Intranet SSL Certificates Must also Support Certificate Transparency

To ensure the security and trust of SSL certificates, in addition to the browser trusted root program, there must also be a certificate transparency mechanism for timely detection of mistakenly issued or maliciously issued SSL certificates, both of which are indispensable, and every Internet SSL certificate has supported certificate transparency since 2013, the same should be true for intranet SSL certificates.

1. ZoTrus has successfully built a SM2 certificate transparency ecosystem.

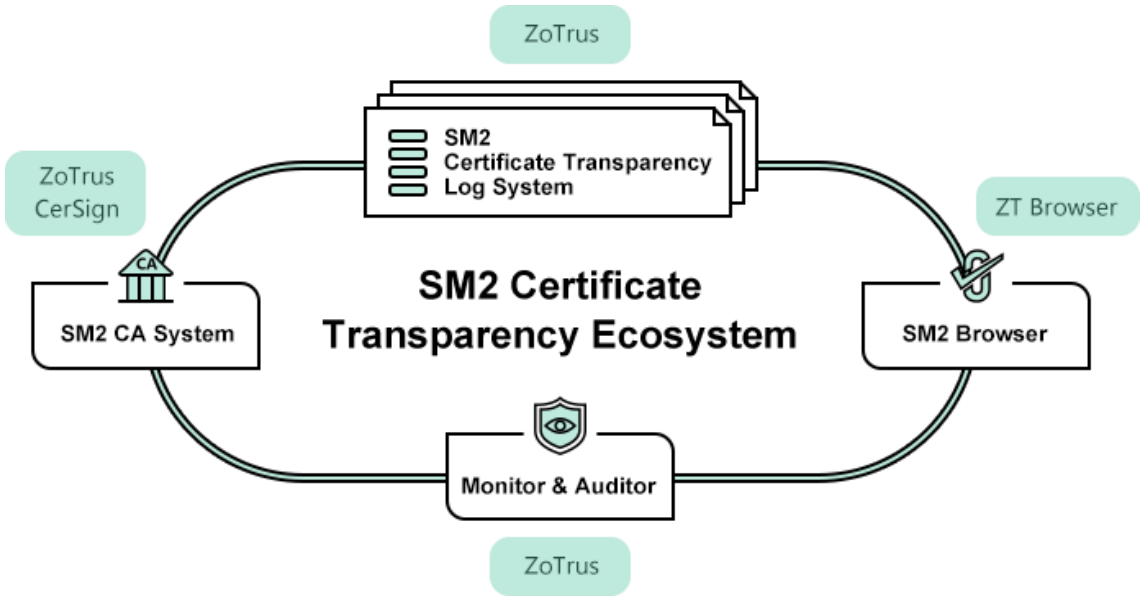
In order to make SM2 SSL certificates as transparency as RSA/ECC SSL certificates, ZoTrus Technology has launched the world's first ZoTrus SM2 Certificate Transparency Log System at the World Internet Conference in Wuzhen China in November 2022, and has been providing certificate transparency services for SM2 SSL certificates issued by CerSign and ZoTrus SM2 SSL certificates and other CA's issued SM2 SSL certificates for a year and a half, effectively ensuring the security and trust of SM2 SSL certificates.

And ZT Browser is the first in the world to support the SM2 certificate transparency and has included the three SM2 certificate transparency log systems operated by ZoTrus Technology, which can verify the embedded SM2 certificate transparency log signature SCT data in real time and display the certificate transparency details of this SM2 SSL certificate in the padlock details.

ZoTrus has upgraded the CA system to issue SM2 SSL certificates that support the SM2 certificate transparency, and each SM2 SSL certificate is submitted to the ZoTrus SM2 certificate transparency log system to obtain the certificate transparent log signature data, and embedded it in each issued SM2 SSL certificate, so as to realize the transparency of each SM2 SSL certificate and effectively protect the security and trustworthiness of the SM2 SSL certificates.

ZoTrus Technology is the first in the world to create a full product line for the SM2 certificate transparency ecosystem and uses SM2 algorithms to perfectly realize the certificate transparency of

SM2 SSL certificates. Not only that, ZoTrus Technology took the lead in formulating the "Certificate Transparency Specification" commercial cryptography standard with reference to the International Certificate Transparency Standard (RFC6962), and worked with relevant ecological vendors to jointly create a SM2 certificate transparency ecosystem based on commercial cryptography standards, jointly ensure the security and trustworthiness of SM2 SSL certificates, jointly contribute to ensuring the security of SM2 HTTPS encryption.



