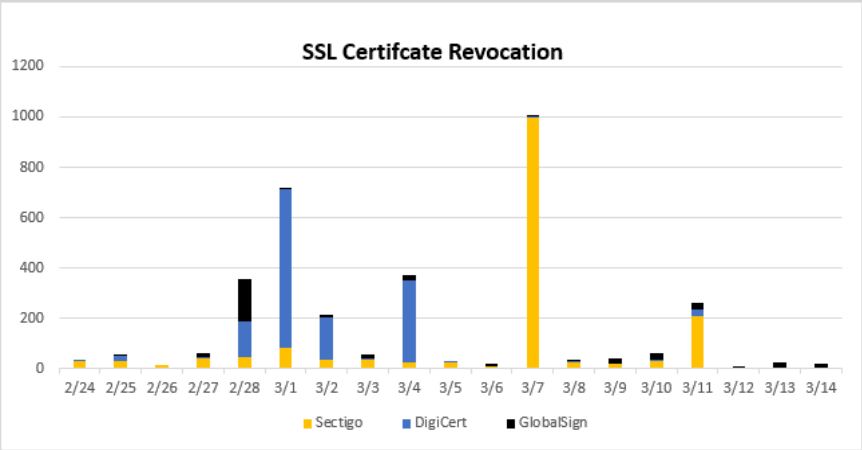
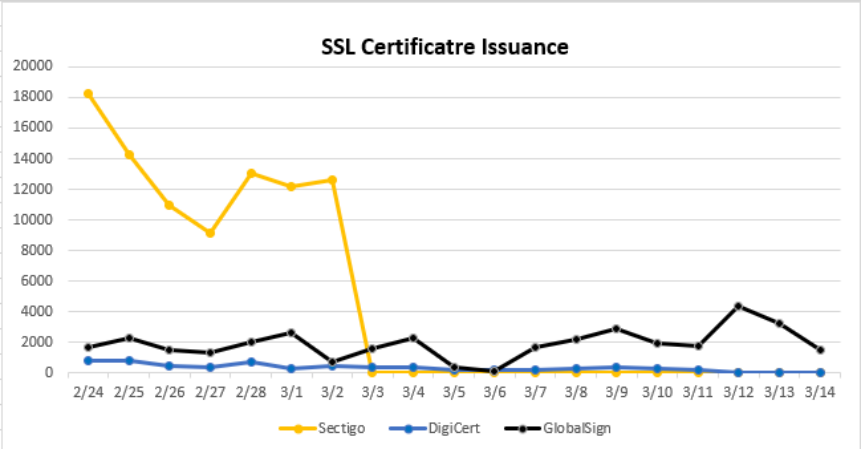
Is China ready for the SSL certificate “Broken Supply”?

On February 24 this year, the conflict between Russia and Ukraine occurred, and many RSA algorithm SSL certificates of Russian government websites and bank websites were revoked and not issued. Sectigo stopped issuing certificates on March 3rd, DigiCert stopped issuing certificates on March 12th, and other CAs also stopped issuing certificates. Stopping certificate issuance is a "broken supply", that means, the website cannot implement https encryption! And starting from February 27th, Sectigo began to revoke the issued SSL certificates, and a total of 1576 certificates were revoked within 13 days. DigiCert started from February 28th, and a total of 1266 certificates were revoked. To revoke a certificate is to disable it! The certificate that has been issued to you is forbidden to use! Supply broken means no longer supplying, and revocation means that even if the good is delivered, it is still not allowed to be used!





(C) 2022 **ZoTrus Technology Limited**

The picture below is a page of the author's speech at the 7th China Internet Security Conference on August 20, 2019. At that time, the author put forward the point of view that China must be prepared for the "broken supply" of SSL certificates - Is China ready for RSA SSL certificate “Broken Supply”? Does China have a “Spare Tire”?. At that time someone said it couldn't happen, but now it's actually happening in Russia! This must be worthy of our thought and vigilance!

The security implications of the Russian-Ukrainian conflict to China are in all aspects. In terms of Internet security, especially website security, the RSA algorithm SSL certificate has been revoked or broken supply, which has sounded the alarm for China Internet security, especially the security of critical information infrastructure. China must quickly enter the era of SM2 HTTPS encryption, to cope with the very uncertain international situation and ensure China Internet security.

