Commercial cryptography HTTPS encryption ecosystem construction

[This article comes from the official WeChat account of CCID Cryptography Information Security, Author: Richard Wang]

Abstract

China is vigorously promoting the comprehensive application of commercial cryptography in all walks of life, and has achieved some gratifying results, many applications have almost completely replaced the international cryptography algorithms. However, progress in the application of HTTPS encryption on websites has been slow, and almost all e-government websites and online banking systems still use the international RSA/ECC algorithm to implement HTTPS encryption. After the Russia-Uzbekistan conflict, a large number of RSA algorithm SSL certificates deployed on Russian e-government websites and bank websites were revoked and supply-broken. This warns that China must accelerate the deployment and application of commercial cryptography SSL certificates. However, China commercial cryptography SSL certificates started late, and various related technical specifications and solutions are not perfect, and related system software must be reconstructed to support commercial cryptography algorithms, which will inevitably affect the rapid popularization and application of commercial cryptography SSL certificates. This article introduces in detail how to establish the supply ecosystem and application ecosystem of China commercial cryptography SSL certificates, which can effectively improve the China commercial cryptography HTTPS encryption ecosystem, so as to realize the rapid popularization and application of commercial cryptography SSL certificates and popularize the application of commercial cryptography to reliably protect China website and system security.

I. Introduction

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 commercial cryptography 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 COMMERCIAL CRYPTOGRAPHY 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, various ecological products and ecological construction of commercial cryptography SSL certificates have made great progress and are becoming more and more perfect.

The trigger point of the popularization of the commercial cryptography SSL certificates 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 COMMERCIAL CRYPTOGRAPHY 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 COMMERCIAL CRYPTOGRAPHY SSL certificates! It has deeply touched the consensus of the cryptography industry and has made full efforts to enhance the supply capacity of COMMERCIAL CRYPTOGRAPHY SSL certificates, providing sufficient solutions that can meet the deployment needs of various application parties.

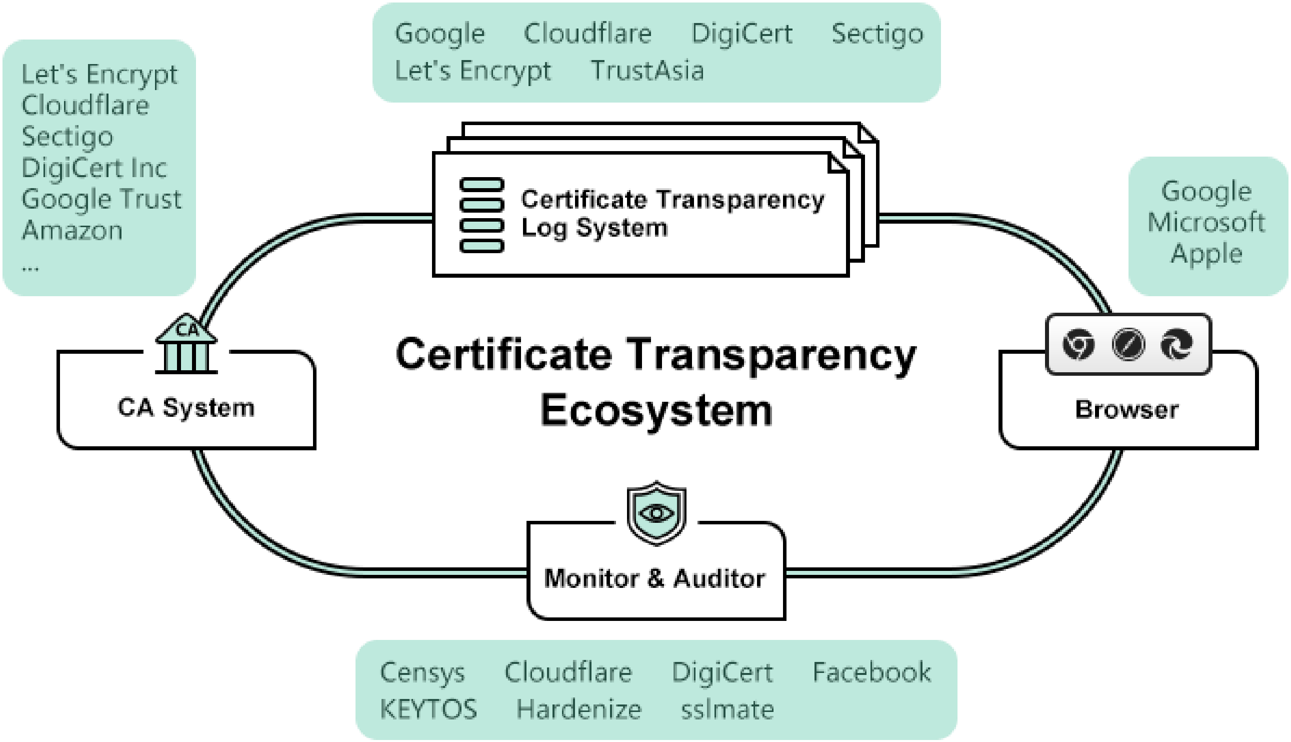
II. Introduction to the International Cryptography HTTPS Encryption Ecosystem