2. **Upgrade the SM2 Certificate Transparency Log to support the certificate transparency of intranet SSL certificates.**

The three SM2 CT logs operated by ZoTrus Technology only supported the SM2 SSL certificates for certificate transparency, and it did not support RSA/ECC SSL certificates. In order to make the RSA algorithm SSL certificates issued by the RSA root CA specially set up by CerSign and ZoTrus for intranet SSL certificate also support certificate transparency, ZoTrus Technology continues to invest in research and development, and upgrades the existing SM2 certificate transparency log system supports RSA and ECC SSL certificates. This is a bit of a challenging R&D work, but after the hard work of the R&D team, three operating ZoTrus SM2 Certificate Transparency Log System have been upgraded that all supports three-algorithm SSL certificates and realizes full-algorithm SSL certificates to support the SM2 certificate transparency. This is another technical innovation of commercial cryptography that it is worth writing a special article to talk about why the SM2 Certificate Transparency Log System must support SM2/RSA/ECC three-algorithm SSL certificates.

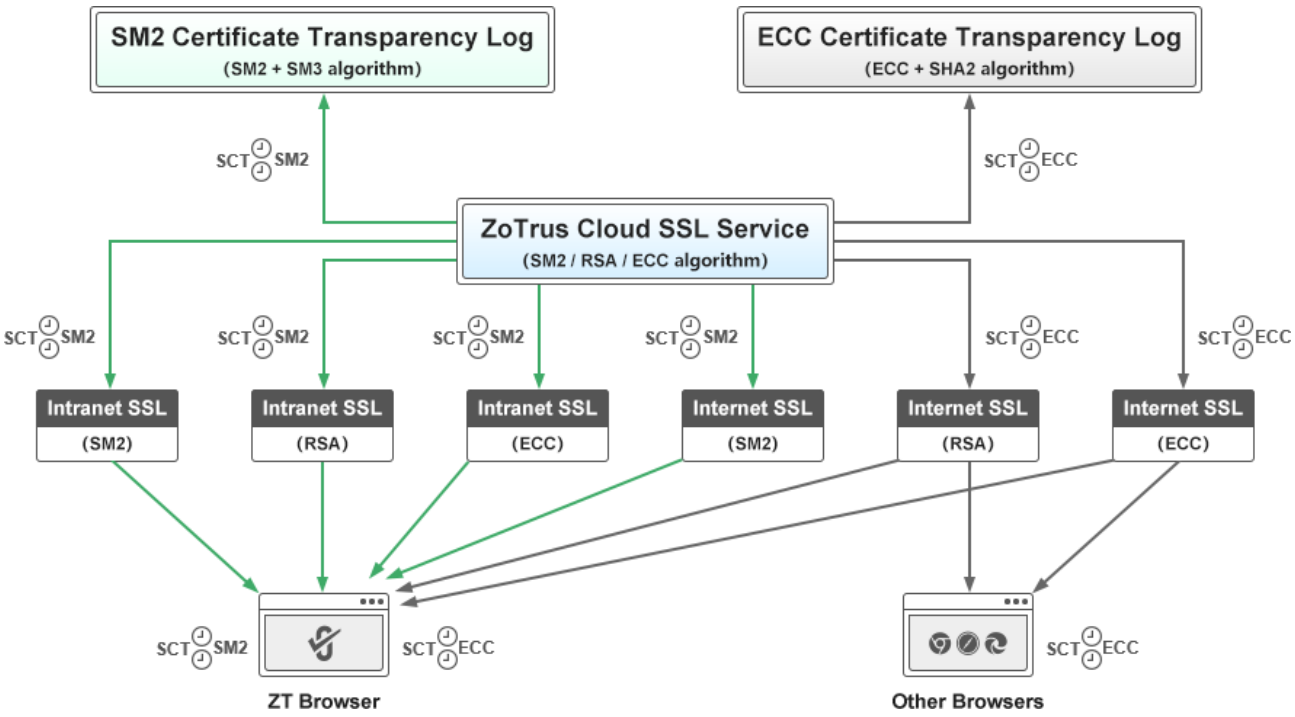
Before the upgrade, the ZoTrus CT Logs only support the SM2 algorithm SSL certificates, because the log signing key algorithm and HASH algorithm can only choose one algorithm, and the international CT log uses the ECC+SHA2 algorithm, the ZoTrus SM2 CT log uses the SM2+SM3 algorithm. Now, in order to ensure the security of the intranet web system, we plan to issue an intranet-specific RSA algorithm SSL certificate for customers who cannot upgrade the intranet web server to support the SM2 algorithm.

