SM2 CT is a must to ensure the security of SM2 HTTPS encryption

All browsers display "Not secure" to HTTP website, because HTTP is a cleartext transmission protocol, and the information transmission from the browser to the server (cloud) is plaintext, and it is very easy to be illegally stolen and illegally tampered with. The only feasible technical measure is HTTPS encryption transmission. The SSL certificate is deployed in the server to implement HTTPS encryption. This is the foundation and must be of the security of the website. To ensure the security of SSL certificate, the international standard technical measure is that every SSL certificate for HTTPS encryption must be logged in certificate transparency log system to get the SCT data before issuing, and the SCT data must be embedded in the SSL certificate, only in this way, the browser will trust this SSL certificate, and this SSL certificate can be deployed in web server for HTTPS encryption. This certificate transparency mechanism is to ensure the security of the SSL certificate, which is the basis of Internet security.

The certificate transparency mechanism has successfully protected the security and trust of the global trusted RSA/ECC SSL certificate with a total of 7.4 billion SSL Certificates. China is vigorously promoting the popularization of SM2 SSL certificate to achieve SM2 HTTPS encryption, to cope with the currently uncertain international environmental situation. China must also have its own SM2 certificate transparency mechanism to ensure the security of SM2 SSL certificate, thereby ensuring the security of SM2t HTTPS encryption, and then reliably ensure the security of China’s website and the Internet.

The premise of SM2 HTTPS encryption security is the SM2 certificate transparency, that is, the certificate transparent log system implemented by SM2 algorithm. Only each SM2 SSL certificate is transparent can ensure the security of SM2 SSL certificate. SM2 HTTPS encryption and SM2 certificate transparency mechanism, together with China's current implementation website filing

mechanism, domain name registration real-name system, form a complete website security protection system from domain name registration (website birth) to website operation to website security (encryption). which will be truly powerful to ensure the security and controllability of China's websites and the Internet, each mechanism is indispensable.

The main technical and management advantages of the SM2 certificate transparency mechanism are:
(1) Ensure the open and transparent disclosure of the issuance behavior of each SM2 SSL certificate, timely discover various maliciously and mistakenly issued SM2 SSL certificates, and effectively protect the security and interests of the websites.
(2) Provide a real-time and accurate statistics of SM2 SSL Certificate issuance for cryptography administration authority to provide reliable reference data for government decision-making.
(3) Provide a reliable market analysis data for the relevant parties of SM2 SSL certificate and the SM2 HTTPS encryption industry to provide reliable data support for industrial development.

At present, only ZoTrus Technology has successfully developed and reliably operated three SM2 certificate transparency log systems, and only ZT Browser supports the verification of SM2 certificate transparency security mechanism, and only CerSign and ZoTrus issued SM2 SSL certificate embed SCT data, this is not enough! The author calls on the cryptography administration department to establish a national-level SM2 certificate transparency log system to build and operate the SM2 certificate transparency log system from the height of national security. And the author also calls on all SM2 supported browsers to support the SM2 certificate transparency mechanism, and the CA operators that can issue the SM2 SSL certificate to log each SM2 SSL certificate in SM2 certificate transparency log system as soon as possible. Only in this way can a SM2 certificate transparency mechanism ecosystem be well established, so that the SM2 certificate transparency can truly play a greater security protection role in China Internet security, to truly protect China's Internet security.

Richard Wang

Sept. 30, 2022
In Shenzhen, China