The popularization of the SM2 HTTPS encryption is not only the need to deal with the current uncertain international situation, but also the needs of the compliance of Cryptography Law and Cyber Security Law. Maybe some readers think that the current websites security SM2 ecology is not mature and cannot meet the popularity of popularization that cannot meet the technical requirements of SM2 HTTPS encryption, this article specifically talks about this wrong understanding.

To implement HTTPS encryption, there must be a CA issuing SSL certificate, and the certificate is logged in certificate transparency system. There must be a browser to trust the root CA certificate for issuing SSL certificate, the web server supports the cryptographic algorithm used by the SSL certificate,

(C) 2022 **ZoTrus Technology Limited**

and the browser must support the of the cryptographic algorithm for using HTTPS encryption protocol to achieve a secure webpage access. In other words, only browsers (including mobile Apps), SSL certificates, and web servers support SM2 algorithms to achieve SM2 HTTPS encryption. And CDN and WAF also need to support SM2 algorithm, together with other elements to establish a SM2 certificate application ecosystem. The author clearly tells everyone that this ecology is mature now, and it is time to popularize the SM2 HTTPS encryption!

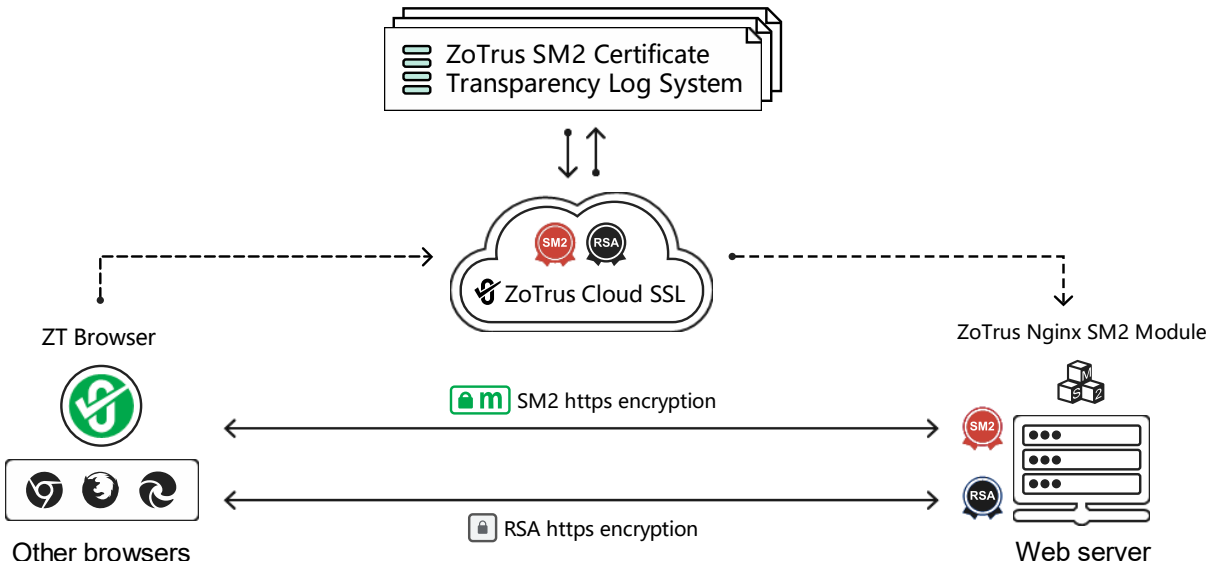
Please look at the list of ecological product manufacturers who support the SM2 SSL certificate and the SM2 algorithm listed. It should be able to believe that my point of view is correct.