At present, HTTPS encryption based on the international cryptographic system has been widely used around the world, effectively protecting the security of data communication on the global Internet. Since 2013, 8.4 billion international cryptographic algorithm RSA/ECC SSL certificates have been issued reliably. The international HTTPS encryption ecosystem mainly includes the international certificate transparency ecosystem and the automatic certificate management ecosystem. These two systems realize the reliable and secure supply and rapid deployment and application of international algorithm SSL certificates.

2.1 International Certificate Transparency Ecosystem

The international certificate transparency ecosystem is the first important ecology of the international cryptographic HTTPS encryption ecosystem. This is a system led by Google, including a certificate transparency log system, browsers that support certificate transparency, and CA systems (SSL Certificate Providers) for issuing SSL certificates that support certificate transparency, and third-party services that monitor and supervise certificate issuance behaviors using certificate transparency log system data. There are multiple organizations participating in the four parts of this ecosystem to jointly ensure the reliable supply of international algorithm SSL certificates.

An important player in the international certificate transparency ecosystem is Google. The reason why Google can take the lead in achieving certificate transparency is of course inseparable from the influence and market share of Google Chrome. Google released the certificate transparency log system, which first occupied the moral high ground - "transparency", and secondly, of course, using the influence of its browser has come up - if the SSL certificate issued by the CA does not support certificate transparency, Google Chrome will not trust it, and there will be a "Not secure" warning! Later, Apple Safari browser also joined the camp of helping certificate transparency, and the same does not trust SSL certificates that do not support certificate transparency! Later, the addition of the Microsoft Edge browser also distrusts SSL certificates that do not support certificate transparency! If the browser does not support certificate transparency, it is equivalent to trusting the SSL certificate issued maliciously and used for attacks, how can such a browser guarantee the Internet security of browser users? Browsers are the first major players in the Certificate Transparency ecosystem.



