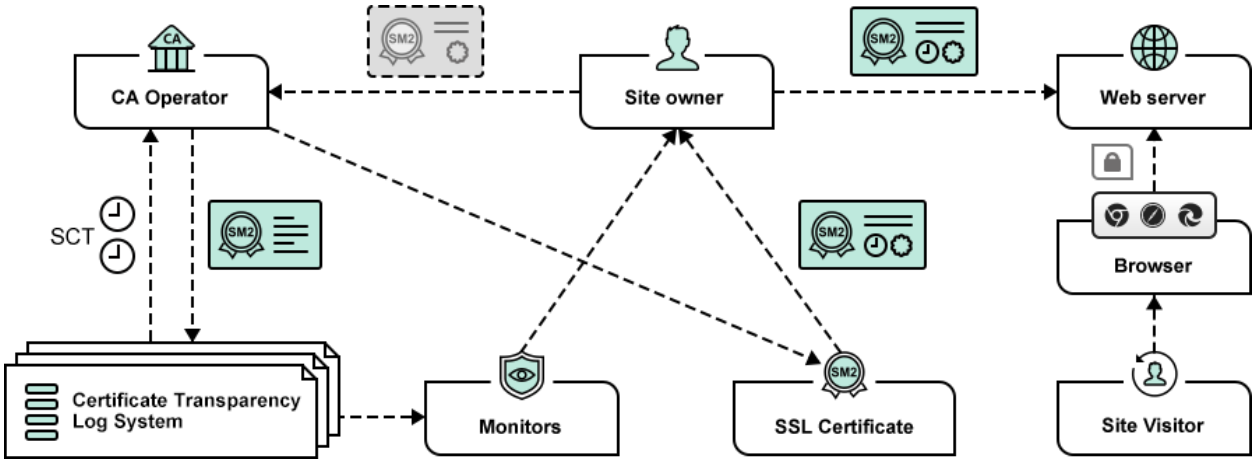
Who will secure the SM2 SSL certificates?

With the in-depth implementation of the "China Cryptography Law", the SM2 SSL certificate application has developed a rapid development trend. In the article "The things about SM2 SSL certificate", the author has pointed out the various issues existing in SM2 SSL certificate. These are some technical issues, which are easy to solve. The author wrote at the end of the article, "there is another very important issue that is more complicated, it cannot say it clearly in a few words. I will write an article independently next time." That's it for this article. This topic is indeed a bit complicated. Therefore, I wrote a blog about certificate transparency before this topic - " Who is securing the world's 7.3 billion SSL Certificates?". I strongly recommend readers to read this introductory article about certificate transparency before reading this article. This certificate security mechanism led by Google has successfully protected the security of 7.3 billion RSA/ECC algorithm SSL certificates in the world.

Let me briefly summarize the content of that article first. All globally trusted international algorithm RSA/ECC SSL certificates use the certificate transparency mechanism to ensure the security of the SSL certificates. For the follow-up comparison, I call this mechanism as "International Certificate Transparency". This mechanism requires that each globally trusted SSL certificate must submit the precertificate to the certificate transparency log system designated by Google for logging this certificate before this certificate is issued, and get the returned SCT data, the CA operator must embed the SCT data in the extension field of the SSL certificate to issue a formal certificate to the end user, so that the browser will trust this SSL certificate. Third-party monitors can monitor the issuance of each SSL certificate in real time by querying the certificate transparency log database. This is a certificate transparency ecosystem with multi-party participation. It is a zero trust to the CA system and the CA operator's certificate issuance behavior, which can effectively protect the security of the globally trusted international algorithm RSA/ECC SSL certificates.

