ACME Client Software Innovation - Hardwareization

The first product of ZoTrus SM2t HTTPS automation management solution was to learn from the international ACME solution and developed an SM2 ACME client software - SM2cerBot. However, this SM2 ACME client software was offline from the official website last month, and many users came to ask why it was offline. This article will talk about this topic and focus on the second product of our solution - SM2 ACME client hardware: ZoTrus HTTPS Automation Gateway. Explaining our R&D process clearly is intended to provide users with a reference for decision-making in the selection of dual-algorithm SSL certificate automatic management solutions.

1. Difficulties encountered by the SM2 ACME client software

As the validity period of SSL certificates will be shortened to 47 days, automatic management of SSL certificates has become an inevitable choice. The international automatic management solution for SSL certificates is to install a client software - ACME client, such as CertBot, on the Web server, and then configure the ACME service parameters of the ACME service provider, so that the SSL certificate application, validation and deployment can be completed automatically. This solution is very mature. Not only is it based on the RFC8555 standard, but there are also two major ACME service providers (LE and GTS) that provide worldwide users with RSA/ECC algorithm SSL certificates with a validity period of 90 days for free. Since 2013, more than 20 billion SSL certificates have been automatically issued for users around the world, and LE alone has more than 500 million valid SSL certificates.

However, this very mature SSL certificate automation solution cannot solve all problems, such as the user's Web server cannot install ACME client software, or the user's system is running and cannot be shut down for a moment to enable ACME service. China is vigorously promoting the popularization of commercial cryptographic algorithms to implement HTTPS encryption, which requires ACME service to support the automatic application and deployment of SM2 SSL certificates. And it is not like the international ACME solution that you can just get an SSL certificate, but you also need to reconstruct the Web server to support the commercial cryptographic algorithm to implement SM2 algorithm HTTPS encryption.

ZoTrus SM2 ACME client software - SM2cerBot is an ACME client software that can automatically complete the application of dual-algorithm (RSA and SM2) SSL certificates, automatically complete the deployment of dual SSL certificates, and automatically complete the Web server software upgrade to support the SM2 algorithm. In theory, this solution is already the best solution, which can meet the cryptographic compliance and global trusted HTTPS encryption application requirements. However, it encountered great difficulties in the actual user environment, mainly included:

(1) Great harm to business systems: Since the original Nginx server software needs to be uninstalled and recompiled to support the SM2 algorithm, this change will cause great harm to the application system that has been running, and it may cause the business system to be unable to run again. This risk is too great because the user's business system may be a government system or an online banking system that cannot be stopped.

(2) Difficulty in operating system adaptation: Commonly used operating systems are Ubuntu and CentOS or others. These systems have released many versions. The ACME client needs to be compiled and adapted on each version. This workload is huge, but it is too difficult for users to compile it themselves.

(3) Business cannot be interrupted: The user's business system is running and cannot be interrupted or interrupted in rotation. In other words, the user's Web server cannot be changed at all, and no third-party software can or is allowed to be installed, and the Web service is not allowed to be restarted.

It is precisely because of these practical deployment difficulties that ZoTrus Technology decided to abandon the continued development and technical support of the SM2 ACME client software. Last month, it decided to take the client software offline and no longer recommend this solution to customers. This is because it is not a solution suitable for the automatic management of dual algorithm SSL certificates in China and cannot meet users' actual application needs for zero impact on existing business systems.

2. The best solution – SM2 ACME client software hardwareization

The problems that SM2 ACME client software faced is that it will affect the normal operation of the user's business system, which is unacceptable to users. ZoTrus Technology has come up with a better solution - install the SM2 ACME client software on the hardware server, and it provides users with a

hardware and software integrated device. In this way, it is possible to achieve the automatic application and deployment of dual-algorithm SSL certificates without modifying the user's original system or installing any software on the user's Web server. This all-in-one machine can automatically apply for and deploy dual-algorithm SSL certificates and automatically implement HTTPS encryption. This all-in-one machine replaces the work originally completed by the user's Web server. This all-in-one machine is the product that everyone has seen now - ZoTrus HTTPS Automation Gateway.