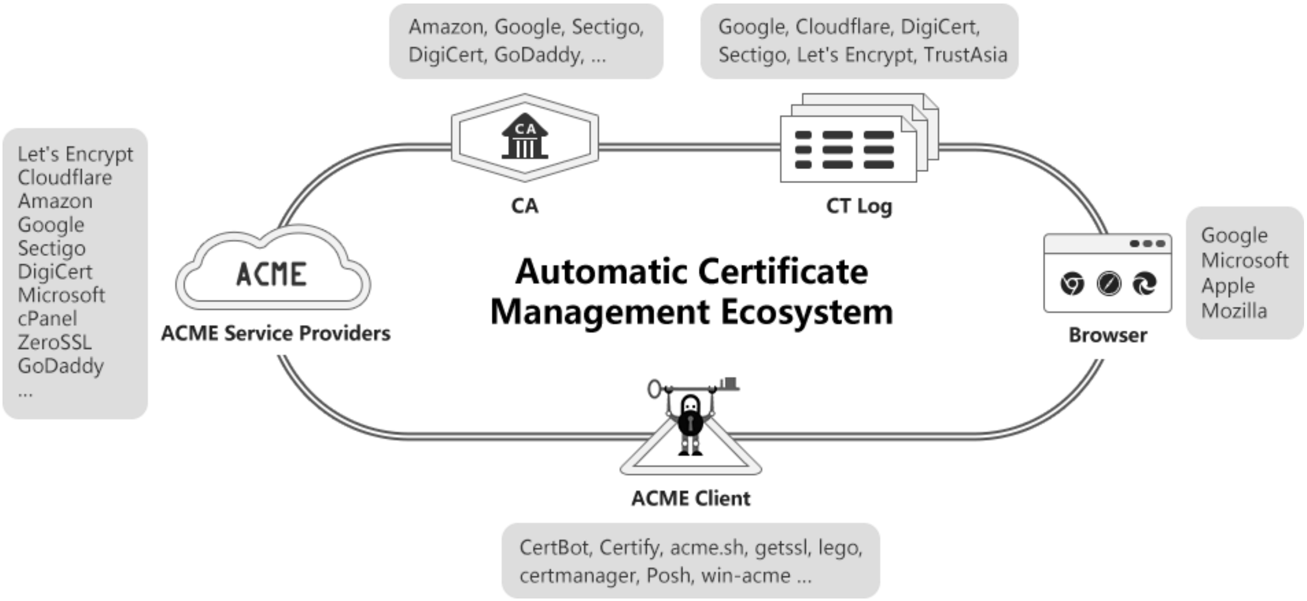
The second important participant in the international certificate transparency ecosystem is the operator of the certificate transparency log system. There must have certificate transparency log system first. This is the source, or it is led by Google. Google not only developed the certificate transparency log system, but also made this system completely unconditionally open source, encouraging many companies to deploy and maintain their own certificate transparency log systems to jointly provide certificate transparency log services for SSL Certificate Providers (CA operators). At present, besides Google's own certificate transparent\cy log system, the participants of the certificate transparency log system certified and trusted by Google Chrome include: Cloudflare, the world's leading CDN service provider, and 4 famous CAs: Sectigo, DigiCert, Let's Encrypt and TrustAsia.

The SSL Certificate provider (CA operator) is the third participant. It is not only the service object of the certificate transparency ecology but also the object of supervision. At present, the international SSL certificates issued by dozens of CA operators in the world have already supported certificate transparency. Each type of SSL certificate has been submitted to the above certificate transparency log systems certified and trusted by Google for transparency.

The last important participant is the monitoring and auditing party. The responsibility of this party is to ensure that all SSL certificates that have been embedded in SCT data are visible in the certificate transparency log system, and to observe suspicious certificates in the log. Users can subscribe to these service providers' services in order to receive notifications in a timely manner. These services can help website owners discover suspicious certificates in a timely manner and effectively protect the legitimate rights and interests of website owners.

2.2 International automatic certificate management ecosystem

The international certificate transparency ecosystem effectively guarantees the reliable and trusted supply of global trusted SSL certificates. However, the deployment of SSL certificates 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 RFC8555 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% now. This has given us a lot of inspiration, that is, the popularization of commercial cryptography SSL certificates cannot follow the old path of manual application and deployment of certificates but must take the new path of automatic certificate application and deployment.


Amazon, Google, Sectigo, DigiCert, GoDaddy, ...
Google, Cloudflare, DigiCert, Sectigo, Let's Encrypt, TrustAsia
CA
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 ...