For intranet RSA SSL certificates support certificate transparency, there are two technical routes: one is to continue to use the current SM2 CT logs, adding support for RSA algorithm SSL certificates, and the other is to establish a new set of international algorithm CT log. If we choose the simplest solution of the second option, directly use Google's open-source CT log system to deploy one set to provide CT log service for RSA/ECC algorithm intranet SSL certificates, we need to operate and maintain two sets of CT log systems, which greatly increases the operation and maintenance cost.

And if we choose the first solution, we need to do a lot of research and development work, not only the SM2 CT log system needs to do a lot of modification to support the RSA/ECC algorithm SSL certificates, but also ZT Browser needs to be modified to support the validation of RSA/ECC SSL certificates that embedded a SCT data signed by SM2 algorithm in the SSL certificate, the code that was originally responsible for validating the SCT data of the RSA/ECC SSL certificate by open-source Chromium cannot be used because the original validation code does not support the SM2 algorithm.

Considering that the cost of operating and maintaining two sets of algorithm CT systems has been greatly increased, and considering that the RSA/ECC algorithm SSL certificate and the SM2 algorithm SSL will be used both for a certain period of time in the current practical application, ZoTrus Technology, as the leader in formulation of the SM2 certificate transparency standard and the leader of SM2 certificate transparency technology, ZoTrus must make technical preparations in advance so that the SM2 certificate transparency log system supports both SM2 algorithm SSL certificates and RSA/ECC algorithm SSL certificates. Therefore, we decided to upgrade the existing SM2 certificate transparency log system to support SSL certificates issued by three algorithms (SM2/RSA/ECC). The current international certificate transparency log system uses the ECC algorithm but supports RSA and

ECC algorithm SSL certificates. This is for the same reason: one system supports multiple cipher algorithms for SSL certificates.



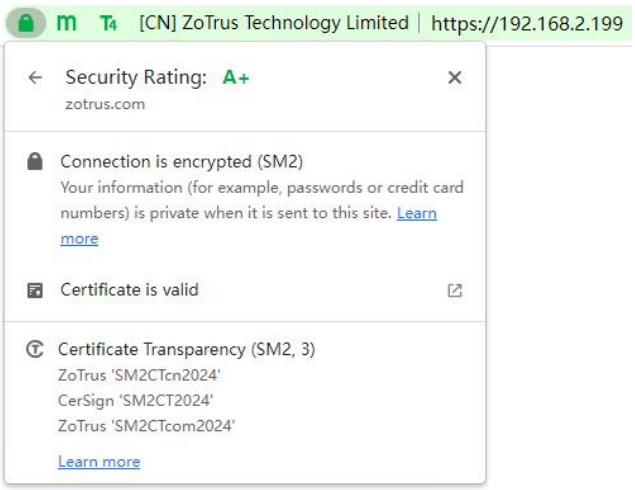
The upgraded ZoTrus SM2 Certificate Transparency Logs are not only used for the certificate transparency log of the SM2 SSL certificates submitted by the all CAs trusted by ZT Browser, but also for CerSign and ZoTrus publicly trusted SM2 SSL certificates and intranet SM2/RSA SSL certificates, to ensure the reliable supply of the CerSign and ZoTrus SSL certificates, and ensure that the intranet RSA/SM2 SSL certificate adopts the same certificate transparency policy as the publicly trusted SSL certificates. The ZoTrus SM2 Certificate Transparency Log System does not accept the publicly trusted RSA/ECC SSL certificates submission by other CAs, and it is limited to the intranet RSA/ECC SSL certificates submission that issued by the intranet RSA/ECC algorithm SSL root CA trusted by ZT Browser.

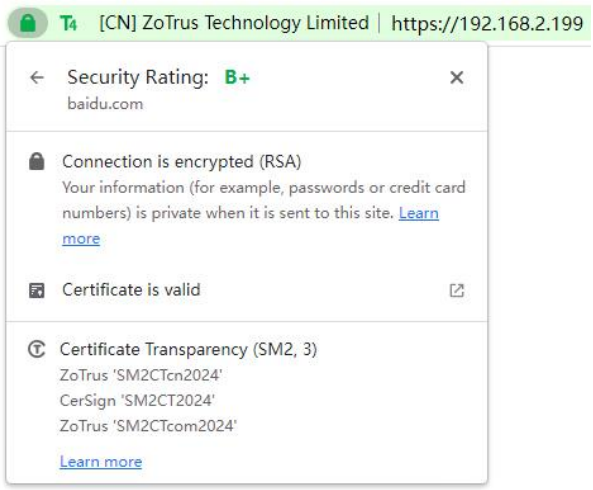
3. Upgrade ZT Browser to support the certificate transparency of intranet SSL certificates.

