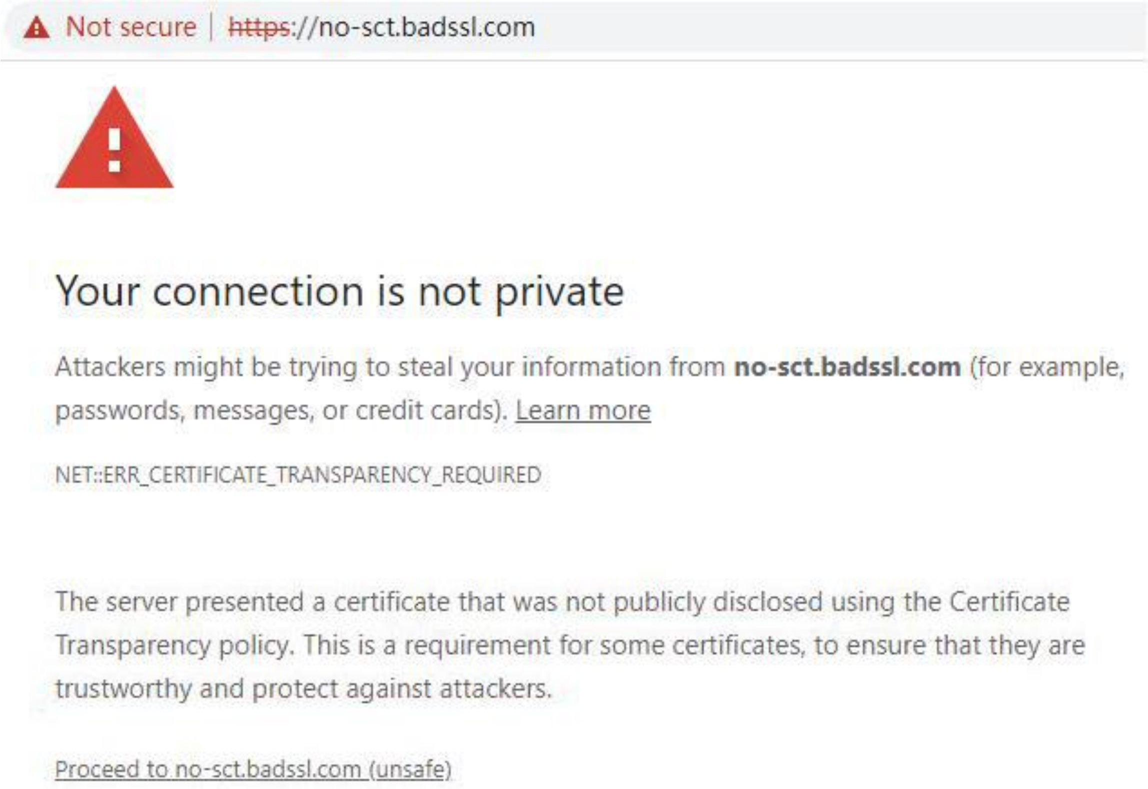
Certificate Transparency is zero trust to SSL certificate issuance

To issue an SSL certificate, user must first verify the domain name control. However, what if the CA system maliciously or mistakenly issues an unverified SSL certificate for a domain name? The certificate transparency mechanism designed by Google is to solve this problem.

Certificate Transparency (CT) is a system for logging and monitoring the issuance of TLS certificates. CT greatly enhances everyone's ability to monitor and study certificate issuance, and these capabilities have led to numerous improvements to the CA ecosystem and Web security. As a result, CT is rapidly becoming critical infrastructure. CT is an Internet security standard for monitoring and auditing digital certificates. The standard creates a system of public logs that seek to eventually record all certificates issued by publicly trusted certificate authorities, allowing efficient identification of mistakenly or maliciously issued certificates. Version 2.0 of the Certificate Transparency mechanism, the latest, is described in the experimental RFC 9162, which obsoletes the earlier version 1.0 described in RFC 6962. At present, all CA operators are still using version 1.0.