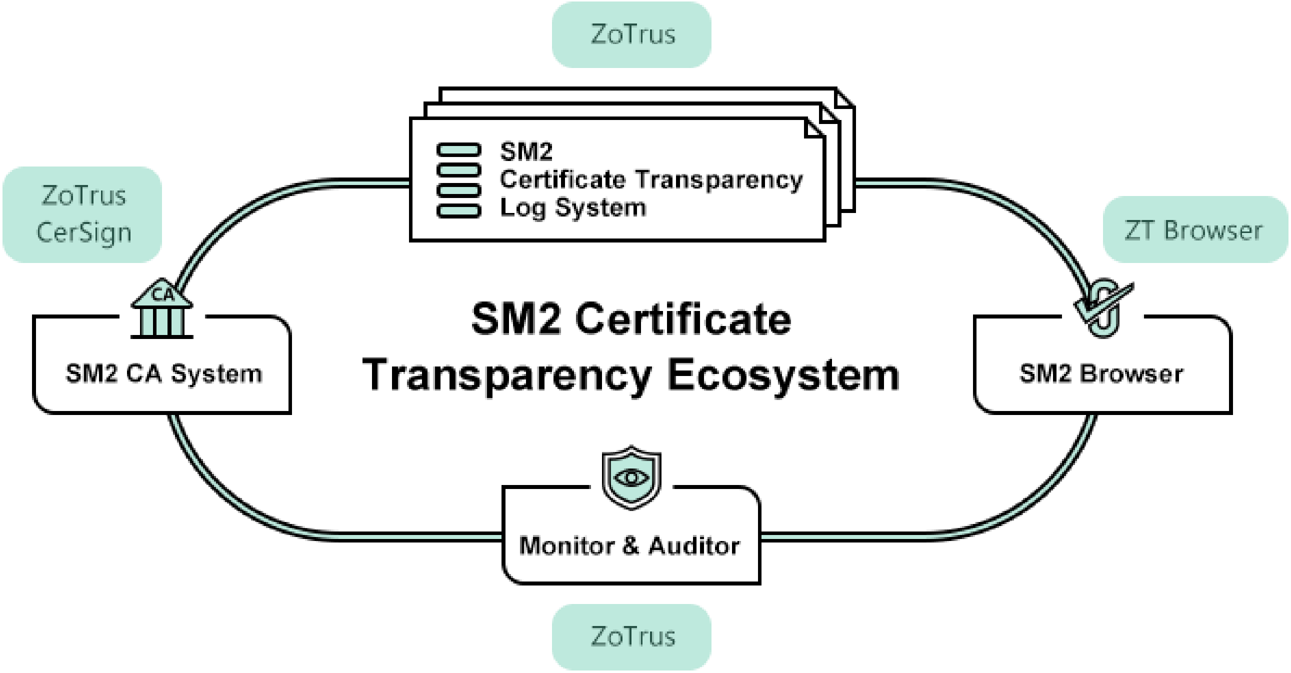
III. Commercial cryptography HTTPS encryption ecosystem construction

The international cryptography HTTPS encryption ecosystem guarantees the security and trustworthiness of 8.4 billion international algorithm SSL certificates around the world, and successfully realizes the international algorithm https encryption to ensure the security of data communication on the global Internet. However, this system does not support commercial cryptography algorithms, cannot be used to ensure the security of commercial cryptography SSL certificates, and cannot be used for rapid deployment and application of commercial cryptography SSL certificates to implement commercial cryptography algorithm HTTPS encryption. China must refer to this international system to build a system that supports commercial cryptography algorithms, including a commercial cryptography certificate transparency system and a commercial cryptography automatic certificate management ecosystem, so as to ensure the successful realization of secure and reliable commercial cryptography SSL certificate supply and rapid deployment of applications to achieve commercial cryptography HTTPS encryption.

