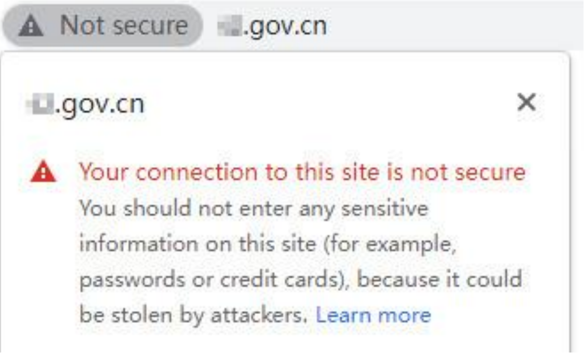
Website security needs to be "Visible"

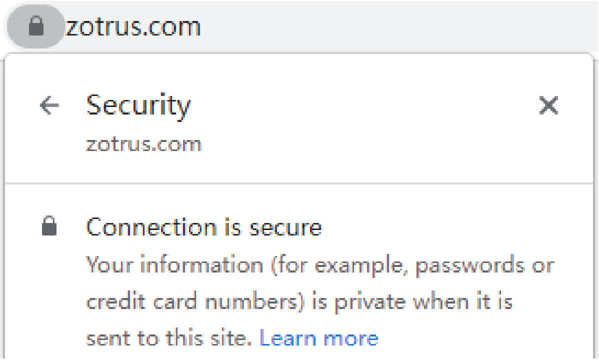
Today is Programmer Day. As an old programmer, the author writes this article to reveal the masterpiece of new programmers - ZT Browser, which is the first in the world to support the SM2 Certificate Transparency, and the first SM2 browser to make the website security be "visible". I also take this article to wish all new and old programmers a happy programmer day.

Whether a website is secure is generally invisible. To make it visible to site visitors, all browsers display "**Not secure**" for http websites, which is to let site visitors see that this website is not secure. HTTP protocol is a cleartext transmission protocol, various confidential information is transmitted in cleartext from the browser to the server, which is very easy to be illegally stolen and illegally tampered with. Therefore, all browsers directly display "Not secure" in the address bar to let it "visible" for all site visitors! As shown in the left image below, Google Chrome displays "Not secure". Similarly, if the browser uses https to access the website, the padlock is displayed, which is also to let it "visible" for all site visitors to see the "Connection is secure". The right picture below shows the padlock and "Security" displayed by Google Chrome.



Your connection to this site is not secure

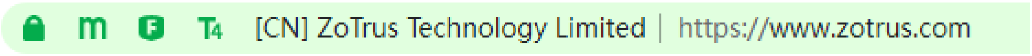
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more



Connection is secure

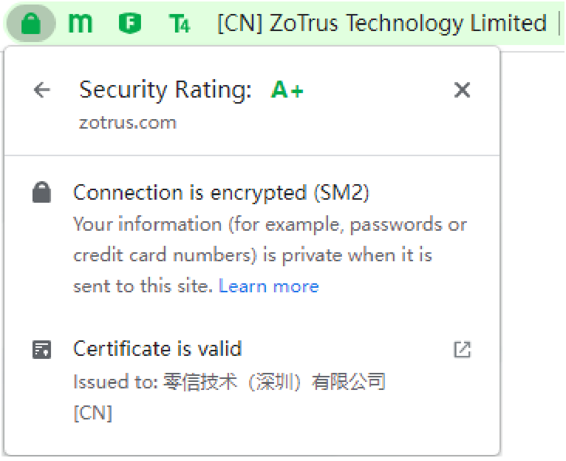
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

In the author's opinion, just two "**visible**" designs are not enough. Therefore, in addition to displaying "Not secure" for http websites and displaying padlock for https websites, ZT Browser also adds 5 very distinctive "visible" security features, which can really help site visitors see that the website is secure or not that they are visiting. As shown below.



The first "visible" security is the padlock icon.