(C) 2022 **ZoTrus Technology Limited**

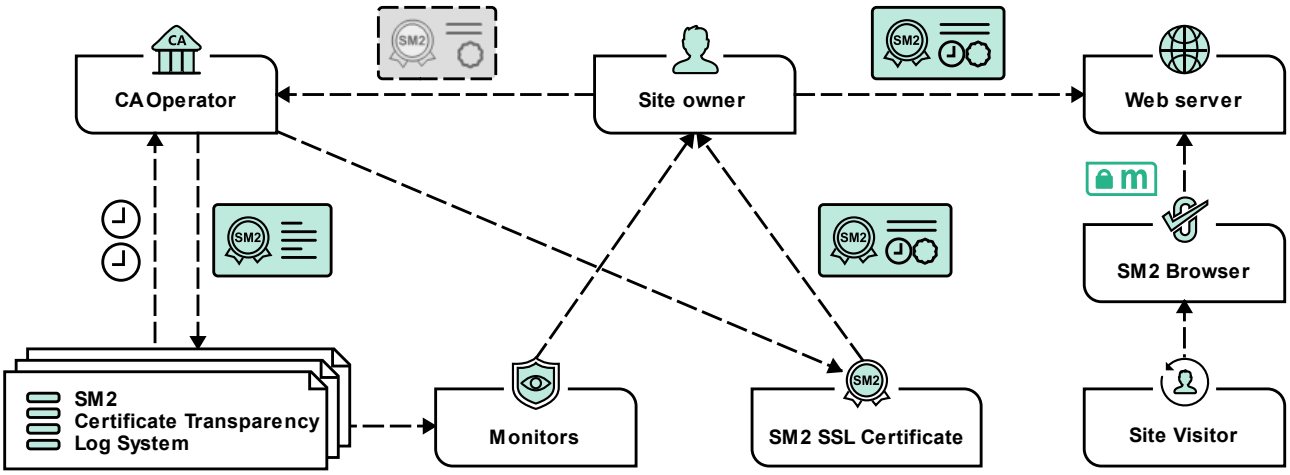


However, this very good mechanism for protecting the security of the SSL certificate cannot be used to ensure the security of SSL certificates that use SM2 algorithm, because the international certificate transparency log system does not support the SM2 algorithm and SM2 SSL certificates. Therefore, all SM2 SSL certificates on the market does not support certificate transparency, what should we do? Of course, China must also have its own certificate transparency mechanism, the author named it as "SM2 Certificate Transparency". ZoTrus Technology has invested in research and development, which lasted for more than a year, and successfully developed a full ecological product line of SM2 Certificate Transparency. The world's exclusive first release of the SM2 certificate transparency log system is the core system of the certificate transparency mechanism. It refers to the international certificate transparency log system but changed the cryptography algorithm from ECC algorithm to SM2 algorithm, and fully support the SM2 algorithm and SM2 SSL certificate.

To construct SM2 certificate transparency mechanism, it is not enough for the SM2 certificate transparency log system only, there must be a CA operator to submit the issued SM2 SSL certificate to the SM2 certificate transparency log system to get the signed SCT data, but there is no such CA system in the market. As the saying goes, asking for people is better to ask for yourself. ZoTrus Technology continued to invest in research and development, and innovatively developed the ZoTrus Cloud SSL System, which is the first SM2 CA system in the world that support the SM2 certificate transparency, the issued SM2 SSL precertificate all post to the SM2 certificate transparency log system to get the signed SM2 SCT data, after obtaining the SCT data, the SM2 SCT data is embedded into the issued SM2 SSL certificate, then it can be deployed on the website to realize the SM2 https encryption.

(C) 2022 **ZoTrus Technology Limited**

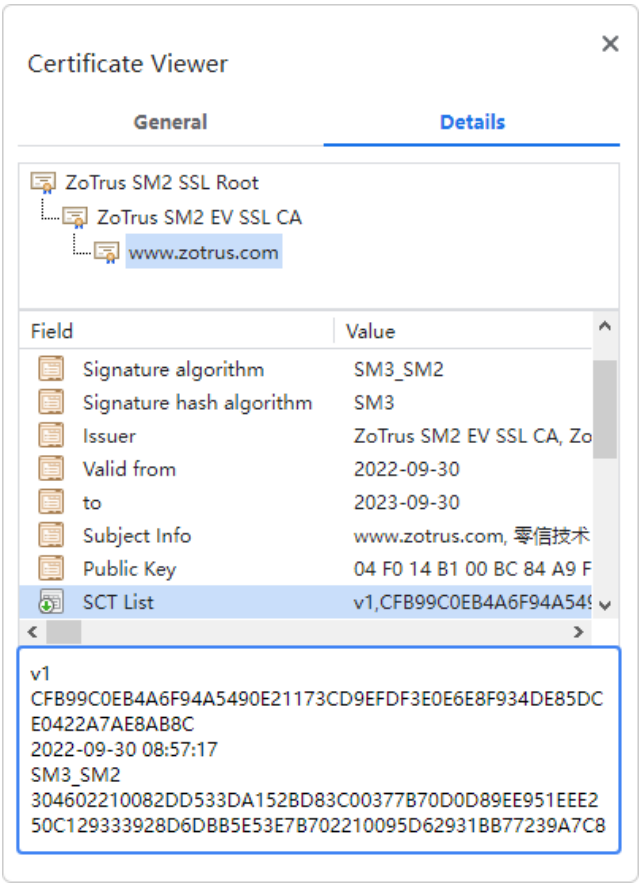
However, there is still one key product missing, that is the browser support. Similarly, there is no browser in the market that support SM2 certificate transparency. So, ZoTrus Technology continues to invest in research and development, and has realized that ZT Browser is the world's first to support SM2 certificate transparency, it includes and trust the ZoTrus Certificate Transparency Log System, and support verification of the SM2 SCT data in the SM2 SSL certificate, which forms a practically-operable SM2 certificate transparency ecosystem through various self-developed systems, a certificate transparency mechanism that uses the SM2 algorithm for the entire chain has created innovatively and exclusively in the world by ZoTrus! The last section is the third-party monitor system, ZoTrus SM2 Certificate Transparency Log System has opened an API interface in accordance with the RFC6962 standard for third-party monitors and auditors. ZoTrus Technology also will provide a real-time online query interface on the official website of the SM2 Certificate Transparency, allowing users to query all the logged SM2 SSL certificates in the SM2 Certificate Transparency Log System easily, to find the suspicious SM2 SSL certificates in time.