3.1 Commercial cryptography certificate transparency construction

Although a number of China CAs have begun to issue commercial cryptography SSL certificates since 2019, and there are also browsers made in China that support commercial cryptography SSL certificates, but the most important regulatory system in this ecosystem has not been established, and there is no certificate transparency log that supports commercial cryptography algorithms, commercial cryptography SSL certificates will of course have no way to support commercial cryptography certificate transparency, and browsers will also have no way to start supporting commercial cryptography certificate transparency. Of course, regulators will have nowhere to obtain certificate issuance data to perform regulatory functions. Establish a commercial cryptography certificate transparency ecosystem with reference to the international certificate transparency ecosystem. Fortunately, ZoTrus Technology launched the world's first commercial cryptography certificate transparency log system at the Wuzhen 2022 World Internet Conference on November 8, 2022, and released commercial cryptography certificate transparency related ecological products, successfully creating a SM2 certificate transparent ecosystem (SM2 CT), this ecosystem has been highly recognized and recognized by the cryptographic industry after its release.

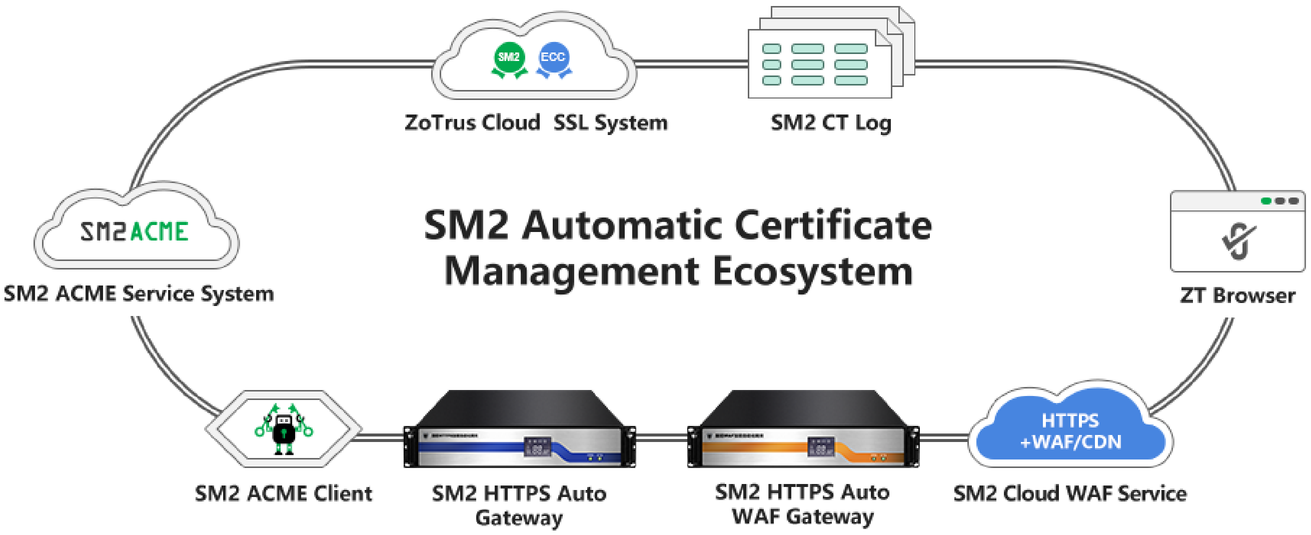
At present, the commercial cryptography certificate transparency ecosystem has achieved initial results. Not only the commercial cryptography SSL certificates issued by ZoTrus and CerSign support the commercial cryptography certificate transparency, but many Chinese CAs have begun to upgrade the existing CA system to support the commercial cryptography certificate transparency. Not only ZT Browser supports commercial cryptography certificate transparency, but several browsers have already started planning to upgrade to support commercial cryptography certificate transparency. The most gratifying thing is that the commercial cryptography administrative authority also plans to build a national commercial cryptography certificate transparency log system to exercise its regulatory functions as a competent authority, and several companies are interested in operating a commercial cryptography certificate transparency log system. There are also third-party market research agencies interested in providing certificate market analysis services based on commercial cryptography certificate transparency log data. These gratifying concerted actions will quickly form a commercial cryptography certificate transparency ecology. China will soon have a reliable supply of commercial cryptography SSL certificates, providing a secure and reliable "source" for the popularization and application of commercial cryptography HTTPS encryption.