This solution is not only to transfer the SSL certificate deployment and HTTPS encryption and decryption functions of the Web server or other gateway devices that originally needed to install SSL certificates to this SM2 ACME client hardware, but also to add the automatic application of dual-algorithm SSL certificates, completing domain name validation and certificates deployment, and support SM2 algorithms (SM2/SM3/SM4). Therefore, the SM2 ACME client hardware is equal to a high-performance network security hardware platform + Nginx that supports SM2 algorithms + high-speed cryptographic card + ACME client software + RSA/ECC SSL certificates + SM2 SSL certificates + WAF system. In fact, it is a cryptographic machine (HSM device) with built-in private keys and certificates. It not only provides ACME client functions, but also ensures the security of SSL certificate keys, ensuring that the keys do not leave the hardware and are not manually processed by anyone. It is secure than the traditional manual application for SSL certificates with multiple people handling the keys.

Since the HTTPS encryption and decryption work has been moved from the Web server to the ACME client hardware, the computing power burden of the Web server has been reduced by 20-30%, allowing the Web server to be dedicated to processing user business systems. This function is actually the role of the traditional SSL gateway, which is why ZoTrus Technology named this SM2 ACME client hardware as "HTTPS Automation Gateway", or "ZoTrus Gateway" for short.

3. ZoTrus Gateway is not just a piece of ACME client hardware

ZoTrus Gateway is not only a hardware SSL gateway that implements ACME functions and automatically applies for and deploys dual-algorithm SSL certificates, but it also integrates a WAF module. This is because if the HTTPS traffic is unloaded through the gateway and then directly transferred to the subsequent Web server without analysis, then the user still needs to purchase a WAF device, which increases the complexity and reliability of the user's system. It is better to directly add a traffic cleaning function after unloading the HTTPS encrypted traffic to intercept malicious traffic and release clean traffic, providing greater security for the subsequent Web server.

The built-in WAF module in ZoTrus Gateway is a Web application firewall developed based on the open source ModSecurity system. Its high-performance WAF protection function has been evaluated by the authoritative third-party testing platform WAFER, and the results show that its Detection Ability is A (highest level), its Distinguishing Ability is A (highest level), and its true positive detection rate is as high as 97.34% (there is still room for improvement). However, the traditional WAF devices commonly used by users do not support automatic management of SSL certificates, and users need to manually configure SSL certificates on the WAF device to implement WAF protection in HTTPS encryption mode.

ZoTrus Gateway not only supports automatic management of SSL certificates, and it does not sell a bare machine without an SSL certificate to customers, but it sells an automatic management hardware package with a dual-algorithm SSL certificate (SM2 OV SSL certificate + ECC DV SSL certificate) for up to 255 websites for 5 years. The hardware itself is also guaranteed to be used for 5 years, and a faulty machine can be replaced directly for free.

ZoTrus Gateway not only includes dual- algorithm SSL certificates, but also it ensures that the dual SSL certificates will not be interrupted due to various reasons. It automatically configures SSL certificates for the gateway. Because the ZoTrus Cloud SSL Service System has been connected to many international CAs and China CAs, it can reliably issue RSA/ECC SSL certificates and SM2 SSL certificates to the websites. Customers can also choose the familiar SSL certificate brands.

ZoTrus Technology not only has the SM2 ACME client hardware, nor does it only package dual SSL certificates, nor does it only integrate WAF functions, but it also provides a free SM2 algorithm supported browser -ZT Browser, which is clean and ad-free. ZT Browser not only gives priority to using the SM2 algorithm to implement HTTPS encryption, but also it adds a WAF protection icon behind the padlock in the browser address bar, clearly informing site visitors that the website they are visiting has not only implemented SM2 HTTPS encryption, but also WAF protection, complying the commercial cryptography requirements and cybersecurity protection requirements.

4. The software hardwareization of the ACME client is the best dual-algorithm SSL certificate automatic management solution

ACME client software is necessary for the automatic management of SSL certificates. Today, when the RSA cryptographic system has been perfectly integrated into all IT products and Internet infrastructure, to achieve HTTPS encryption, users only need software that can automatically complete the application and deployment of SSL certificates, of course, except for special cases such as old systems that cannot install ACME client software.

However, China's commercial cryptographic algorithms are far from being universally supported, so the best solution is to simply not transform the existing system, without installing any software, and directly use a hardware device to achieve protocol layer conversion, so that users can easily and

painlessly achieve the automatic management of dual-algorithm SSL certificates. This is the SSL certificate automation solution that customers really want.

Richard Wang

June 25, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 94 articles in English (more than 127K words) and 216 articles in Chinese (more than 639K characters in total).