If an SSL certificate does not be logged in the CT log system required by the Google Chrome, the Google Chrome will have a security warning. As shown in the figure below, it displays " ERR_CERTIFICATE_TRANSPARENCY_REQUIRED" This is zero trust to the SSL certificate issuance. Never trust every SSL certificate without a certificate transparency. The browser clearly tells the website visitors that this is NOT a trusted SSL certificate.



Not secure | ~~https~~://no-sct.badssl.com

Your connection is not private

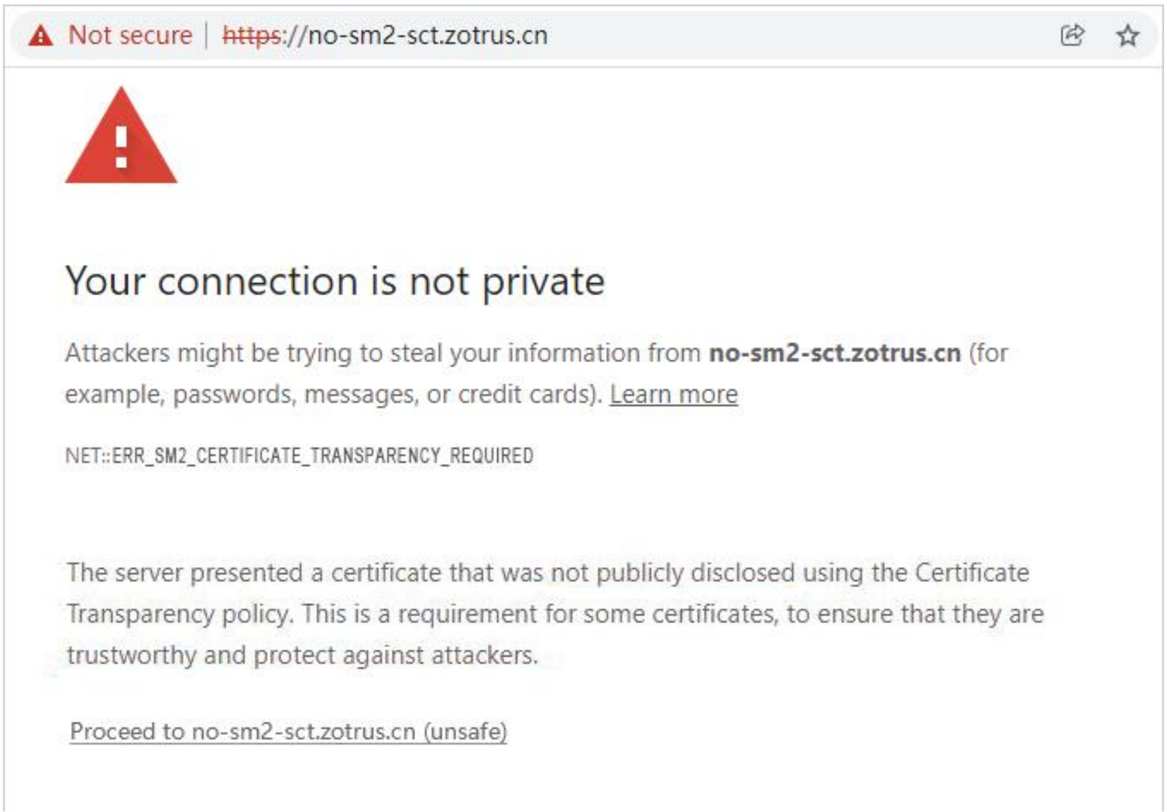
Attackers might be trying to steal your information from **no-sct.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

The server presented a certificate that was not publicly disclosed using the Certificate Transparency policy. This is a requirement for some certificates, to ensure that they are trustworthy and protect against attackers.

