In 2023, ZoTrus Contributed China's Solutions to Global Internet Security

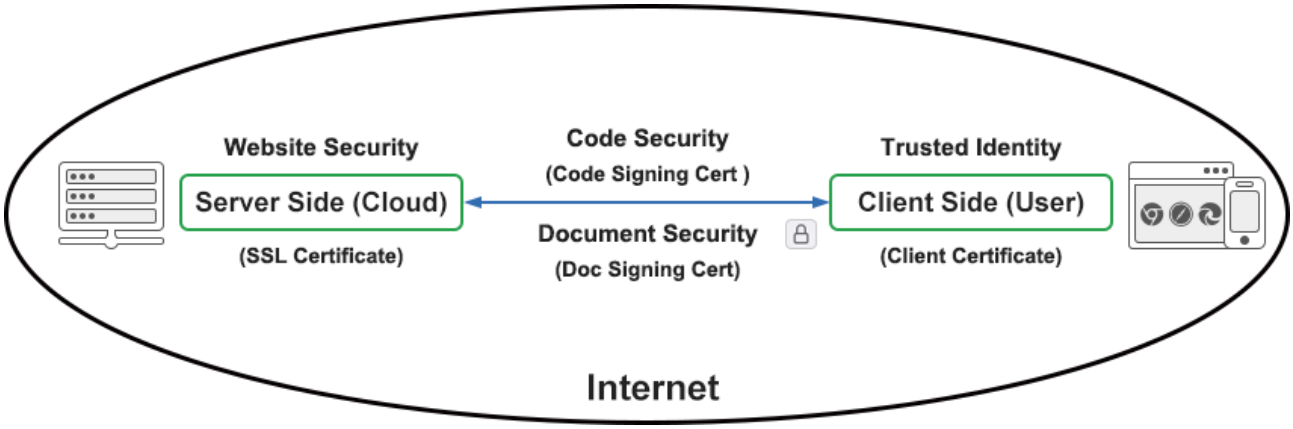
The year 2023 is coming to an end, and the new year 2024 is about to begin. Looking back on 2023, ZoTrus Technology has not failed to live up to its glory and contributed China's solutions to global Internet security. Looking forward to 2024, ZoTrus will continue to provide more innovative products and services for global Internet security.

1. Cryptography has fully protected the security of the global Internet

The Internet has been commercialized and popularized since the 90s, and the biggest technical contribution is the invention of SSL certificate and the support of HTTPS encryption in browsers and Web servers. Without these, there would be no prosperity of today's Internet. Because when the Internet was invented, due to its internal use, no encryption measures were considered at all, and all of them were plaintext transmissions, including the No.1 biggest Internet application - Web service that it uses HTTP plaintext transmission protocol, the first Internet application - Email is also plaintext transmission - IMAP and SMTP protocol, and the domain name resolution service (DNS) is also a plaintext protocol. Only having SSL certificate can the HTTPS encrypted transmission protocol be realized, and an additional "S" is Secure. Only having SSL certificate can IMAPS and SMTPS encrypted email sending and receiving protocols be realized, and an additional "S" is Secure. Only having SSL certificates can DoH (DNS Over HTTPS) and DoT (DNS Over TLS) encrypted DNS services be realized, and an extra "S" is Secure.

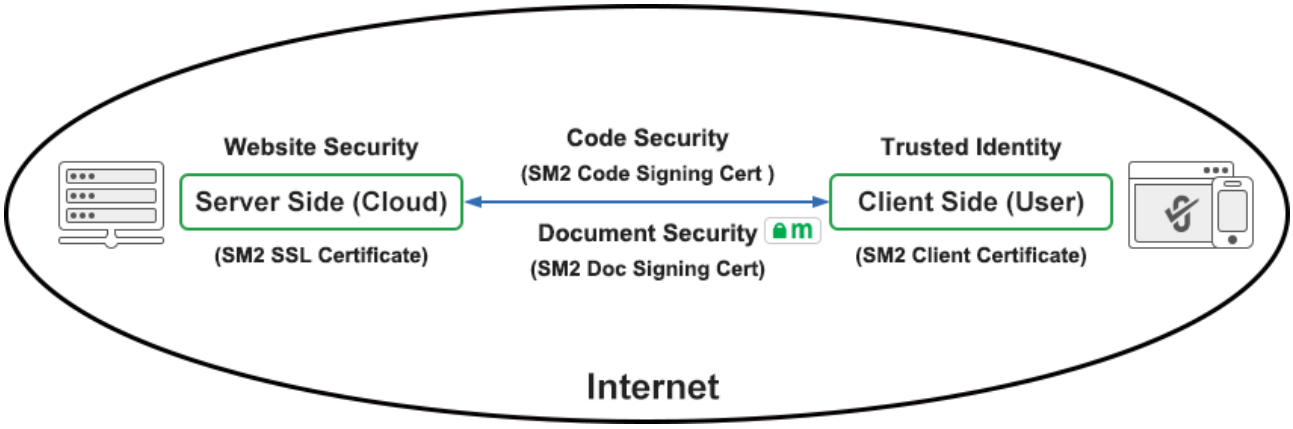
The SSL certificate not only ensures the trusted identity of the server, but also ensures the encryption of information transmission from the server to the client. In addition, client certificates are used to ensure the client identity trust and email encryption, document signing certificates are used to prove document trust and document encryption, and code signing certificates are used to trust software code identity. In other words, it is the largest application of cryptography-PKI/CA and its products to ensure the security and trust of the global Internet, and this cryptographic system is the RSA algorithm cryptosystem, which has successfully ensured the security of the global Internet and the Internet of