Different from the padlock of other browsers, clicking on the padlock will display the website security rating in real time, clearly telling site visitors how secure this website is. It is divided into six security levels A, B, C, D, E, F, and the security level is scored from six dimensions, including SSL certificate, protocol support, key exchange, cipher strength, cloud WAF protection and trusted identity validation. The highest level is A+. And ZT Browser changed the "connection is secure" to "connection is encrypted (SM2)", because the deployment of an SSL certificate can only indicate that the connection from the browser to the server is encrypted, it does not equal security! The brackets after "connection is encrypted" show the cipher algorithm used for this encrypted connection, such as RSA, ECC, and SM2. SM2 is a China cipher algorithm that ZT Browser preferred.

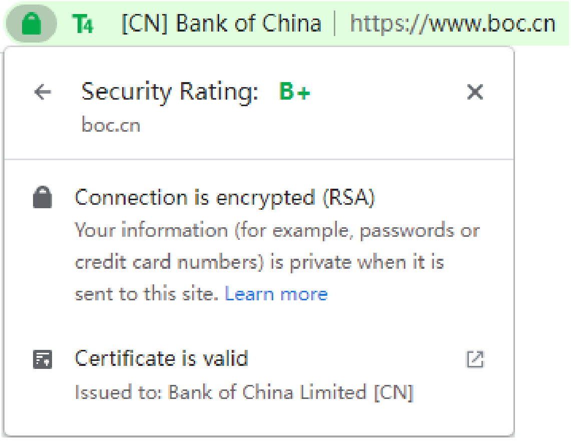


m F T4 [CN] ZoTrus Technology Limited |

Security Rating: A+
zotrus.com

Connection is encrypted (SM2)
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid
Issued to: 零信技术（深圳）有限公司 [CN]



T4 [CN] Bank of China | https://www.boc.cn

Security Rating: B+
boc.cn

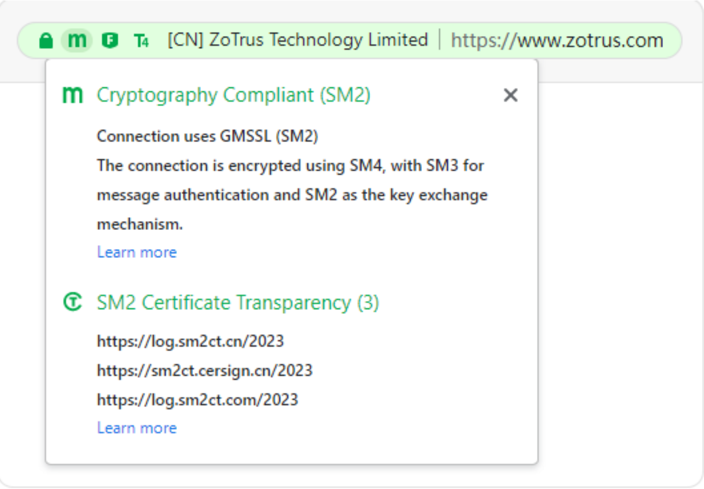
Connection is encrypted (RSA)
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid
Issued to: Bank of China Limited [CN]

The second "visible" security is the SM2 encryption icon(m).

This icon clearly tells website visitors that this website has deployed a SM2 SSL certificate, and the browser uses SM2 algorithm to realize the SM2 https encryption, allowing site visitors to see that this website is cryptography protection compliant. Click on the SM2 encryption icon, not only can you see the website is "Cryptography Protection Compliant (SM2)" and explanation of the role of each cipher algorithm of SM2/SM3/SM4.

And site visitors can also see the SM2 Certificate Transparency icon, which clearly tells the site visitor whether the SM2 SSL certificate used for SM2 https encryption meets the ZT Browser requirements of the SM2 certificate transparency. If the SM2 SSL certificate embedded ZT Browser trusted SCT list, then it will display “SM2 Certificate Transparency”. If the SCT list is not embedded, it will display " SM2 Certificate NOT Transparency ". This "visible" is very important, it can effectively prevent maliciously issued SM2 SSL certificate that used for attacks and frauds, thereby protecting the security of the SM2 SSL certificate. Only the SM2 SSL certificate itself is secure and trusted guarantee, truly guarantee the security and trust of the SM2 https encryption.



