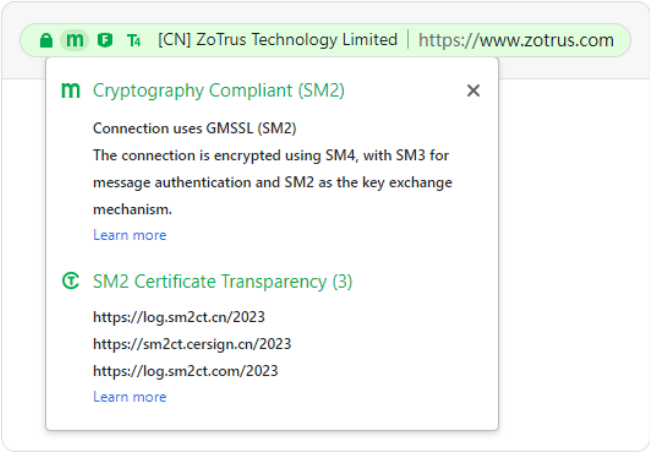
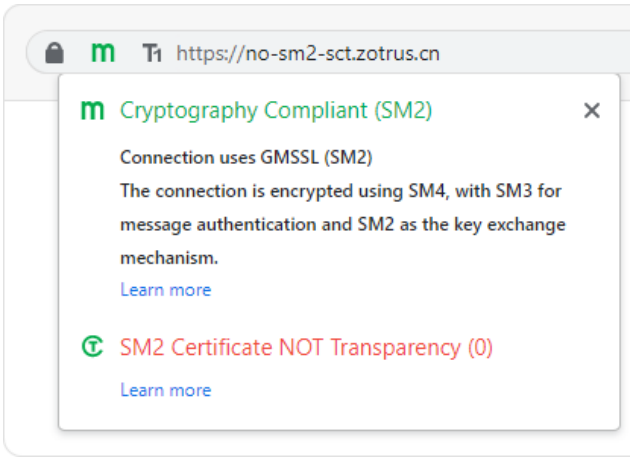
ZT Browser Makes Certificate Transparency more Transparent

Certificate Transparency is an important technology to ensure the security of SSL certificate itself. It can effectively detect mistaken issued or maliciously issued SSL certificates in a timely manner. As of today, certificate transparency has successfully provided certificate transparency for more than 10.1 billion SSL certificates around the world.

But who is providing Certificate Transparency service for those 10.1 billion+ SSL certificates? Non-professionals may not know anything about this, even SSL certificate users, they only know which CA they applied for SSL certificates from, but they may not have heard of certificate transparency, but certificate transparency is important for SSL certificate users that users should be concerned about whether a CA has issued an SSL certificate for their domain name without the user's knowledge, and what should be done if an SSL certificate is issued that is not known to them. Certificate transparency is a transparent publicity mechanism that protects the legal rights and interests of users. It is a bit like a notary service. The certificate transparency service provider is a notary office, which proves when a CA issued an SSL certificate for a domain name. This is guaranteed by a cryptographic algorithm and cannot be repudiated and indefensible. It can be seen that who is the certificate transparency service provider seems to be a matter that needs to be more transparent.

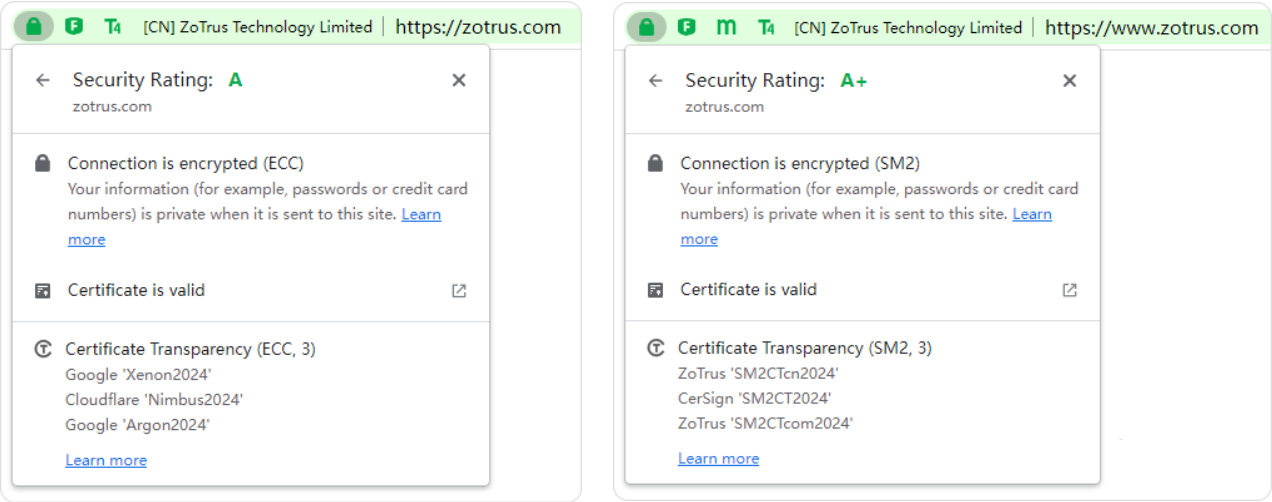
As the world's first browser that supports both international certificate transparency and SM2 certificate transparency, ZT Browser only enhanced the display of SM2 certificate transparency information before this upgrade, and it did not display the international certificate transparency information.