Everything for more than 40 years. And 11.5 billion SSL certificates have been issued since 2013 when the certificate transparency log were operated, which effectively protects the information transmission security of web applications, emails, and DNS etc.



2. Commercial Cryptography (ShangMi) provides China's solution for global Internet security

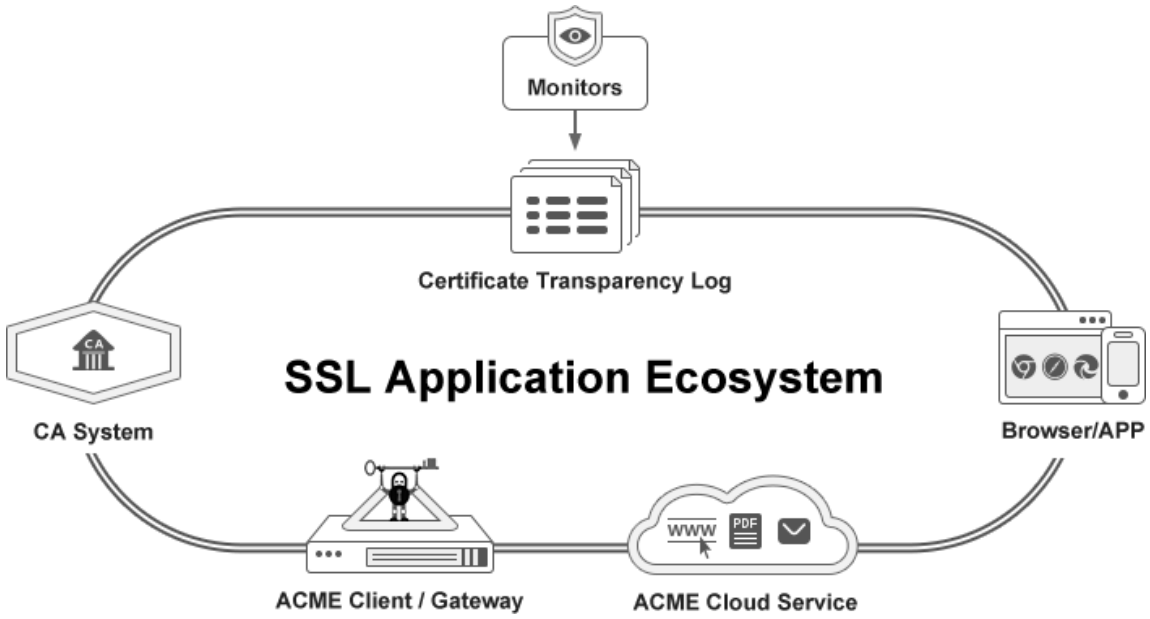
Because the RSA algorithm cryptosystem is so important, Internet security is inseparable. Therefore, this monopoly technology has become a sanction tool, which is a leading to systemic risk to global Internet security. As a big country in technological innovation, China has provided solution to break the monopoly of cryptography technology, which is the commercial cryptographic algorithm - SM2/SM3/SM4/SM9 algorithm, which has become an international standard algorithm like the RSA/ECC algorithm. China has established a complete commercial cryptography ecosystem with reference to the RSA cryptographic system, including the establishment of a series of commercial cryptography standards, the development of CA system that can issue various commercial cryptography algorithm digital certificates, and the development of a large number of Internet application software based on commercial cryptography, such as SM2 browsers, SM2 document readers, SM2 email clients, etc., to achieve SM2 HTTPS encryption, SM2 IMAPS and SMTPS encryption, SM2 DNS encryption and other Internet security applications.