[CN] ZoTrus Technology Limited | https://www.zotrus.com

Cryptography Compliant (SM2)

Connection uses GMSSL (SM2)

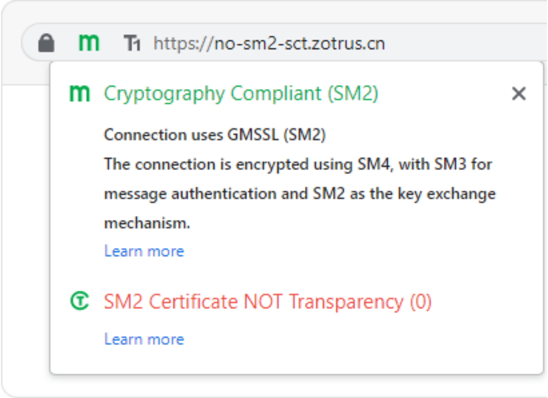
The connection is encrypted using SM4, with SM3 for message authentication and SM2 as the key exchange mechanism.

Learn more

SM2 Certificate Transparency (3)

https://log.sm2ct.cn/2023
https://sm2ct.cersign.cn/2023
https://log.sm2ct.com/2023

Learn more



https://no-sm2-sct.zotrus.cn

Cryptography Compliant (SM2)

Connection uses GMSSL (SM2)

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

Learn more

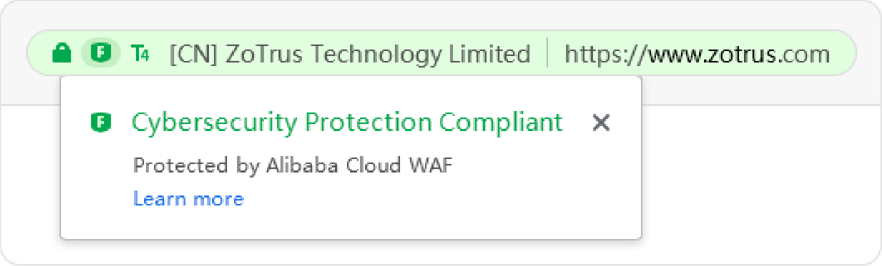
SM2 Certificate NOT Transparency (0)

Learn more

The third "visible" security is the cloud WAF protection icon(F).

This icon clearly tells the website visitor that the website already has cloud WAF protection. This "visible" is very important for website security. Cloud WAF protection will check every web connection whether it is a malicious attack, allow normal connections and block malicious connections to effectively ensure the secure operation of the website. A website with only https encryption without cloud WAF protection is still insecure.

Clicking on the cloud WAF protection icon, website visitor not only clearly know that this website has cloud WAF protection, but also "Cybersecurity Protection Compliance", because cloud WAF protection is one of the requirements in the Cybersecurity Protection Compliance. And it will also show which service provider provides this cloud WAF protection, which can also enhance the confidence of website visitors in website security protection. The cloud WAF service integrated by ZoTrus Website Security Cloud Service is provided by the industry-leading Alibaba Cloud WAF.



T4 [CN] ZoTrus Technology Limited | https://www.zotrus.com

Cybersecurity Protection Compliant ×

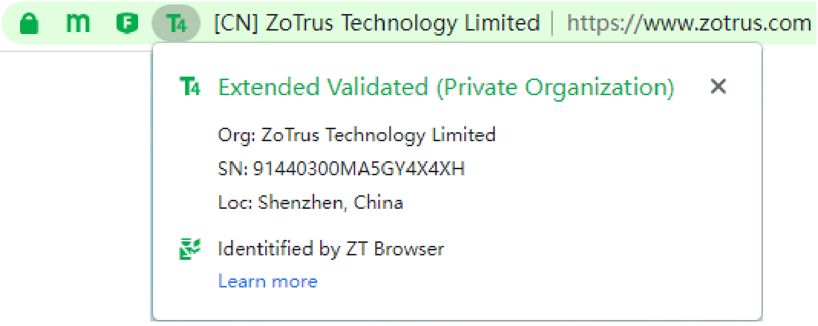
Protected by Alibaba Cloud WAF

Learn more

The fourth "visible" security is the trusted level icon (T4).