3.2 Commercial cryptography automatic certificate management ecosystem construction

The rapid popularization and application of international SSL certificates is due to the construction of the international automatic certificate management ecosystem, including the establishment of the ACME standard (RFC 8555) and the provision of international SSL certificate automation management services by multiple companies. This is a new way to quickly deploy SSL certificates. However, the international certificate automation management system only supports international cryptographic algorithm RSA/ECC SSL certificates and does not support commercial cryptographic algorithm SM2 SSL certificates. This new automated way is not our way. China must also establish a road to automatic certificate management ecosystem that supports commercial cryptographic algorithms.

The good news is that ZoTrus Technology has vigorously created the second ecosystem of commercial cryptography SSL certificates – Commercial Cryptography Automatic Certificate Management Ecosystem (SM2 ACME), which is specially created for the rapid popularization and application of commercial cryptography SSL certificates. This ecosystem includes multiple products in the commercial cryptographic certificate transparency ecosystem, including the ZoTrus Cloud SSL System with the SM2 ACME Service System, dual-algorithm dual SSL certificates, the SM2 Certificate Transparency Log system, ZT Browser, and the new developed the SM2 ACME Client, SM2 HTTPS Gateway and Website Security Cloud Service that support SM2 ACME.



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, to realize the dual-algorithm dual-SSL certificate of SM2 SSL certificate and ECC SSL certificate application and deployment with one click, and automatically implement https encryption using commercial cryptography. 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, to realize the zero change of the original web server and the commercial cryptography https encryption. For users who do not want to deploy or cannot deploy a hardware gateway, they can choose ZoTrus Website Security Cloud Service, which can realize commercial cryptography https encryption, cloud WAF protection, CDN distribution and website trusted identity certification with zero modification and zero installation, only need to do the domain name resolution for the four-in-one website security service.

With the commercial cryptography automatic certificate management ecosystem products and solutions, it becomes very easy to popularize commercial cryptography SSL certificates to realize commercial cryptography HTTPS encryption, and it can achieve the same rapid growth as international SSL certificates after automatic deployment, and popularize commercial use of the commercial cryptography SSL certificate is just around the corner, and the obstacle of rapid popularization and use of commercial cryptography SSL certificate must be eliminated, this has been verified and confirmed by the rapid popularization of international SSL certificate deployment.

IV. Conclusion

The reason why the international SSL certificate has achieved great success in ensuring the security of global Internet data communication is due to the construction of two ecosystems, one is the certificate transparency ecosystem, which effectively guarantees the secure and reliable supply of international algorithm SSL certificates; the other is the automatic certificate management ecosystem, providing technical means and solutions for the rapid deployment of international algorithm SSL certificates. China must refer to these two ecosystems to construct the commercial cryptography certificate transparency ecosystem and the commercial cryptography automatic certificate management ecosystem, in order to ensure the rapid and healthy development of commercial cryptography SSL certificate.

The SM2 certificate transparency ecosystem created by ZoTrus Technology is an ecosystem that guarantees the reliable supply of commercial cryptography SSL certificates, and the SM2 automatic certificate management ecosystem is an ecology that realizes the rapid deployment and application of commercial cryptography SSL certificates. These two ecosystems fully refer to the successful route of the 8.4 billion international algorithm SSL certificates, and are customized according to the current situation of commercial cryptography algorithms, making full preparations for the popularization of commercial cryptography SSL certificate applications in China and the popularization of commercial cryptography https encryption is just around the corner, and Chinese websites will open the year of commercial cryptography algorithm protection! In this way, even if one day in the future, the same situation as Russia's SSL certificate is revoked and supply-broken, it will not have any impact on China websites, because at that time China website did not use its sanction tool (RSA SSL certificate) at all! The first year of commercial cryptography HTTPS encryption is coming!

Richard Wang

Jan. 17, 2023
In Shenzhen, China