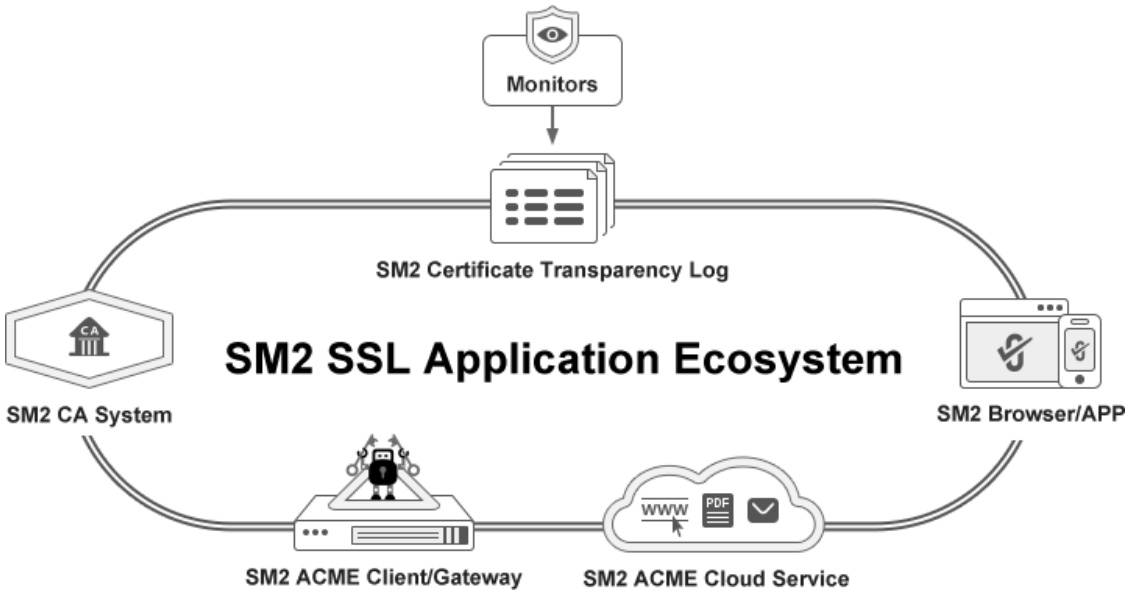
China Commercial Cryptography has not only begun to be used to ensure the security and trust of Internet in China, but also another option for global Internet users, an option that can also be used to ensure global Internet security, which is already very complete like the RSA algorithm cryptosystem, which can also ensure the security and trust of Web applications, emails, e-documents and DNS etc. This is the contribution of China Cryptography to global Internet security, allowing global users to have more choices, ensuring a more stable and healthy development of the global Internet, and ensuring that global Internet users can enjoy Internet services without interruption and without discrimination.

3. ZoTrus provides innovative solutions to give global Internet users more choices

SSL certificate and HTTPS encryption are the core security products and applications of global Internet security, SSL certificate is the world's most used cryptographic product, which is an ecology around the issuance, supervision and application of SSL certificates, including the CA system that can issue SSL certificates, the certificate transparency log used to supervise the issuance of SSL certificates and the supervision and audit based on this system, and the browsers used to realize HTTPS encryption. ACME client software, hardware gateway, and cloud service for automating the application and deployment of SSL certificates. This ecosystem ensures that SSL certificates can be reliably issued and quickly deployed for application, thus ensuring the basic communication security of the global Internet.



Similarly, the use of SM2 SSL certificates and SM2 HTTPS encryption is also the core security products and applications of global Internet security that users can choose, and there is also a need for an ecosystem around the issuance, supervision and application of SM2 SSL certificates, including a CA system that can issue SM2 SSL certificates, a certificate transparency log used to supervise the issuance of SM2 SSL certificates and supervision and auditing based on this system, and SM2 browsers used to realize HTTPS encryption. ACME client software, hardware gateway, and cloud service used to automate the application and deployment of SM2 SSL certificates. This ecosystem ensures that SM2 SSL certificates can be reliably issued and quickly deployed for application, so as to realize the use of commercial cryptography to ensure the basic communication security of the global Internet.