The ZoTrus Cloud SSL Service System submits each intranet SSL certificate to the upgraded ZoTrus SM2 Certificate Transparency Log to achieve transparency of the intranet SSL certificate, which is also the first in the world, not only realizing the intranet SM2 SSL certificates support the SM2 certificate transparency, but also ZT Browser is the world's first to realize the real-time verification

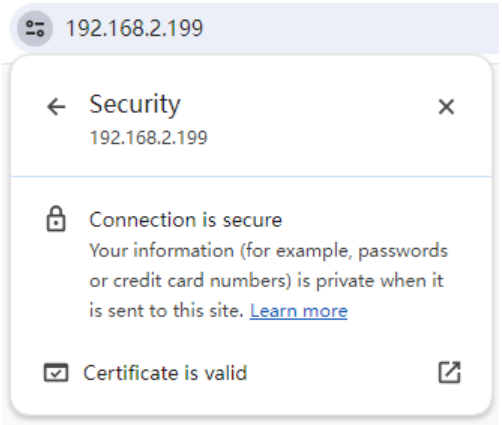
and display the SM2 certificate transparency details in the RSA algorithm SSL certificate.

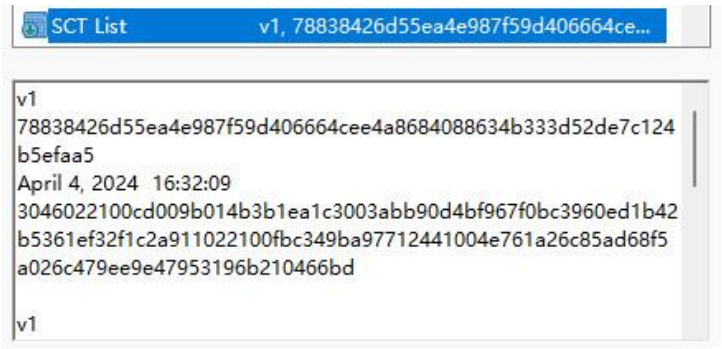
As shown in the figure on the left below, ZT Browser not only trusts and displays the intranet EV SSL certificate as the green address bar, but also clicks on the padlock, and you can see that this intranet SSL certificate is an SM2 algorithm SSL certificate, which uses the SM2 algorithm to achieve HTTPS encryption, and the certificate transparency signature data is signed by the SM2 algorithm. As shown in the figure below on the right, this intranet EV The SSL certificate is an RSA algorithm SSL certificate, which also supports the SM2 certificate transparency, and the RSA algorithm SSL certificate realizes HTTPS encryption, but the certificate transparency signature data is signed by the SM2 algorithm, which is the world's first RSA algorithm SSL certificate supports SM2 certificate transparency, and ZT Browser is the first in the world to realize the verification of the SM2 certificate transparency signature data in the RSA algorithm SSL certificate, which is another technological innovation.





Since Google Chrome does not verify whether the intranet SSL certificate supports certificate transparency, nor does it parse the embedded certificate transparency SCT data of the intranet SSL certificate, it does not affect the normal browsing of Google Chrome users for website deployed intranet RSA algorithm SSL certificates, although Google Chrome does not support the SM2 algorithm, as shown in the below figure on the left. Windows Certificate Viewer can still parse the SM2 certificate transparency log data (SCT List), but it does not display the CT log signing algorithm, as shown in the below figure on the right.





4. **Intranet SSL certificates support certificate transparency, which is as secure and trustworthy as Internet SSL certificates.**

ZoTrus Technology is the first in the world to realize the SM2 algorithm certificate transparency log system, and supports the intranet SSL certificate issued by the SM2 algorithm, RSA algorithm and ECC algorithm, so that each intranet SSL certificate can achieve certificate transparency no matter what algorithm is used, which effectively protests the security and trustworthiness of the intranet SSL certificate, and users can use the issued intranet SSL certificate with confidence as if they were using an Internet SSL certificate.

No matter what algorithm the SSL certificate uses, it supports the SM2 algorithm to achieve certificate transparency, and this scientific research achievement and application practice provides a very good technical exploration and operation and maintenance practice for establishing a national central certificate transparency log system to uniformly supervise the RSA/ECC SSL certificates and SM2 SSL certificates deployed and used in China.

Richard Wang

April 22, 2024
In Shenzhen, China