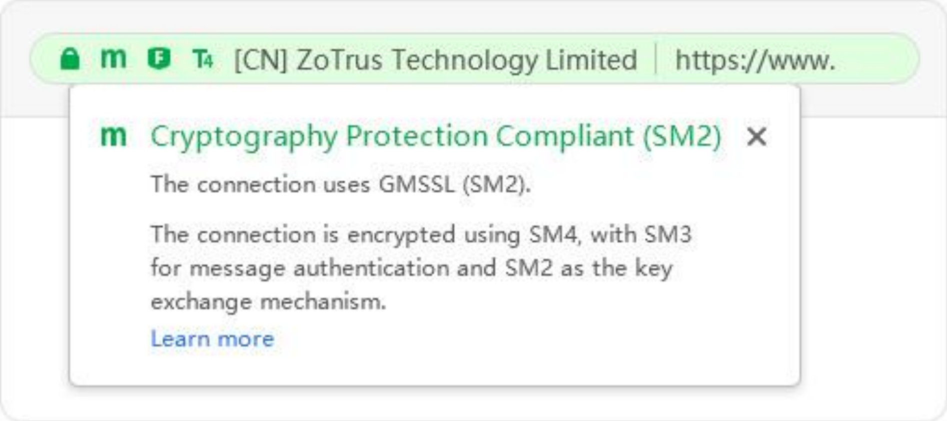
ZT Browser is a Free SM2 Algorithm Supported Browser

Website doesn't deploy an SSL certificate and all browsers will show it as "Not secure", which is zero trust for http plaintext transmission. If the website deploys the China algorithm SM2 SSL certificate, foreign browsers do not support it, and it will prompt: Unsupported protocol. The client and server don't support a common SSL protocol version or cipher suite. Although the SM2/SM3/SM4 algorithms have become ISO/IEC international standards in 2018 and 2021, there is still a long way to go before they become a CA-related international standard followed by global CAs and supported by all browsers. The good news is that Chinese browsers have already taken action. There are several brands of browsers that support SM2 SSL certificates, meeting the requirements of Chinese government users for compliance with the "China Cryptography Law".

However, the author believes that, at present, the Chinese browser's SM2 algorithm and the SM2 SSL certificate support still have many places that are not in place, I will not comment here. The support of the SM2 algorithm and the SM2 SSL certificate is the first product of ZoTrus Technology - the first highlight of the ZT Browser. Not only support SM2 SSL certificate and follow the cryptographic standard specifications such as "GM/T 0024 SSLVPN Technical Specification" and "GB/T38636-2020 Information Security Technology Transport Layer Cryptographic Protocol (TLCP)", but also have innovation in browser’s UI, the website that deployed SM2 SSL certificate, as shown in the figure below, adds an m icon at the address bar near the security padlock to highlight that this website has deployed the SM2 SSL certificate to realize the encryption of using SM2 algorithm.



Cryptography Protection Compliant (SM2)

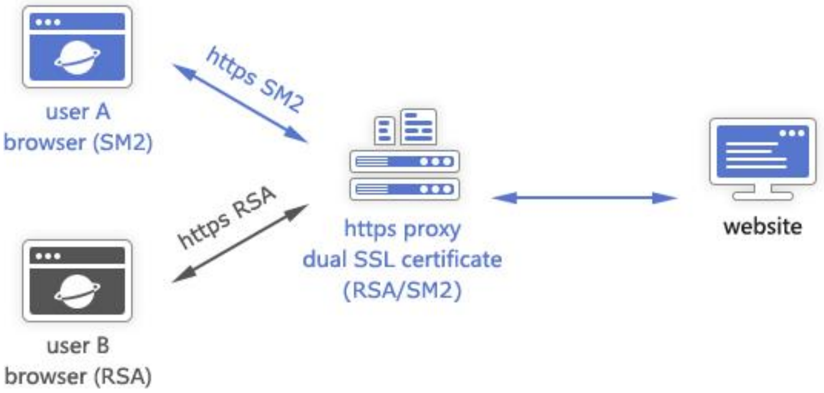
The connection uses GMSSL (SM2).

The connection is encrypted using SM4, with SM3 for message authentication and SM2 as the key exchange mechanism.

