 **ZoTrus Technology Limited**

certificates (Intranet SM2 Root and Intranet RSA Root) signed sub-CA for customers to automatically issue intranet SSL certificates that bind to unvalidatable public IP addresses and public domain names. According to ZT Browser Internal SSL Root CA Trust Program, ZT Browser only includes intranet root CA certificates that issue compliant internal IP addresses (Reserved IP addresses) and internal domain names for intranet SSL certificates. Therefore, to issue intranet SSL certificates for public IP addresses or public domain names, it only can be done by the root CA certificates that ZT Browser does not trust. This is equivalent to ZoTrus Intranet Gateway providing customers with a free, browser-untrusted self-built CA system for issuing any required intranet SSL certificates. This is a practical Intranet CA that ZoTrus Intranet Gateway offers free of charge, solving the problem of using public IP addresses within the intranet and enabling these customers to achieve automatic management of intranet SSL certificates.

Since ZT Browser does not trust these two self-signed roots issued intranet SSL certificates, customers need to manually install and trust the RSA root CA certificate. This will allow commonly used browsers to trust the intranet SSL certificate issued by the self-signed root CA. If SM2 algorithm support is required, the SM2 root CA certificate needs to be manually imported into ZT Browser's Certificate Manager - Local Certificates - Custom. ZT Browser will then trust the self-signed root CA issued SM2 algorithm intranet SSL certificate. The certificate chain of these two self-signed root CA issued intranet SSL certificates is shown in the figure below. The sub-CA name follows the same naming rule as the sub-CA name of the root CA certificates trusted by ZT Browser, except for the addition of the letter 'S' at the end.



4. Intranet traffic requires HTTPS encryption even more; only self-sufficiency is the ultimate solution.

The standard for Internet SSL Certificate Automation is “ACME”, it means "summit" or "ultimate", signifying an ultimate solution. However, this solution doesn't address the challenge of automating intranet SSL certificate management. ZoTrus Technology's Intranet SSL certificate automation

(C) 2025 **ZoTrus Technology Limited**

solution achieves self-sufficiency and automation for Intranet SSL certificates, making it the ultimate solution for Intranet SSL certificate automation. It not only solves the problem of automating the issuance of compliant Intranet SSL certificates but also addresses browser trust issues. Furthermore, it resolves the difficulties many large organizations in China face in applying for Intranet SSL certificates due to the non-standard use of public IP addresses. Customers no longer need to invest heavily in building internal CA systems; they only need to deploy ZoTrus Intranet Gateway to automatically implement HTTPS encryption protection for intranet traffic, meeting users' application needs for cryptography compliance, compatibility with RSA algorithms, and PQC migration.

Richard Wang

December 1, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 103 articles in English (more than 141K words) and 240 articles in Chinese (more than 715K characters in total).

(C) 2025 **ZoTrus Technology Limited**