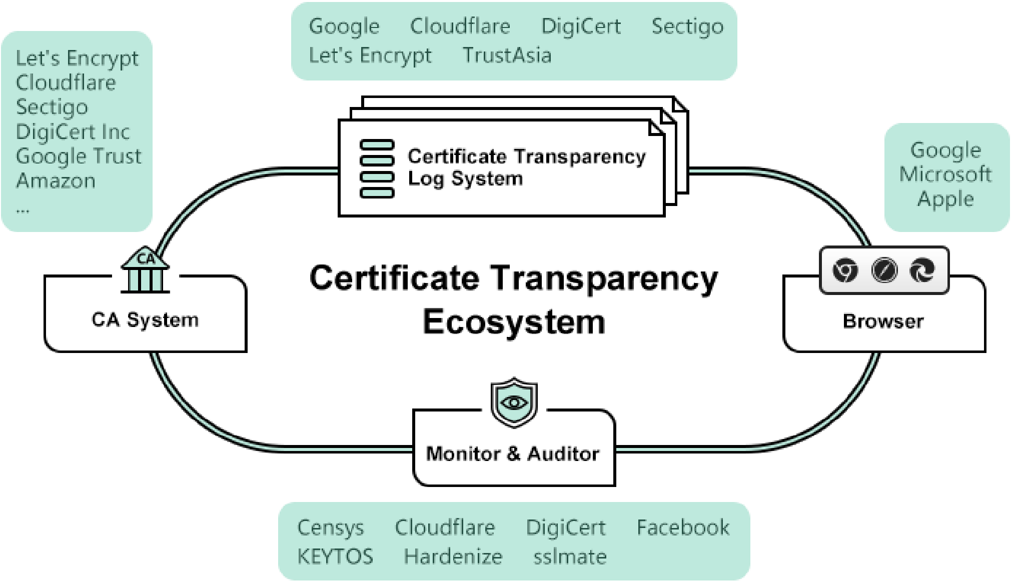
2023, the First Year of Popularization of SM2 HTTPS Encryption in China

At the "2018 Cyberspace Trust Summit" (2008.12.17), the author first proposed the concept of "China Cyberspace Trust Ecological Construction Framework", and proposed the application idea of the SM2 SSL certificate - first "dual-certificate system" and then becoming a "single-certificate system", this "dual- certificate system" is deploying dual-algorithm and dual-SSL certificate for transition. After the SM2 application ecology matures, the "single-certificate system" is naturally realized (only the SM2 SSL certificate needs to be deployed). Through the continuous efforts of the cryptography industry in the past 4 years, especially the official implementation of the "Cryptography Law" on January 1, 2020, the author has reason and confidence to believe that 2023 is "the first year of popularization of national secret HTTPS encryption".

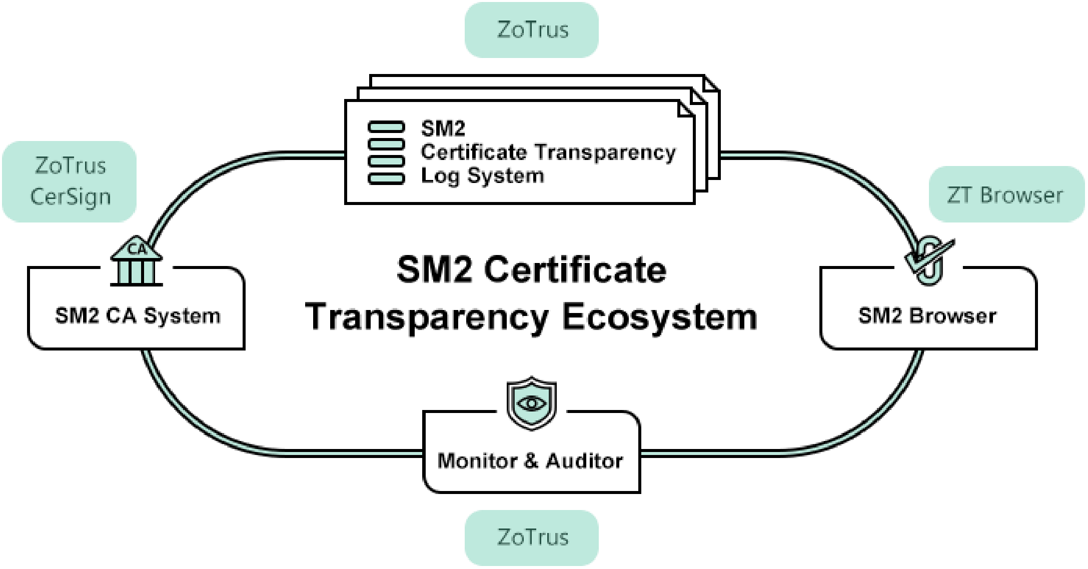
The author's self-confidence comes from the two major SM2 SSL certificate ecosystem created by ZoTrus: the SM2 Certificate Transparency (SM2 CT) ecosystem and the SM2 Automatic Certificate Management Ecosystem (SM2 ACME). The first ecosystem is a reliable supply ecology of the certificate SSL certificate, and the second is a reliable solution for rapid deployment application ecology of the SM2 SSL certificate. The two ecosystems fully refer to the successful route of the 8.4 billion international SSL certificates that have been issued and are customized according to the application status of the SM2 algorithm, making full preparations for the popularization of SM2 SSL certificate applications in China. Therefore, the author calls year 2023 is the "first year of popularization".

