

Zero reconstruction for SM2 https encryption

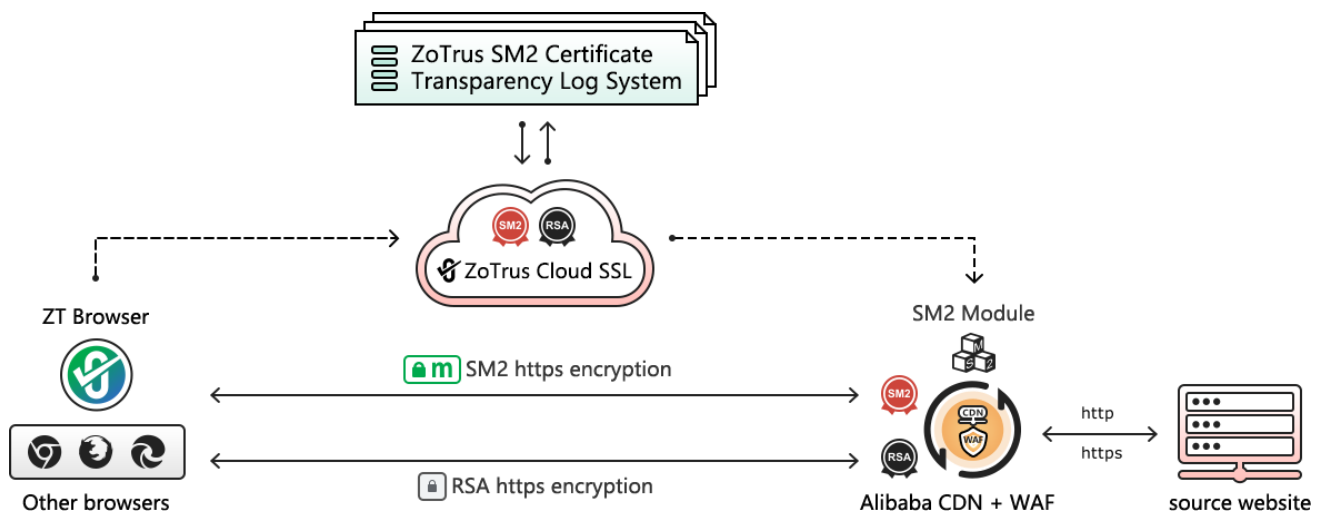
"Commercial Cryptography Reconstruction" is a hot word now, "Commercial Cryptography" refers to China standard algorithm, and "reconstruction" refers to updating the current information system's cryptography technology, products, and services, to meet the requirements of the "Cryptography Law", GB/T 39786-2021 "Information Security Technology - Baseline Requirements for the Cryptography Application of Information System" and related laws, policies, standards and other compliance requirements, to achieve cryptography autonomy.

Document No. 36 of 2018 jointly issued by the Office of the Central Government and the Office of the State Council, "Work Plan for Cryptographic Application and Innovation Development in Financial and Important Fields (2018-2022)", requires that financial and important fields (including e-government website systems) be completed by the end of 2022 implement and complete the reconstruction of China cryptography applications. The document issued by the People's Bank of China in 2021 further requires the financial sector to use China cryptography to account for 100% of transactions by the end of 2022. There are only two months until the end of the year. Although various "Cryptography Reconstruction" work is in full swing, it is easier said than done to reconstruct a cryptography application ecosystem. ZoTrus Technology produces a solution that does not require any reconstruction of the website to realize SM2 HTTPS encryption, which will greatly accelerate the popularization and application of SM2 HTTPS encryption, meet the compliance requirements of financial websites, e-government websites, and other important fields, and greatly reduce the burden of the compliance pressure and compliance costs of financial institutions and government agencies.

To realize SM2 HTTPS encryption, the browser must support the SM2 algorithm and the SM2 SSL certificate, and the web server supports the SM2 algorithm and the SM2 SSL certificate. The CDN network system for big traffic websites also need to support SM2 algorithms and SM2 SSL certificates. The entire system is an ecological reconstruction that transforms the international cryptography system