1. CA operators who can issue SM2 SSL certificates: CerSign, ZoTrus, GDCA, TrustAsia, Shanghai CA, CFCA, iTrus, WoTrus, Shaanxi CA, NetCA, Gizhou CA, Sichuan CA etc.
2. Browsers that support SM2 algorithm and SM2 SSL certificate: ZT Browser, MeSign Browser, Qi anxin Browser, 360 Browser, Redlotus Browser, etc. It is recommended to use the completely free ZT Browser.
3. Web servers supporting SM2 Algorithm and SM2 SL Certificate: Nginx + SM2 module. If the web server is not using Nginx, it can be set the Nginx as on-premises proxy for SM2 https encryption. ZoTrus provides a free SM2 Module for Nginx with on click re-compiled.
4. The certificate transparency log system that supports SM2 algorithm and SM2 SSL certificate: ZoTrus SM2 Certificate Transparency log system. This log system is trusted and included in ZT Browser to verify whether the SM2 SSL certificate has been transparent.
5. CDN and WAF services that support SM2 algorithm and SM2 SSL certificate: Alibaba Cloud, Wangsu.
6. Mobile App SM2 algorithm Module: CFCA
7. There are many other products and manufacturers that support the SM2 algorithm, so I won't list them one by one . . . . . .

For https encryption, considering the best user experience, the website cannot require users to designate the use of the SM2 supported browser. Therefore, the best solution is to deploy the dual SSL certificate (one SM2 SSL certificate and one RSA/ECC SSL certificate). All SM2 supported browsers must support the adaptive encryption of dual certificates, ZT Browser is preferred to use SM2 algorithm to implement HTTPS encryption, only when the website does not deploy SM2 SSL certificate, the RSA

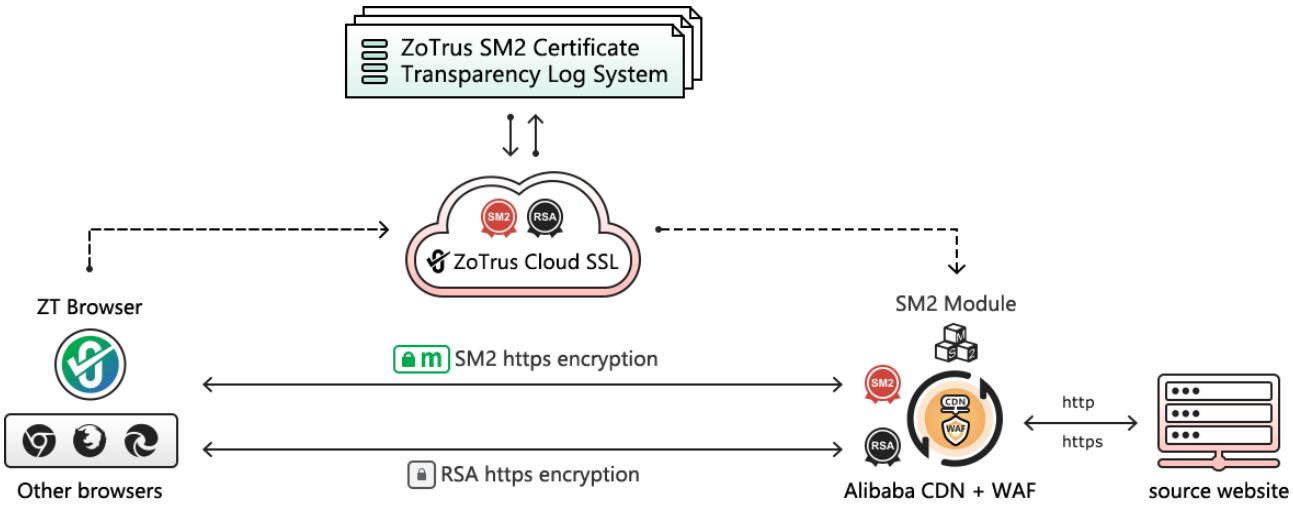
(C) 2022 **ZoTrus Technology Limited**

algorithm is used to implement HTTPS encryption. To allow everyone to experience the effect of the dual SSL certificate deployment, we deployed the test website: https://sm2test.cersign.cn, please use ZT Browser and other browsers to visit this SM2 HTTPS encryption test website, you will see that the ZT Browser preferentially use SM2 algorithm for https encryption, and the SM2 encryption icon **m** is displayed in the address bar. Users can also download the completely free Nginx SM2 algorithm supported module on this website, just re-compile Nginx to support SM2 SSL certificate and SM2 algorithm. And users can also apply for a completely free 90-day period of free SM2 SSL certificate to experience the mystery of dual certificates deployment!