The trigger point of the "first year of popularization" was that within a week after the Russia-Ukraine conflict in February last year, more than 3,000 RSA algorithm SSL certificates of the Russian government and bank websites were revoked, resulting in many government websites and bank websites being unable to access normally. Not only that, but the RSA SSL certificate is also not allowed to be issued to Russian government websites and bank websites at the same time. This has sounded the security alarm for China government websites and bank websites because China government websites and bank websites are also using RSA algorithm SSL certificates! This Internet security incident has made government authorities and the security industry fully aware of the importance and urgency of popularizing and applying China commercial algorithm SM2 SSL certificate for https encryption! Therefore, this incident has formed a consensus in the industry, which is very important! As early as the author pointed out in his speech at the 7th Internet Security Conference in 2019, "Is China ready for the supply-broken and revocation of RSA SSL certificates?" At that time, some "experts" retorted, saying that I was "alarmist"! But now, this incident actually happened in Russia, and everyone immediately reached a consensus. This is the trigger point for the first year of popularization of SM2 SSL certificates! It has deeply touched the consensus of the cryptography industry and has made full efforts to enhance the supply capacity of SM2 SSL certificates, providing sufficient solutions that can meet the deployment needs of various application parties.

The author will first talk about the construction of the reliable supply capacity of the SM2 SSL certificate. The reason why RSA SSL certificates have been able to reliably issue 8.4 billion SSL certificates since 2013 and reliably protect the security of the global Internet is because of the Certificate Transparency ecology, which ensures the reliable supply of RSA SSL certificates. There is a CA system (SSL certificate provider) that can issue SSL certificates that support certificate transparency, browsers that can verify certificate transparency, and third-party supervision and audit of certificate issuance. This ecosystem ensures the reliable supply of RSA SSL certificates.



