What is SM2 ACME? Ultimate Solution for SM2 HTTPS encryption

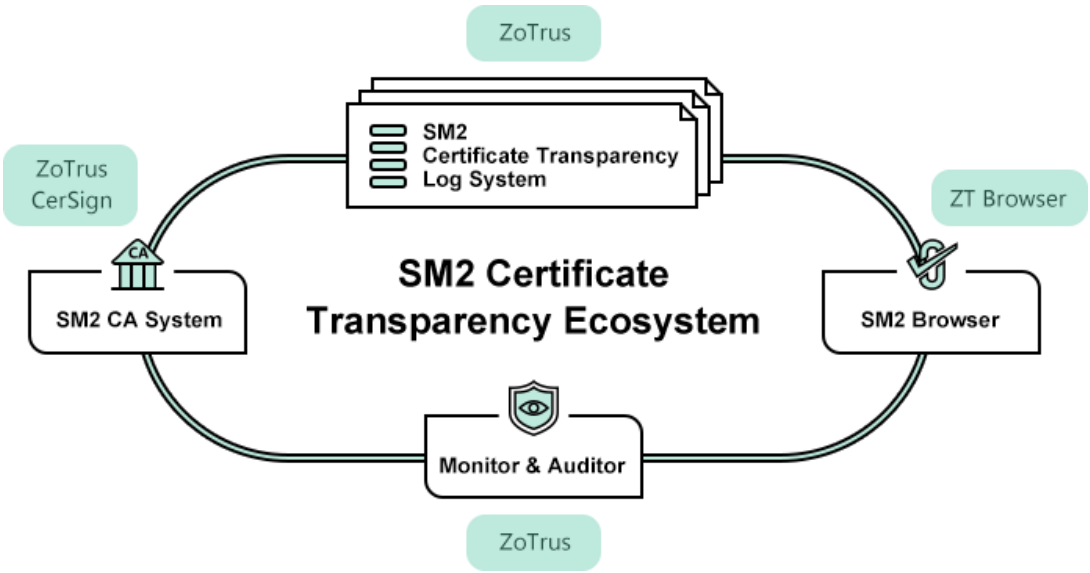
The English word "acme" means "peak, apex, highest point". In the computer and Internet industry, it is the name of a very well-known international standard. "ACME" is the abbreviation of Automated Certificate Management Environment. This is an RFC 8555 international standard for automatic application and deployment of SSL certificate, including ACME client and ACME server. At present, the total number of SSL certificates that have been logged in the Google Certificate Transparency Log System is as high as 8.2 billion, of which the total number of automatic application and deployment has reached 7 billion, accounting for 85%. It can be seen that automatic deployment of SSL certificates is an inevitable trend, because users need to implement https encryption simply and easily. This is probably why this RFC standard's authors names this standard as "ACME", because they believe that this is the ultimate solution for SSL certificate management, completely getting rid of the tedious manual application and deployment of SSL certificate, and completely eliminating the huge security risk caused by forgetting to renew the SSL certificate that the business system will be paralyzed!

When the author knows the standard English name ACME for the first time, I couldn't understand why the word "Environment" was used. Isn't it more accurate to use "System"? But if "System" is used, the English abbreviation will be "ACMS", which is not a common word, and it is inconvenient to remember. The use of Environment is justified, but the advantage is that the abbreviation has become "acme", which highlights the technical level and literary atmosphere of this RFC standard.

Back to the topic, although the ACME standard is good, it is only applicable to the automatic deployment of international algorithm SSL certificates (RSA and ECC), and it does not support the automatic deployment of Chinese algorithm SSL certificates (SM2), so we cannot apply this protocol to realize SM2 certificate automatic management. To realize SM2 automatic certificate management to realize SM2 https encryption, it is not enough to provide only an automatic certificate management **environment**, but need an automatic certificate management **ecosystem** that all related systems support SM2 algorithm, because the existing common used Web servers do not support SM2 algorithm, the browsers do not support SM2 algorithm, the CDN/WAF does not support SM2 algorithm, and the