Proceed to no-sct.badssl.com (unsafe)

Similarly, to ensure the security and trust of SM2 SSL certificate, the SM2 SSL certificate also requires certificate transparency, but because the current certificate transparency log system does not support the SM2 algorithm, so China must have the certificate transparency log system that that support the SM2 algorithm. ZoTrus Technology has invested in research and development, which lasted for one year. Today, the world's first SM2 certificate transparency log system was launched, this system used SM2 algorithm to digitally sign the CT data with reference to the RFC 9162 standard. ZoTrus Certificate Transparency Log System is included and trusted by ZT Browser. The original plan was that if a SM2 SSL certificate did not include SCT data that required by ZT Browser, ZT Browser would be like a Google Chrome to have the same security warning. As shown in the figure below, it will prompt " ERR_SM2_CERTIFICATE_TRANSPARENCY_REQUIRED", this is the zero trust to the issuance of SM2 SSL certificate. Never trust every SM2 SSL certificate without a SM2 certificate transparency. The browser clearly tells the website visitors that this is NOT a trusted SM2 SSL certificate.



Your connection is not private

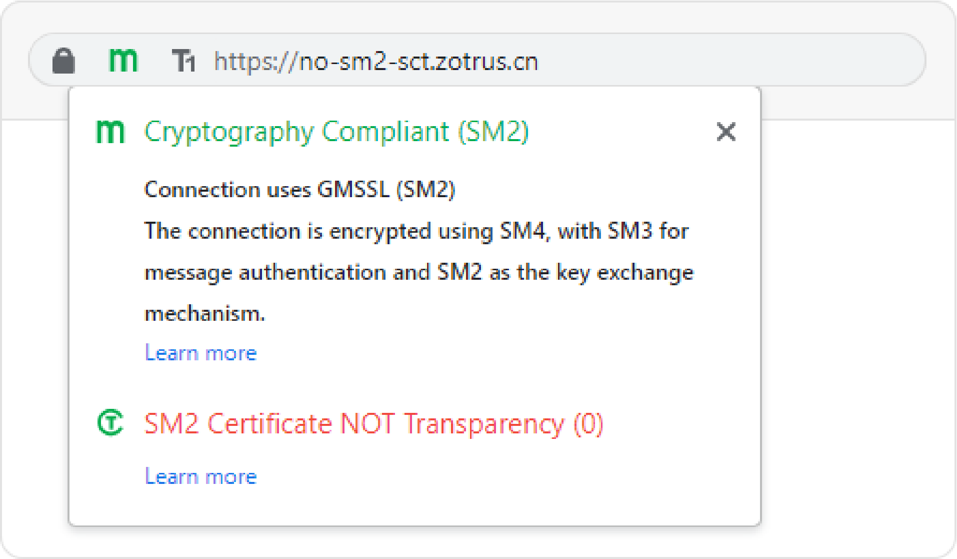
Attackers might be trying to steal your information from **no-sm2-sct.zotrus.cn** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_SM2_CERTIFICATE_TRANSPARENCY_REQUIRED

The server presented a certificate that was not publicly disclosed using the Certificate Transparency policy. This is a requirement for some certificates, to ensure that they are trustworthy and protect against attackers.

Proceed to no-sm2-sct.zotrus.cn (unsafe)

However, considering that the CA operators that issue SM2 SSL certificate need time to upgrade the certificate issuance system to embed the SCT data in the SM2 SSL certificate for every issued SM2 SSL certificate, ZT Browser decides that the mandatory requirement of each SM2 SSL certificate must have SCT data from July 1, 2023. Before that, it only displayed "SM2 Certificate NOT Transparency" in SM2 encryption icon. This is for reminding site visitors to pay attention and choose to deploy the SM2 SSL certificate that supports certificate transparency to protect the online security and interests of their website security.



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 certificate transparency log system has successfully protected the security and trust of the RSA/ECC SSL certificate about 7.4 billion in the world. This is the total data from 2013 to now 10 years. Today, the ZoTrus certificate transparency log system and ZT Browser's CT support for SM2 SSL certificate will also make contributions to the security of the SM2 SSL certificate. Welcome the relevant parties of the SM2 SSL certificate actively joined the SM2 Certificate Transparency Ecology, only every SM2 SSL certificate is transparent can it truly protect the security and trust of the SM2 HTTPS encryption to protect China Internet security.

Richard Wang

Sept. 30, 2022
In Shenzhen, China