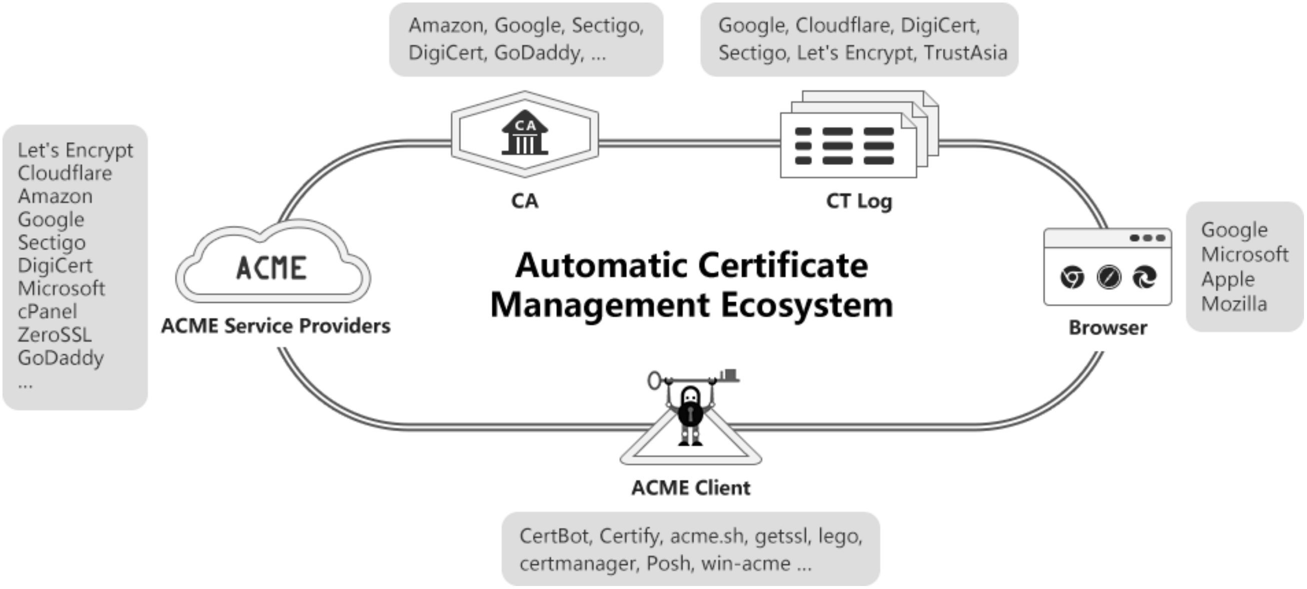
Although several China CAs have begun to issue SM2 SSL certificates since 2019, and some browsers support SM2 SSL certificates, the most important monitoring system in this ecosystem has not been established, and there is no certificate transparency log system that supports SM2 algorithm. So, of course, the SM2 SSL certificate cannot support the certificate transparency, and the browser cannot support the certificate transparency, and the supervisor will not be able to obtain the certificate issuance data to perform the supervisory function. The author discovered this key problem many years ago. The first thing to do after starting a new business in June 2021 is to establish a SM2 certificate transparency ecosystem with reference to the international certificate transparency ecosystem. On November 8, 2022, it was launched at the Wuzhen 2022 World Internet Conference and launched the world's first SM2 certificate transparency log system. After the release of this ecosystem, it has been recognized and recognized by the cryptographic industry.



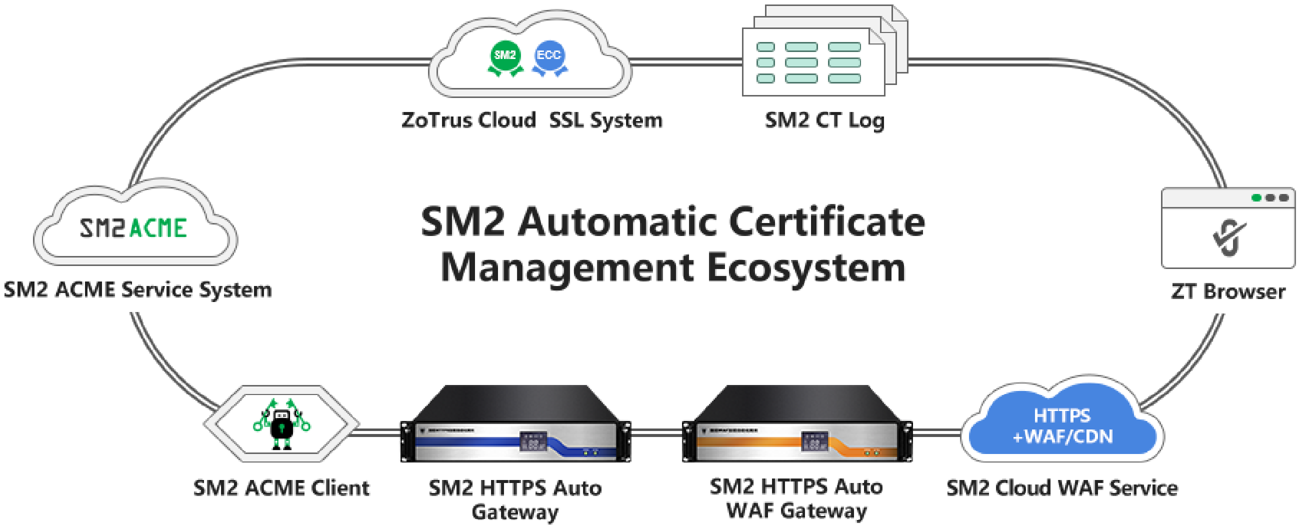
Now, the SM2 certificate transparency ecosystem has achieved initial results. Not only the SM2 SSL certificates issued by ZoTrus and CerSign support the SM2 Certificate Transparency, but many Chinese CAs have begun to transform the existing CA system to support the SM2 Certificate Transparency. Not only ZT Browser supports the SM2 Certificate Transparency, but several browsers have begun to plan to upgrade to support the SM2 Certificate Transparency. The most gratifying thing is that the Cryptography Administration Authority also plans to build a national SM2 certificate transparent log system to exercise its supervisory functions, and several companies are also interested in operating the SM2 certificate transparent log system. There are also third-party market research agencies interested in providing certificate market analysis services based on the SM2 certificate transparency log data. These gratifying concerted actions make the author firmly believe that the SM2

Certificate Transparency ecology will be formed soon, and the reliable supply capacity of SM2 SSL certificates will soon be available, providing a secure and reliable supply for the first year of popularization of SM2 HTTPS encryption.