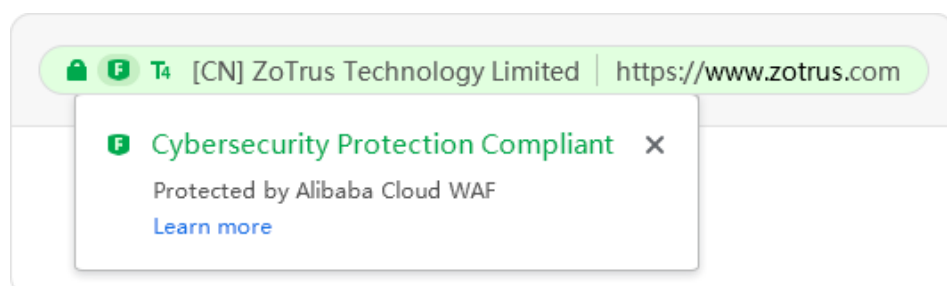
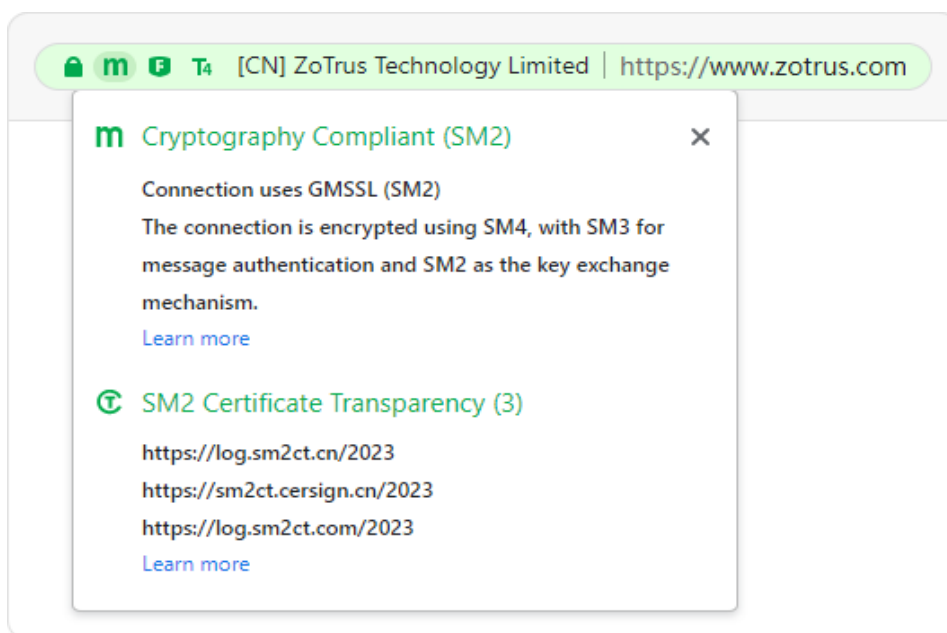
into a China cryptography system, which is a big project. Now there are some browsers that support the SM2 algorithm and the SM2 SSL certificate, including the completely free ZT Browser, and there are already many CA operators that can issue the SM2 SSL certificate. However, the reconstruction of Web services is not so easy, because there is various Web server software, such as Microsoft's IIS, IBM's WebSphere, Oracle's WebLogic, as well as Apache, Tomcat and Nginx, etc. Most of this Web server software are from big manufacturers' proprietary software, there is no interface for reconstruction at all! Only the open-source Nginx is convenient to reconstruct to support the SM2 algorithm and the SM2 SSL certificate. ZoTrus Technology has completed the SM2 algorithm support reconstruction of Nginx, and it is completely free for all users to download and use.

So, how can we achieve zero reconstruction of SM2 HTTPS encryption? How to achieve it without reconstruction? ZoTrus Website Security Cloud Service has done it! It is a zero-reconstruction implementation of zero-application SSL certificate, zero-installation SSL certificate, zero-reconstruction server software, and zero-installation of any software! Customers only need to do 3 domain name resolutions to achieve SM2 HTTPS encryption with zero reconstruction, which meets the cryptography compliance requirements of the website, supports all non-SM2 support browsers, and achieves cryptography compliance and global trust at the same time without the limitation of using browser. This is a innovative website security cloud service based on Alibaba Cloud CDN+WAF service, which integrates SM2 HTTPS encryption, cloud WAF protection, CDN distribution, and website trusted identity validation, allowing customers to easily achieve cryptography compliance and website security autonomy and self-control.



It is worth mentioning that this is the only solution in China that adopts the SM2 SSL certificate that supports the SM2 Certificate Transparency to automatically realize the SM2 HTTPS encryption solution, because financial websites and government websites are important critical information infrastructures, and their SM2 SSL certificates used must support the SM2 Certificate Transparency, otherwise it is very likely that websites in these important fields will be easily attacked, illegally counterfeited and illegal information theft due to the lack of supervision and the mistakenly or maliciously issuance of the SM2 SSL certificate.

As you can see from the above brief introduction, users do not need to reconstruction the web server or the existing website system. They only need to set the existing website that does not support SM2 algorithm as the source site, which can be either http or https website. The only thing that needs to be "changed" is that the user needs to use a browser that supports the SM2 algorithm. It is recommended to use a completely free ZT Browser. The SM2 algorithm is given priority and the SM2 encryption (**m**) is displayed directly in the address bar, so that the SM2 encryption is at a glance.



ZoTrus Website Security Cloud Service not only realizes the SM2 https encryption with zero reconstruction, but also realizes cloud WAF protection, which effectively protects the security of the website; and at the same time realizes the distribution of CDN content, which will greatly improve the user experience of visiting the website. ZoTrus Website Security Cloud Service realizes cryptography protection compliance and cybersecurity protection compliance with one click, welcome to purchase and enjoy it.

Richard Wang

Nov. 4, 2022

In Shenzhen, China