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, there are still many issues in supporting the SM2 algorithm for SM2 browsers. The first and biggest problem is that the browsers on the market that support SM2 algorithm have all become paid products, which is very detrimental to the popularization and application of SM2 SSL certificates in China. In order to popularize the application of the SM2 SSL certificate, there must be a completely free SM2 algorithm supported browser, because the common sense of Internet users is that the browser should be free, just like the four major browsers in the world are completely free.

Compared with other SM2 browsers, ZT Browser has the following four highlights:

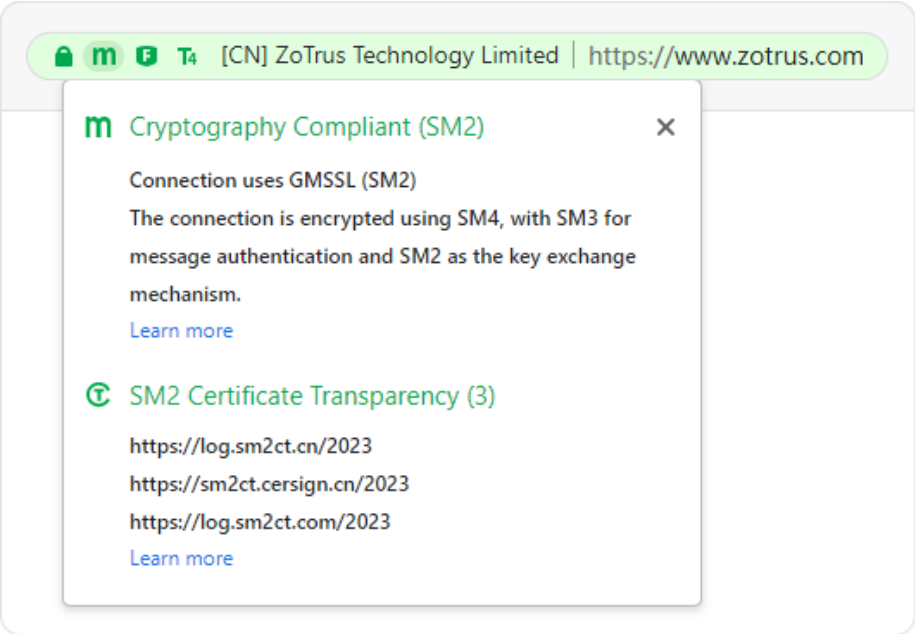
Highlight 1: Completely free, no ads!

ZT Browser is a permanent and completely free SM2 browser that supports SM2 algorithms and SM2 SSL certificates. Of course, it is also a general-purpose browser based on Google Chromium kernel with the same performance and functions as Google Chrome. The only difference is that it supports SM2 algorithm and international algorithm to realize https encryption. ZT Browser is not only a completely free SM2 browser, but also a very clean browser without any third-party advertisements.

(C) 2022 **ZoTrus Technology Limited**

Highlight 2: SM2 encryption is visible!

ZT Browser not only supports SM2 SSL certificates to implement https encryption, but also directly adds an "m" icon behind the padlock mark in the address bar, clearly telling site visitors that this website uses SM2 algorithms to realize https encryption. Click the "m" SM2 encryption icon to view the details, and clearly tell users that this website is "Cryptography Protection Compliant (SM2)". An "m" icon allows all users to know at a glance whether the website is protected by SM2 algorithm when using ZT Browser to access the website, this is easy for anyone to check whether this website is compliant with China Cryptographic Law.



Highlight 3: The world's exclusive support for the SM2 certificate transparency!

ZT Browser not only supports SM2 algorithm, but also exclusively supports SM2 certificate transparency in the world, and it verifies in real time whether the SM2 SSL certificate is embedded with the SCT list field. If there is SCT data signed by the SM2 certificate transparency log trusted by ZT Browser, it will display "SM2 Certificate Transparency" and the certificate transparency log information; if not, it will display " SM2 Certificate NOT Transparency".

Whether an SSL certificate is safe and trustworthy depends on two factors. One is whether the browser trusts the root CA certificate that issued the certificate, and the other is whether the certificate has been logged in certificate transparency log. If any of these factors is missing, Google Chrome will prompt "Not secure". Since 2013, there have been more than 7 billion international

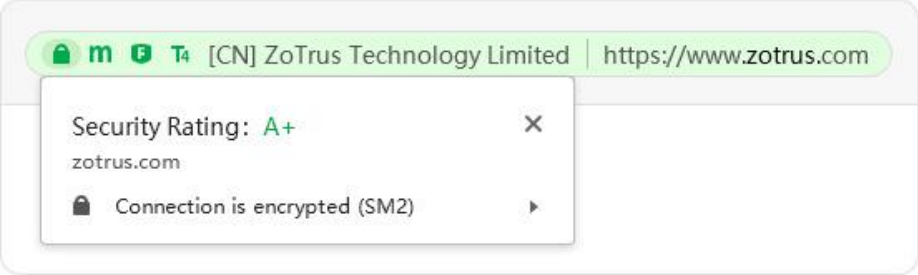
(C) 2022 **ZoTrus Technology Limited**

algorithm SSL certificates in the world that support certificate transparency. ZT Browser not only supports international certificate transparency, but also supports SM2 certificate transparency, ensuring the security and trustworthy of SM2 SSL certificates.

Highlight 4: Prioritize the use of SM2 algorithms!

ZT Browser preferentially use the SM2 algorithm to shake hands with the web server. If the website deploys the SM2 SSL certificate and supports the SM2 algorithm, it will first use the SM2 algorithm for key exchange, use the SM3 algorithm for message authentication, and use the SM4 algorithm for encryption. ZT Browser modifies from the core code to add the SM2 algorithm to the cipher suite together with the RSA/ECC algorithm, instead of the "two skins" of the SM2 algorithm and the international algorithm like some other SM2 browsers which need to be set in a certain menu.

It should be the default function of the SM2 browser to use the SM2 algorithm first to implement https encryption. Only in this way can the SM2 SSL certificate deployed on the web server truly play an encryption role. Otherwise, the international SSL certificate deployed on the server will still be used, and there is no real use the SM2 algorithm to ensure the security of the website.



ZT Browser has included and trusted China SM2 Root CA certificate, SM2 root CA certificates from a dozen CAs, all CerSign and ZoTrus SM2 Roots. 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 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 Internet in China.

Finally, I recommend 3 websites that have deployed the SM2 SSL certificate. You can download the ZT Browser to experience what the SM2 encryption is like: The first website is

(C) 2022 **ZoTrus Technology Limited**

the official website of the Hunan Provincial Government website: https://www.hunan.gov.cn, the second website is the official website of Credit China (Jiangxi): https://www.creditjx.gov.cn. These two 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 third 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.

Richard Wang

Sept. 30, 2022
In Shenzhen, China

(C) 2022 **ZoTrus Technology Limited**