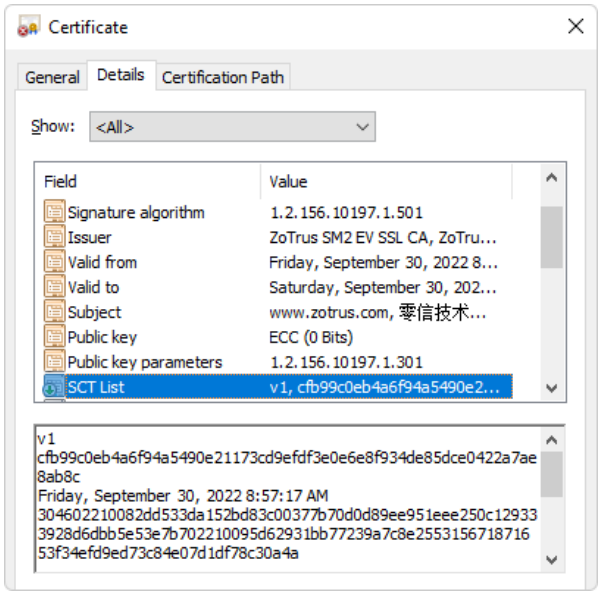


The SM2 certificate transparency mechanism adopts the same technology and the same standard as the international certificate transparency mechanism. The only difference is that the SM2 algorithm is used to realize the digital signature of certificate transparency data, instead of the ECC algorithm, and the browser supports SM2 algorithm to verify the SM2 SCT data. Welcome to use ZT Browser to visit ZoTrus official website, and click the padlock to view the SSL certificate, then you can see the certificate have a SCT List field that displays the SCT data, as shown in the left figure below. If you use the Windows Certificate Viewer to view this SM2 SSL certificate, as shown in the right figure below, the SCT List field and SCT data will also be displayed. But the difference is that since Windows

(C) 2022 **ZoTrus Technology Limited**

does not support SM2 algorithm, the signature algorithm of the SCT data will not be displayed after the SCT signature time, while viewing it with ZT Browser shows that the signature algorithm of the SCT data is the SM3_SM2, clearly tell the user that the SCT data adopts the SM2 algorithm.





From April 15, 2022, Google Chrome requires that SSL certificates with a certificate validity period of less than or equal to 180 days must contain 2 SCT data, and SSL certificates greater than 180 days must contain 3 SCT data. For SM2 certificate transparency policy, ZT Browser will also adopts the same policy. But due to there are currently only three SM2 certificate transparency log systems available provided by ZoTrus, for the time being, only one SM2 SCT data is required for less than or equal to 180 days SM2 SSL certificate, and two SM2 SCT data are required for the greater than 180 days SM2 SSL certificate. If there are more SM2 certificate transparency log systems available on the market in the future that pass the certification of ZT Browser, the same certificate transparency policy as Google Chrome will be implemented.

Today, the author is glad to see that the world's first SM2 certificate transparency mechanism based on SM2 algorithm has been completed and put into use. It not only protects the SM2 SSL certificates

(C) 2022 **ZoTrus Technology Limited**

security issued by CerSign and ZoTrus, but also protects the SM2 SSL certificates security issued by ZT Browser trusted SM2 root CAs. Welcome all the CA operators that issue SM2 SSL certificate to join this certificate transparency log system to protect the security of SM2 SSL certificate. Only all SM2 SSL certificates support the SM2 certificate transparent mechanism can truly ensure the security and trust of all SM2 SSL certificates, other SM2 SSL certificate without joining the certificate transparency mechanism will surely become an unsecure SM2 SSL certificate that may be abused. SM2 Certificate Transparency mechanism can effectively prevent maliciously issued SM2 SSL certificate that used for attacks and frauds, thereby protecting the security of the SM2 SSL certificate itself. Only the SM2 SSL certificate itself is secure and trusted guarantee, then truly protect the security and trust of the SM2 https encryption. And welcome all browsers that support the SM2 algorithm to join this SM2 certificate transparency mechanism to jointly contribute to ensure the security of SM2 SSL certificates.

Finally, considering that it takes time for the CA operators to upgrade the certificate issuance system, ZT Browser currently only displays "SM2 Certificate Not Transparency" for the SM2 SSL certificate that does not embed the SM2 SCT data. From July 1, 2023, ZT Browser will adopt the same certificate transparency policy as Google Chrome and will display "Not secure" warning for the SM2 SSL certificate that does not embed the SM2 SCT data trusted by ZT Browser. In this way, the security and trust of the SM2 SSL certificate is truly guaranteed from the SM2 certificate transparency mechanism.

Richard Wang

Sept. 30, 2022
In Shenzhen, China

(C) 2022 **ZoTrus Technology Limited**