In the past 2023 year, ZoTrus Technology has made great contributions to the ecological construction of SM2 SSL certificate applications, which not only protects the security and trust of China Internet applications, but also provides another option for global Internet users, among which ZT Browser, a completely free SM2 supported browser, has not only become the No. 1 market share SM2 browser in China to implement commercial cryptography HTTPS encryption, but also received the welcome and love of users worldwide from more than 130 countries and regions. Users around the world like the EV green address bar of ZT Browser, the world's first certificate transparency display UI for SSL certificates, and the world's first built-in PDF reader that verifies the digital signature of PDF documents in real time and displays the signer's trusted identity.

ZoTrus has developed all the necessary products in the application ecology of SM2 SSL certificates, and improved the application ecology of SM2 SSL certificates, mainly including the following six innovative products:

(1) **ZT Browser**: A browser based on open-source Chromium that supports SM2 algorithms, supports SM2 certificate transparency, and it is completely free.

(2) **ZoTrus Cloud SSL System**: A CA system and ACME service system that can issue SM2 SSL certificates that support SM2 certificate transparency and can issue dual algorithm (RSA or ECC and SM2) SSL certificates for users at the same time, making HTTPS encryption not only supporting China Commercial Cryptographic system but also being compatible with RSA cryptosystem.

(3) **ZoTrus SM2 CT Log**: A certificate transparency log that provides SSL certificate transparency log service for CAs free of charge, supports SM2/RSA/ECC algorithm SSL certificates, and opens up the log database for free so that third-party providers can provide supervision and audit services for SSL certificates.

(4) **ZoTrus SM2 ACME Client**: SM2cerBot, a free SM2 ACME client software for automating the application and deployment of SM2 SSL certificates, realizes the automatic certificate management of applying for and deploying SM2 and RSA algorithm dual SSL certificates at the same time.

(5) **ZoTrus SM2 HTTPS Automation Gateway**: The world's first hardware gateway product that supports automatic certificate management, automatic configuration of dual algorithm SSL certificates, and automatic realization of HTTPS encryption offloading and forwarding that have passed the China Commercial Cryptography Product Certification, so that the original web server

can automatically realize SM2 HTTPS encryption without any change, adaptive support for RSA algorithm HTTPS encryption.

(6) **ZoTrus SM2 HTTPS Automation Cloud Service**: This is an innovative cloud service that deploys the SM2 HTTPS Automation Gateway on the cloud to provide automatic certificate management, automatic configuration of dual algorithms SSL certificates, and automatic realization of HTTPS encryption offloading and forwarding, so that users can realize the automatic SM2 HTTPS encryption without any change of the original web server and no need to deploy a hardware gateway locally, adaptive support for RSA algorithm HTTPS encryption.

ZoTrus has not only developed a full range of products for the application ecology of commercial cryptography SSL certificates, but also successfully obtained the approval to take the lead in formulating two relevant China commercial cryptography industry standards in December 2023 - "**Certificate Transparency Specification**" and "**Automatic Certificate Management Specification**", which are commercial cryptography standards that are benchmarked and compatible with the two international standards of RFC6962 and RFC8555, and support the use of commercial cryptography to achieve certificate transparency and realize the automatic certificate management. The formulation of these two standards marks a new level of standardization of commercial cryptography products of SM2 SSL certificates, which will provide standard support for the reliable supply and popularization of SM2 SSL certificates, accelerate the popularization and application of SM2 SSL certificates for HTTPS encryption, and accelerate the adoption of commercial cryptography to ensure global Internet security.

4. Looking forward to 2024, ZoTrus will continue to forge ahead and provide more and better SM2 products and solutions

Looking back on 2023, ZoTrus Technology provides a China solution for HTTPS encryption, the core communication security of the global Internet. In 2024, ZoTrus will continue to iterate and improve the full ecosystem of commercial cryptography SSL certificate applications, expand ecological partners, launch the On SM2 HTTPS Plan, continue to contribute to the popularization of commercial cryptography applications, and continue to provide more innovative cryptographic application products for global users.

While improving the ecological products of commercial cryptography HTTPS encryption application, ZoTrus Technology will develop and provide SM2 document security products and services, SM2 email security products and services, SM2 code security products and services, and SM2 trusted identity products and services, and continuously improves the application of various digital certificates in the commercial cryptography system, providing global users with another choice and another reliable option, and promoting and popularizing commercial cryptography to ensure the security and trust of the global Internet and the Internet of Everything.

Richard Wang

December 29, 2023
In Shenzhen, China