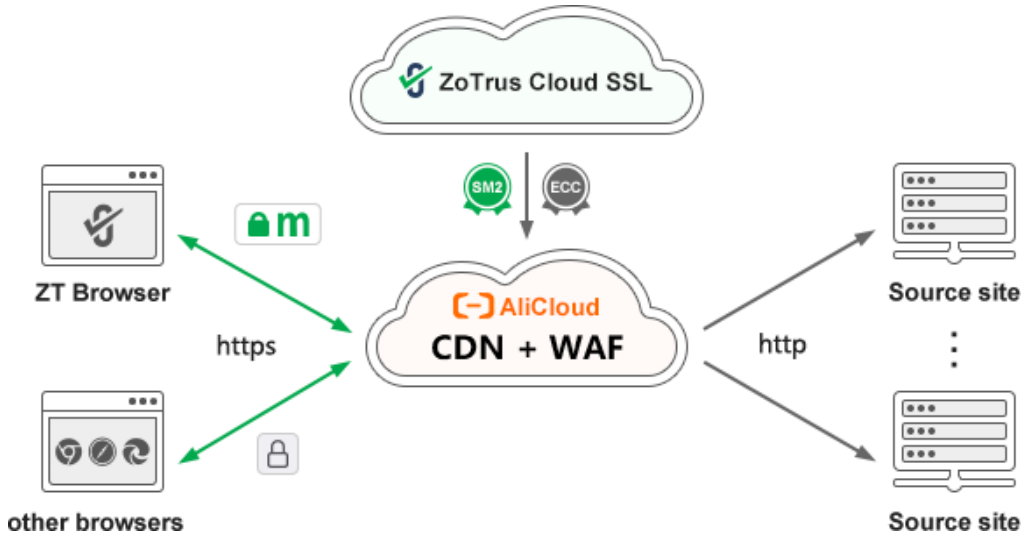
Certificate Transparency Log System does not support SM2 algorithm and the SM2 SSL certificate. To implement the SM2 https encryption, the entire ecosystem based on the existing RSA cryptographic system needs to support the SM2 algorithm. Therefore, the E of SM2 ACME is the first letter of Ecosystem, not the first letter of Environment. This is the most critical difference between the SM2 ACME and the international standard ACME!

The author believes that readers who follow my blog should know that the author released the SM2 Certificate Transparency ecological product at the 2022 World Internet Conference in Wuzhen at November 8. The SM2 SSL certificate application ecological core product realizes the SM2 algorithm support for the whole lifecycle management of the SM2 SSL certificate, which is the same as the international SSL certificate, including the world's first SM2 Certificate Transparency Log System supporting the SM2 algorithm, the world's first SM2 CA system that can issue SM2 SSL certificate that support SM2 certificate transparency, and the world's first SM2 browser that supports SM2 Certificate Transparency.

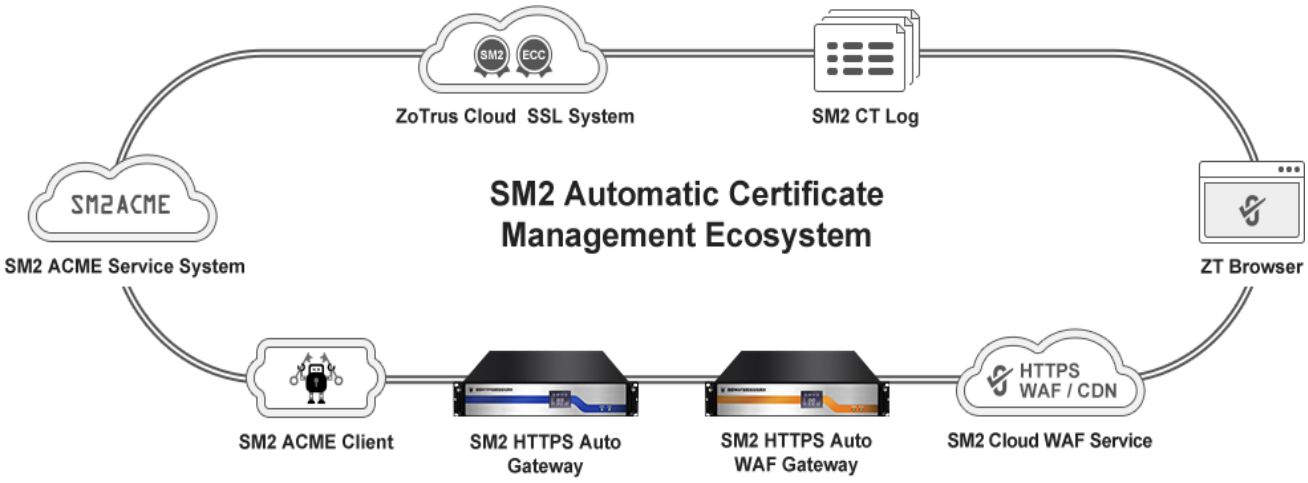


And an innovative cloud service released in Wuzhen is the ZoTrus Website Security Cloud service, which is a typical solution for automatic certificate management to realize https encryption, a zero reconstruction solution to realize SM2 https encryption, and customers do not need to manually apply for SSL certificate from CA operator, no need to install an SSL certificate on the web server, and only need to do 3 domain name resolution to achieve SM2 https encryption, adaptive encryption algorithm,