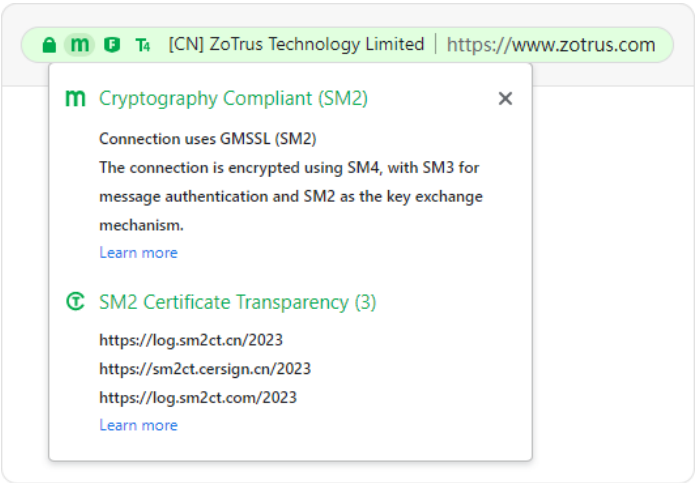


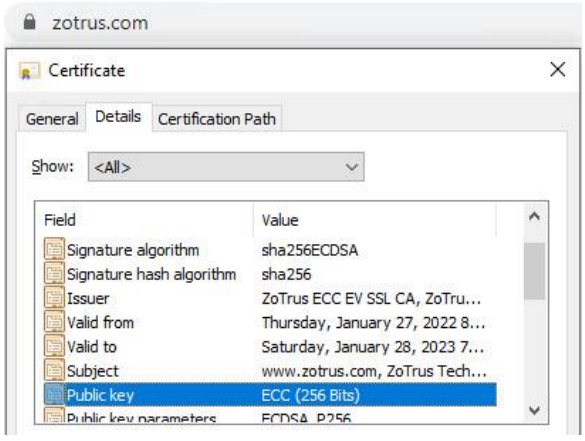
In view of the wide range and difficulty involved in the cryptography reconstruction, ZoTrus Technology released a zero-reconstruction, SM2 https encrypted cloud service-ZoTrus Website Security Cloud Service, there is no need to apply for the SM2 SSL certificate and the RSA/ECC SSL certificate from the CA, and no need to install the SSL certificates on the server, only need to do 3 domain name resolutions that change the origin website as source website for CDN and WAF to realize SM2 HTTPS encryption within 10 minutes, and the CDN+WAF service provides the industry's leading Alibaba Cloud. ZoTrus Technology used the API provided by Alibaba Cloud CDN to fully auto-configure SM2 SSL certificate and ECC SSL certificate to Alibaba Cloud CDN + WAF, to realize cryptography compliance and global trust of HTTPS encryption, quickly realize the website cloud WAF protection, and quickly realize high-speed content distribution.

(C) 2022 **ZoTrus Technology Limited**



Please use ZT Browser and other browsers to visit the ZoTrus official website: https://www.zotrus.com, this website is a real case using ZoTrus Website Security Cloud Service to realize SM2 HTTPS encryption. You will see that ZT Browser prefer to use SM2 algorithm priority for https encryption and displays the SM2 encryption icon **m** in the address bar and displays the cloud WAF icon **F** in the address bar indicating that this website has enabled cloud WAF protection, as shown in the left figure below. If you use other browsers that do not support SM2 algorithm and SM2 Certificate Transparency, the ECC algorithm will be used to implement https encryption, as shown in the right figure below.





The author believes that everyone can see from the above SM2 ecological manufacturers list and ZoTrus Technology HTTPS encryption solutions that China has been prepared in SM2 HTTPS encryption technology and products! Everything is ready, just for you are going to act immediately. You must act immediately to ensure that all websites are secure and controllable in HTTPS encryption in the current uncertain international environment, especially for government websites and financial

(C) 2022 **ZoTrus Technology Limited**

websites, to ensure that even the RSA/ECC SSL certificate is revoked or “broken supply”, it will not affect the end user's normal access to the website.

Finally, please take a look at two real deployment cases of SM2 https encryption, one is the official website of the provincial government and the other is the online banking system of the Bank of China.

Richard Wang

Nov. 4, 2022
In Shenzhen, China

(C) 2022 **ZoTrus Technology Limited**