This icon clearly tells the website visitor that the website's identity has been validated, and the validation level is T4, the highest trusted level, which is equivalent to the EV SSL certificate’s extended validation in international standards. Clicking on the trusted level icon will display the identity information of the website, including the organization name, registration number, registration place and country. The second icon displays which agency the identity validation is validated. Generally, there are ZT Browser or third-party CA operators, etc.

Website trusted identity is as important as https encryption because a fake bank website is also very likely to deploy a free DV SSL certificate so that the browser will display the padlock icon, which poses a security threat to website visitors, who will mistakenly think that Google Chrome prompts "Security" is really a safe website! This is the main reason why ZT Browser does not show "secure" but instead "encrypted".



m T4 [CN] ZoTrus Technology Limited | https://www.zotrus.com

T4 Extended Validated (Private Organization) ×

Org: ZoTrus Technology Limited

SN: 91440300MA5GY4X4XH

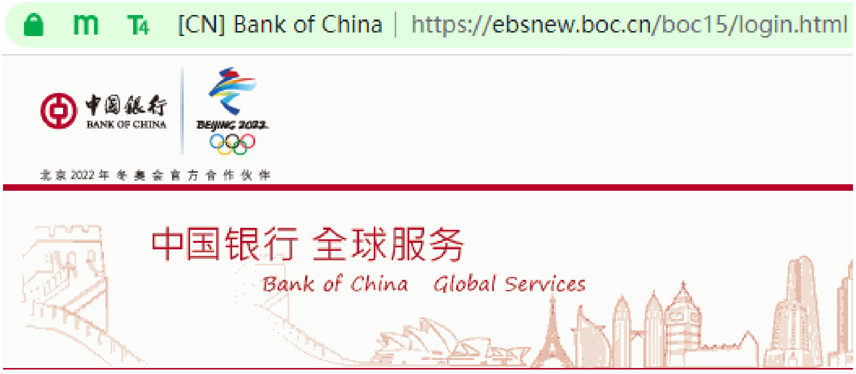
Loc: Shenzhen, China

Identitified by ZT Browser

Learn more

The fifth "visible" security is the green address bar and display organization name and country.

This is very important, clearly and directly tell the site visitor the real identity of this website, regardless of the website page claiming this website's organization name, the address bar displayed organization name is third-party validated. The green address bar is very conspicuous to let website visitors know that the website is a trusted website. In the past, major browsers displayed the green address bar for websites with EV SSL certificates deployed, but unfortunately it disappeared for unknown reasons. ZT Browser brings the green address bar back to the user's sight, which is very useful for preventing websites from being counterfeited. Banks only need to tell its customers that if they can't see the green address bar, it must be a fake bank website, which is very useful and simple and practical. All websites that using ZoTrus Website Security Cloud Service are validated as EV Certification, and a green address bar will be displayed when using ZT Browser to visit.



[CN] Bank of China | https://ebsnew.boc.cn/boc15/login.html

The author believes that readers will be able to fully understand whether a website is secure through the above 5 "**visible**" security, 5 "visible" “Secure” plus 1 "visible” ” Not secure”, a total of 6 "visible" can effectively help website visitors to understand the security status of the website at a glance. These innovations are exclusively provided by ZT Browser globally, which can truly ensure the safety of website visitors. Welcome to download and use ZT Browser for free, stay safe online.

Richard Wang

10.24, 2022
In Shenzhen, China