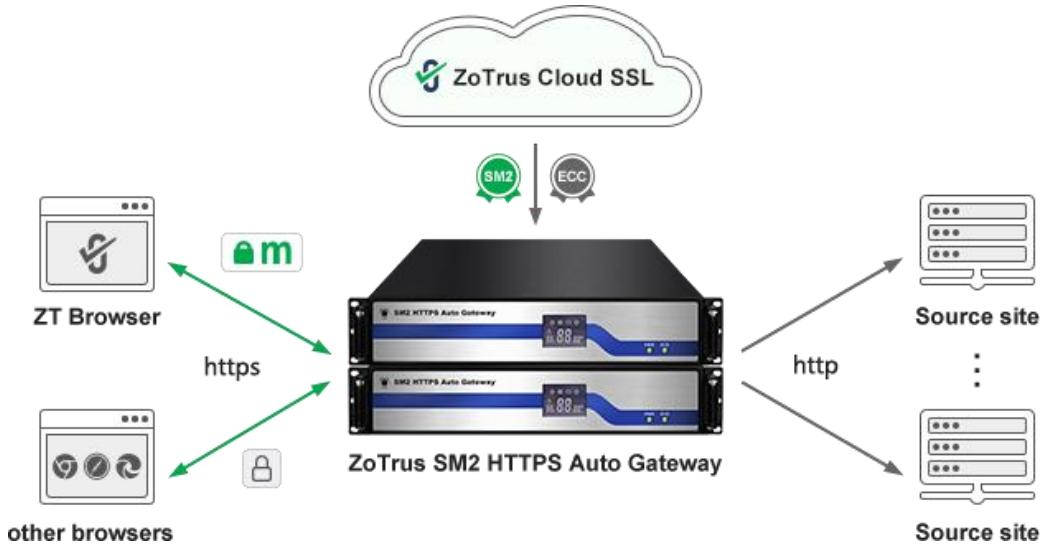
support international algorithm to realize https encryption, and also realize cloud WAF protection and CDN distribution and website trusted identity certification, this is a four-dimensional protection solution for website security.



The release of the SM2 ACME solution this time is to continue to innovate based on the SM2 Certificate Transparency ecology to create an SM2 automatic certificate management ecosystem. In this ecosystem, there are products in the SM2 Certificate Transparency ecology including the SM2 CA System (ZoTrus Cloud SSL System), dual-algorithm dual-SSL certificate issued by the SM2 CA System, SM2 Certificate Transparency log system, and a browser that supports SM2 Certificate Transparency and SM2 algorithm. The newly added products include SM2 ACME Client, SM2 ACME Service System and SM2 HTTPS Auto Gateway. These six SM2 automatic certificate management ecological products form a self-contained system, forming an application ecology that can realize automatic SM2 https encryption, to meet the customers need for cryptography compliance and global trust for website security.



In addition to referring to the international ACME standard, the SM2 Automatic Certificate Management Ecosystem released this time also have SM2 ACME server and a completely free SM2 ACME client - SM2cerBot. We also innovatively released the SM2 HTTPS Auto Gateway, which is designed for solving the problem that e-government Web systems and large-scale enterprise management systems cannot install ACME clients on running web servers. It is an all-in-one high-performance website security hardware gateway device, like the ZoTrus Website Security Cloud Service, it can realize SM2 https encryption without modifying the original web server, but also satisfies such customers who want to deploy the system locally without relying on cloud service for independent and controllable management.



The author believes that readers who have read this whole article will be able to appreciate the uniqueness and innovation of our solutions. In order to help customers to choose a proper SM2 automation certificate management solution according to their business needs, the following four points are summarized.

First, to realize SM2 https encryption, it is impossible to simply copy the international ACME standard, there must be innovation, and there must be an Automatic Certificate Management **Ecosystem** for SM2 algorithm support, rather than a simple **Environment**.

Second, customers can install the completely free SM2 ACME client - SM2cerBot on the Web server, automatically configure the free 90-day period or the charged one-year SM2 SSL certificate and ECC

SSL certificate, and automatically install the SM2 algorithm module, which automatically realizes the adaptive algorithm https encryption. It not only realizes the same function of automatically deploying SSL certificates as other ACME client software, but also realizes the automatic support of SM2 algorithm, and realizes the automatic management of double-algorithm double-SSL certificates.

Third, for customers who cannot install the SM2 ACME client software on the web server, they can choose to deploy a plug-and-play SM2 HTTPS Gateway with a built-in SM2 ACME client in front of the existing Web server, to realize zero change to the current web server to enable SM2 https encryption, ensures that the e-government web system and large enterprise management system can be seamlessly upgraded from http to https and SM2 https.

Fourth, for customers who neither want nor can install the ACME client on the existing server, nor want to purchase and locally deploy hardware gateway device, the simpler solution is to use the Website Security Cloud Service, which only needs to do three domain name resolutions, ZoTrus Cloud SSL System will automatically configure dual SSL certificates to the Alibaba Cloud CDN+WAF system, the original website can be turned into the source site of the CDN+WAF, and it will be more cost-effective and easier to complete the SM2 https encryption reconstruction, easily realize the four-in-one comprehensive website security protection of https encryption, cloud WAF protection, CDN distribution and website trusted identity certification at the same time.

Richard Wang

Jan 06, 2023
In Shenzhen, China