

Open source SM2 ACME client and provide free SM2 ACME public service

January 7, 2026

Readers interested in certificate automation know that there are many open-source ACME clients, such as CertBot. Let's Encrypt recommends 90 of them on its official website. These open-source ACME clients have greatly promoted the widespread application of automatic management of SSL certificates. For China to popularize its SM2 SSL certificates, it naturally needs the automatic management of SM2 SSL certificates, SM2 ACME clients, and SM2 ACME public services. ZoTrus Technology, as a leading developer of SM2 ACME technology and the leading drafter of the cryptographic industry standard "Automatic Certificate Management Specification", has finally found the time to develop a public-interest SM2 ACME client and make it completely open-source after completing the development of its SM2 ACME product — ZoTrus HTTPS Automation Gateway. Simultaneously, it provides free SM2 ACME services to the public. This article discusses this significant achievement, hoping that industry peers can join ZoTrus Technology in contributing to the popularization of SM2 ACME service.



1. ACME is not a product, but an ecosystem.

ACME is an abbreviation for "Automatic Certificate Management Environment", and it's also an English word meaning "ultimate". The RFC 8555 standard uses this word as an abbreviation for its technical standard with a very clear meaning: this is the ultimate solution for SSL certificate

management; there is no better solution. This solution is not a single product, but an ecosystem (environment), encompassing multiple products within that ecosystem, going beyond simply automating certificate application.

The first requirement is a Certificate Authority (CA) capable of providing ACME services, accepting certificate applications and performing domain control validation according to related standards, and issuing SSL certificates for ACME clients to download and deploy. Of course, the root CA certificate used to issue SSL certificates must be included and trusted by the four major browsers.

The second is the ACME client, which handles SSL certificate applications, including private key and CSR generation, submitting the CSR to the ACME server, and retrieving and configuring the certificate on the web server after issuance. The biggest challenge with this client is adapting to various operating systems and web servers. If it's not paid software, it can only rely on the spirit of internet generosity and encourage experts to contribute their work. Another crucial aspect is gaining user trust, as the software is installed on the user's web server; the current solution is open source.

The third is cryptographic middleware, such as the commonly used OpenSSL. This is very important as it provides support for various cryptographic algorithms required for HTTPS encryption.

Another participant is the browsers. Although this fourth party doesn't directly participate in ACME service, browser cryptographic algorithm support and trusted root CA certificates are essential elements. This is why the four major browsers are actively promoting ACME.

2. What are the challenges in building a SM2 ACME ecosystem?

To build a SM2 ACME ecosystem, it must refer to the international ACME ecosystem, but it is more difficult than the international ecosystem in the following four aspects:

First, there must be a CA that provides both SM2 SSL certificates and RSA/ECC SSL certificate issuance ACME service, the SM2 SSL certificate trusted by commonly used SM2 supported browsers and the RSA/ECC SSL certificates trusted by the four major browsers. But there are very few CAs in China that can issue dual-algorithm SSL certificates, and they all still use the traditional manual application business model for SSL certificates. Currently, there are no China CAs that can provide

SM2 ACME service.

Second, currently, there is no usable SM2 ACME client software available on the market, let alone open-source one. Why not? Because you can't make bricks without straw; without the first prerequisite, there's no second element. Even if someone were enthusiastic enough to develop one, there would need to be one SM2 ACME service to interface with it.

Third, because commonly used web server software does not support SM2 algorithms, the ACME service cannot only provide ACME client and ACME service, but also web server algorithm middleware that supports Chinese cryptographic algorithms. Currently, commonly used ones are DongsuoSSL and openHiTLS.

Fourth, currently, all browsers that support the Chinese cryptographic algorithm are paid software, except ZT Browser. This is one of the biggest difficulties in popularizing the Chinese cryptographic HTTPS encryption in China.

3. ZoTrus knows the road ahead is fraught with difficulties, but it still perseveres.

ZoTrus Technology positioned itself as a leader in automatic cryptographic applications. Its first project was automatic SSL certificate management, essentially building its own entire ACME ecosystem – a self-reliant approach rather than relying on others. After more than four years of development, ZoTrus Technology has completely solved the four major challenges mentioned above, and is the world's only company to have created the three essential products required for the ACME ecosystem:

First, SM2 ACME Service: ZoTrus Cloud SSL Service System (including ACME Service System) not only connects with multiple international CAs to provide RSA/ECC algorithm SSL certificate ACME services, but also connects with multiple China licensed CAs to provide SM2 algorithm SSL certificate ACME services. The automatically issued dual-algorithm SSL certificates are globally trusted and compliant with China cryptographic standards.

Second, SM2 ACME clients: including the free SM2cerBot software released this time and the paid

SM2 HTTPS Automation Gateway. The former requires users to deploy it on their own web server and requires them to deploy the Chinese cryptographic algorithm support middleware; the latter is a solution for users' web servers with zero modification, which not only solves the challenge of certificate automation, but also solves the challenges of Chinese cryptographic compliance and post-quantum cryptography migration.

Third, SM2 supported browser: ZT Browser is a completely free, clean, and ad-free browser that supports both Chinese cryptographic algorithms, international algorithms and post-quantum cryptography algorithms. This completely solves the problem of lack of browser support for the widespread adoption of Chinese cryptographic HTTPS encryption. Precisely because it is user-friendly and free, ZT Browser has become the No. 1 market share Chinese cryptographic supported browser in China.

ZoTrus Technology has completed all the missing products in the entire SM2 ACME ecosystem. In particular, the free provision of SM2 ACME public services and open-source SM2 ACME clients will make a historic contribution to promoting the development of SM2 ACME services, accelerate the popularization and application of commercial cryptographic algorithms in China to achieve HTTPS encryption, and not only effectively safeguard China's cyberspace security, but also provides an optional solution for global Internet security.

ZoTrus Technology firmly believes that dreams, though distant, can be achieved through pursuit; wishes, though difficult, can be fulfilled through perseverance. ZoTrus Technology is committed to contributing to the popularization of Chinese cryptographic HTTPS encryption by providing free ACME services and an open-source ACME client.

Richard Wang

January 7, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.

The author has published 110 articles in English (more than 150K words) and 251 articles in Chinese (more than 739K characters in total).