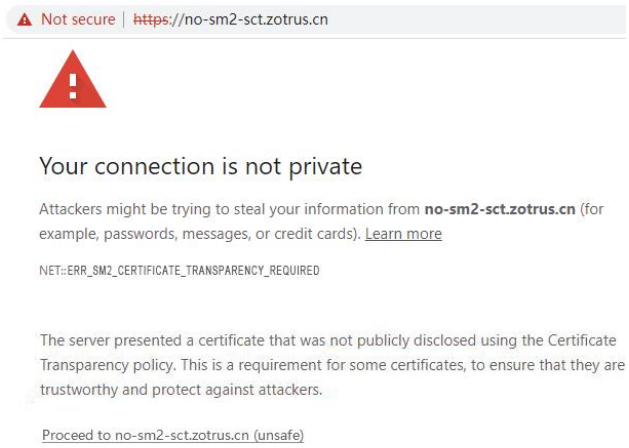
One of the highlights of this version upgrade of ZT Browser is that the global exclusive innovative display of certificate transparency information under the padlock and supports the display of certificate transparency details for RSA/ECC SSL certificates and SM2 SSL certificates, it uses the same interface displays the certificate transparency information of RSA/ECC/SM2 three algorithm SSL certificates, and no longer specifically displays only the SM2 certificate transparency information. The information displayed on the certificate transparency UI includes the cryptographic algorithm of the certificate transparency log signature, how many SCT data embedded in the SSL certificate, and lists the names of all certificate transparency log systems and log system operators.

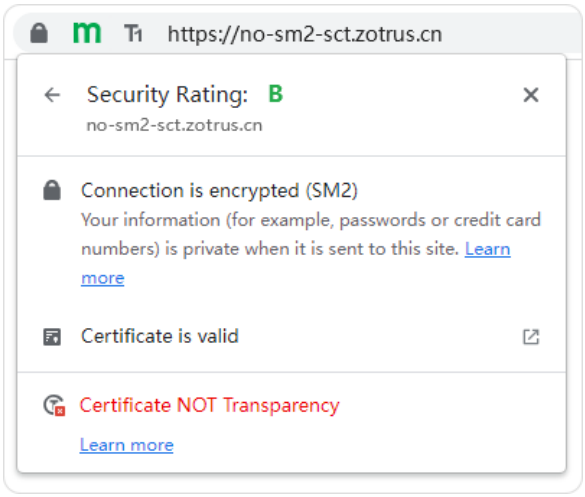
As shown in the left figure below, the cryptographic algorithm of the certificate transparency log service of this SSL certificate is the ECC algorithm, including 3 SCT data (ECC, 3), and the certificate transparency log service is provided by Google and Cloudflare respectively, which Google operated two certificate transparency logs: Xenon2024 and Argon2024, Cloudflare operated one certificate transparency log: Nimbus2024. As shown in the figure on the right below, the cryptographic algorithm of the certificate transparency log service of this SSL certificate is the SM2 algorithm, including 3 SCT data (SM2, 3), and the certificate transparency log service is provided by ZoTrus Technology and CerSign Technology respectively, which ZoTrus Technology operated two certificate transparent log: SM2CTcn20204 and SM2CTcom20204, and CerSign Technology operated one certificate transparent log: SM2CT2024.



That is to say, ZT Browser not only supports identification and verification of certificate transparency SCT data in RSA/ECC SSL certificates and SM2 SSL certificates, not only supports certificate transparency implemented by ECC/SHA2 algorithms and SM2/SM3 algorithms, but also displays the certificate transparency related information is aggregated into one user interface, allowing users to see at a glance the certificate transparency information of SSL certificates for all cryptographic algorithms.

If the RSS/ECC SSL certificate does not embed SCT data, ZT Browser will prompt "Not secure" like Google Chrome, as shown in the left figure below. As for the SM2 SSL certificate, considering that the SM2 certificate transparency standard is still in the process of being formulated, each CA still needs time to upgrade the CA system to support the SM2 certificate transparency, for the time being, ZT Browser only prompts "Certificate NOT transparency" if no ZT Browser trusted SCT data in the certificate, as shown in the right figure below. ZT Browser plans to adopt the same policy as Google Chrome from January 1, 2024 to displayed as "Not secure". It is hoped that the ZT Browser trusted CA can complete the CA system upgrade as soon as possible and issue SM2 SSL certificate embedded with ZT Browser trusted SCT data.





The significance of the UI innovation of ZT Browser is to further enhance the transparency of the certificate transparency service and make the certificate transparency more transparent. It not only allows SSL certificate users to know which company provides certificate transparency services for their SSL certificates, but also let website visitors know which company provides the certificate transparency service for the SSL certificate deployed on this website, which is similar to knowing which notary office issued the paper notarization certificate, which can not only improve the trustworthy of the certificate, but also enhance the certificate transparency service provider's brand, to make the certificates transparency service can also bring brand value to the provider, which is conducive to the healthy development of the certificate transparency ecology.

Richard Wang

August 8, 2023
In Shenzhen, China