Learn more

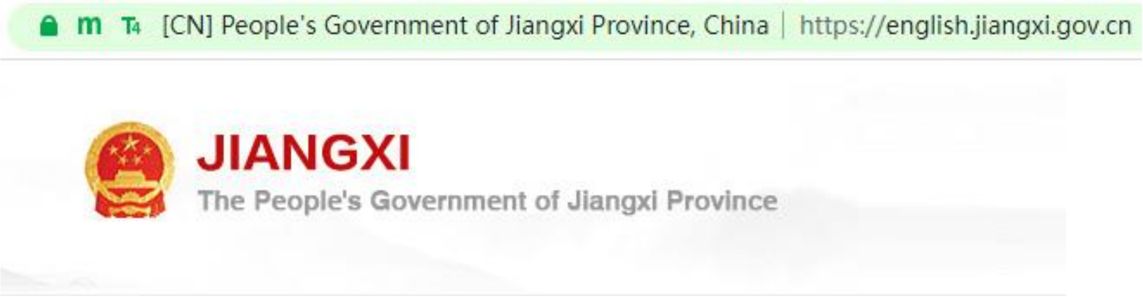
An m icon allows all users to know at a glance whether the website is protected by SM2 algorithm when using the ZT Browser to access a government website. This is easy for anyone to check whether this website is compliant with China Cryptographic Law. Not only that, ZT Browser preferentially uses the SM2 algorithm to communicate with the website. If the website deploys the SM2 SSL certificate, the SM2 algorithm is preferentially used for key exchange, the SM3 algorithm is used for message authentication and the SM4 algorithm is used for encryption. If the SM2 SSL certificate is not deployed, the ECC algorithm is preferred, because the ECC algorithm is faster than the RSA algorithm and can give users a better experience. If the website does not have any SSL certificates deployed, the browser will display the website as "Not secure".

ZT Browser is developed based on the open-source project Chromium 97. The browsing function is already very advanced, and no changes are required. The first function we added is to support the SM2 algorithm and the SM2 SSL certificate, and it is designed to use the SM2 algorithm first if the website deploys dual SSL certificates. Speaking of dual SSL certificates, this is also something the author is very proud of. This is what the author proposed for the first time in his speech at the "Network Trusted Summit" in 2018, see below figure. Now, the dual-certificate auto-adaptation mechanism has become the standard for all websites that deployed the SM2 SSL certificate. When you visit a government website, you may see that the RSA SSL certificate is deployed. In fact, the browser you are using does not support the SM2 algorithm, so the SM2 SSL certificate is not used to achieve https encryption. It is recommended that you use the ZT Browser to visit and try to see if you can see an m icon in the address bar.



ZT Browser has included and trusted China SM2 Root CA certificate and some SM2 root certificates. All CAs that have SM2 root certificates and can issue SM2 SSL certificates are welcome to contact us to include your SM2 root certificates to jointly create a complete closed-loop for SM2 algorithm https encryption application ecosystem, and to make the SM2 algorithm and the SM2 SSL certificate play a greater role to ensure the security of China e-government system and the security of global Internet.

Finally, I recommend 5 websites that have deployed the SM2 SSL certificate. You can download ZT Browser to experience what the SM2 encryption is like: The first website is the official website of the Jiangxi Provincial Government website: https://www.jiangxi.gov.cn, the second website is the Anhui Provincial Government website: https://www.ah.gov.cn, the third website is the Shanghai Cryptographic Administration Bureau website: https://mgj.sh.gov.cn, the fourth website is the official website of Credit China (Jiangxi): https://www.creditjx.gov.cn. These four websites are all deploying SM2/RSA dual-SSL certificate for adaptive encryption, using ZT Browser to visit will use the SM2 algorithm encryption preferentially, but using other browsers don’t have this effect. The fifth website is the online banking service of Bank of China: https://ebssec.boc.cn, which is a website that only deploys the SM2 SSL certificate. If you are using a browser that don’t supports SM2 algorithm, the browser will prompt "Accidentally terminated the connection", don't think this is a problem with the website, it is because the browser you are using does not support SM2 algorithm. Please use the ZT Browser to visit, it will be able to be accessed, and ZT Browser will display an m icon in the address bar and prominently indicates that this website is encrypted with the SM2 algorithm.


m T4 [CN] People's Government of Jiangxi Province, China | https://english.jiangxi.gov.cn
JIANGXI
The People's Government of Jiangxi Province

Richard Wang

June 1, 2022
In Shenzhen, China