Let me talk about the deployment and application ecosystem construction of the SM2 SSL certificate. The deployment of SSL certificates globally developed slowly before 2015, with an average annual growth rate of about 5%. The key constraint to this slow growth rate is that it is too difficult to apply for and deploy SSL certificates. However, after Let’s Encrypt started to automate the provision of free SSL certificates in 2015, the penetration rate of SSL certificates has rapidly increased from 30% to 80% in just three years. Especially after the introduction of the RFC 8555 ACME (Automated Certificate Management Environment) international standard in 2019, the proportion of automated application and deployment of SSL certificates in the world has reached 85%. This has given us a lot of inspiration, the popularization of SM2 SSL certificate cannot follow the old path of manual application and deployment of certificates but must take the new path of automatic application and deployment of certificates.


Amazon, Google, Sectigo, DigiCert, GoDaddy, ...
Google, Cloudflare, DigiCert, Sectigo, Let's Encrypt, TrustAsia
CA
CT Log
Let's Encrypt
Cloudflare
Amazon
Google
Sectigo
DigiCert
Microsoft
cPanel
ZeroSSL
GoDaddy
...
ACME
ACME Service Providers
Automatic Certificate Management Ecosystem
Browser
Google
Microsoft
Apple
Mozilla
ACME Client
CertBot, Certify, acme.sh, getssl, lego, certmanager, Posh, win-acme ...

However, this new path of automation certificate management is not our path, because the international ACME protocol does not support the SM2 SSL certificate, so ZoTrus Technology has vigorously created the second ecosystem of SM2 SSL certificate - the SM2 Automatic Certificate Management Ecosystem (SM2 ACME), this ecosystem is specially created for the rapid popularization and application of SM2 SSL certificates. This ecosystem includes multiple products in the SM2 Certificate Transparency ecosystem, including the ZoTrus Cloud SSL System with the addition of the SM2 ACME Service System, the dual-algorithm dual SSL certificate, the SM2 certificate transparency log system, ZT Browser, ZoTrus Website Security Cloud Service, two new products have been added, the ACME client and the HTTPS Gateway.



The SM2 ACME client and the SM2 ACME Service System are designed with reference to the international ACME standard. Users only need to install the SM2 ACME client software-SM2cerBot on the server and realize the dual-algorithm dual-SSL certificate deployment and https encryption with one click. For users who cannot install the SM2 ACME client software on the server, they can choose to deploy the SM2 HTTPS Gateway with the built-in SM2 ACME client to automatically deploy dual SSL certificates and realize the zero transformation of the original Web server and the zero installation of the SM2 SSL certificate to realize https encryption. For users who do not want to deploy or cannot deploy a hardware gateway, they can choose the Website Security Cloud Service, and only need to do domain name resolution to realize the four-in-one website protection service including SM2 https encryption, cloud WAF protection, CDN distribution and website trusted identity certification.

With the SM2 Automatic Certificate Management Ecosystem products and solutions, it becomes very easy to popularize the SM2 SSL certificate to realize the SM2 https encryption. It can achieve the same rapid growth as the international SSL certificate after the automatic deployment, the popularization of SM2 SSL certificate applications is just around the corner. This is why the author is confident that

2023 is the "first year of popularization of SM2 HTTPS encryption". The rapid popularization and use of SM2 SSL certificate can be realized after eliminating obstacles, this has been confirmed and verified by the rapid popularization of international SSL certificates.
The first year of the popularization of SM2 HTTPS encryption is coming, China websites will start the year of SM2 algorithm protection! In this way, even if the case like Russian SSL certificate supply-broken and revoked happens in some day in the future, it will not have any impact on China websites, because China websites does not use its sanction tool (RSA SSL certificate) at all!

The first year of SM2 HTTPS encryption popularization is coming, are you ready?

Richard Wang

Jan 12, 2023
In Shenzhen, China