Cryptography Core System, National Day Tribute

The National Day is a festival celebrated by the whole China. The author believes that in addition to "celebration", the focus should be "presenting". What to give to the National Day is more important because the prosperity of the country requires the dedication of everyone and every enterprise.

1. It is very gratifying to present the cryptography core system on the National Day.

On September 30th, ZoTrus Technology launched the world's first two core products of the SM2 certificate transparency ecosystem – ZoTrus SM2 Certificate Transparent Log System and ZT Browser that supports the SM2 certificate transparency. The two innovative products are global exclusive first innovative release. Although these two products are free products and cannot bring direct economic benefits, their social benefits and value are huge, and they can effectively protect the security of China SM2 SSL certificate, thereby ensuring China's Internet security. This is the National Day tribute of ZoTrus Technology. The cryptography core system released in time for the National Day has fulfilled the author's wish for many years, and I am very gratified.

As early as December 2018, in the keynote speech of the "2018 Cyberspace Trust Summit" hosted by the China Electronics and Information Industry Development Research Institute under the guidance of the Cybersecurity Coordination Bureau of the Office of Central Cyberspace Affairs Commission of China and the State Cryptography Administration of China, the author proposed to build a "China Cyberspace Trust Ecological Construction Framework", the core idea of which is to refer to the international system to build China's cyberspace trust ecosystem based on the China Commercial Cryptography. Of course, the core is the comprehensive application of the digital certificate using SM2 algorithm, and the most important part is the deployment application of SM2 SSL certificate.

After the Summit, the author led the R&D team to focus on the research and development of products related to the SM2 SSL certificate and released the world's first SM2 algorithm root CA certificate in Chinese in April 2019. And plans to develop the SM2 certificate transparency log system refer to the international certificate transparency log system since then. But unfortunately, it has not been put into action due to various reasons. The author started a new business in June last year, and I can finally do what I want without any constraints. After more than a year of hard work and overcoming all kinds of difficulties, I finally finished what I wanted to do 4 years ago on the National Day. The author is very happy and gratified to share this happiness and related knowledge with readers and friends.

Why is Certificate Transparency important? Why is Google taking the lead in developing a Certificate Transparency system and making it an RFC standard? This must start with Google itself as a victim of SSL certificate mis-issued. You can find many cases by searching the news and reports on the illegal issuance of SSL certificates for gmail.com and google.com. These illegally issued globally trusted SSL certificates are of course used to illegally attack Gmail mailboxes and are used to illegally steal mailbox passwords and email confidential information. As a result, Google took the lead in creating a certificate transparency system, requiring globally trusted CAs to submit the SSL precertificate to the Google Certificate Transparency log system for recordation before issuing each SSL certificate, which is open and transparent disclosing the issuing behavior of each SSL certificate, which is why it is called "Certificate Transparency". After submitting the record, the certificate transparency log system will return a logged certification to the CA system - a digital signature data signed by the private key of the certificate transparency log system - SCT data, the CA system must embed this SCT data in the officially issued SSL certificate, only this SSL certificate can be trusted by Google Chrome, and then this SSL certificate is useful.

Readers and friends who are interested in Certificate Transparency, please refer to the author's other blog posts related to Certificate Transparency. This article will not repeat what has already been written but will only talk about who are the participants in the Certificate Transparency ecosystem, and how to build China SM2 SSL certificate transparency ecology.

2. International Certificate Transparency ecology, great success.

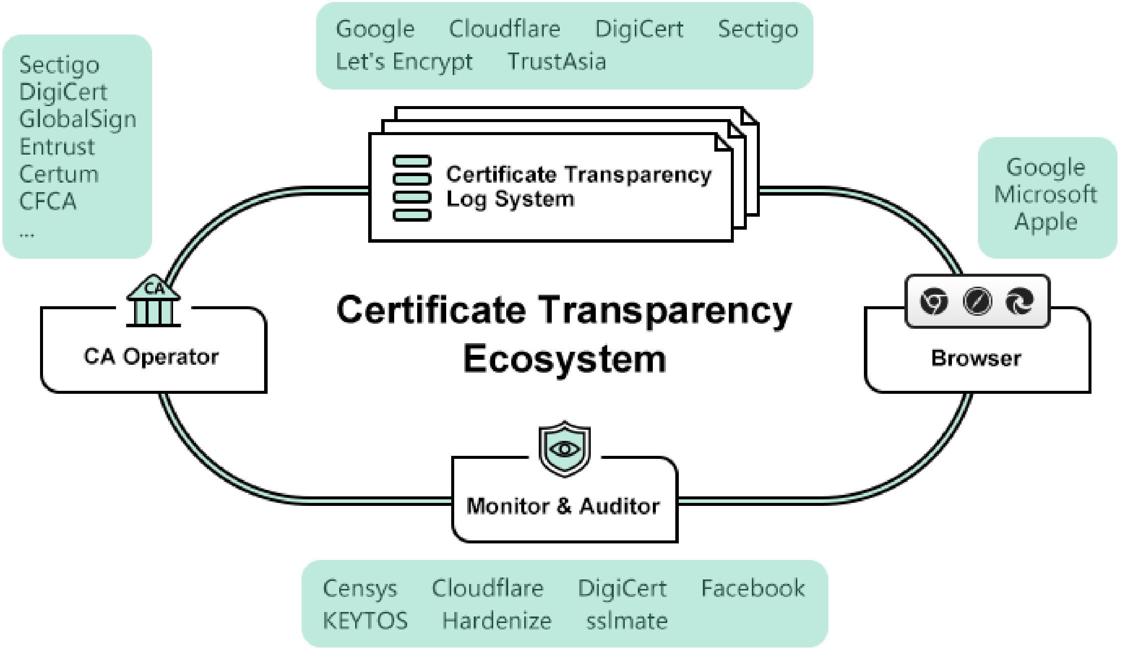
To facilitate the comparison below, this article refers to the current ecosystem of certificate transparency services for global trusted SSL certificates as "International Certificate Transparency". Since 2013, this ecosystem has successfully protected the world's 7.5 billion international algorithm RSA/ECC SSL Certificate security.

Since 2013

7,518,733,699

certificates have been logged

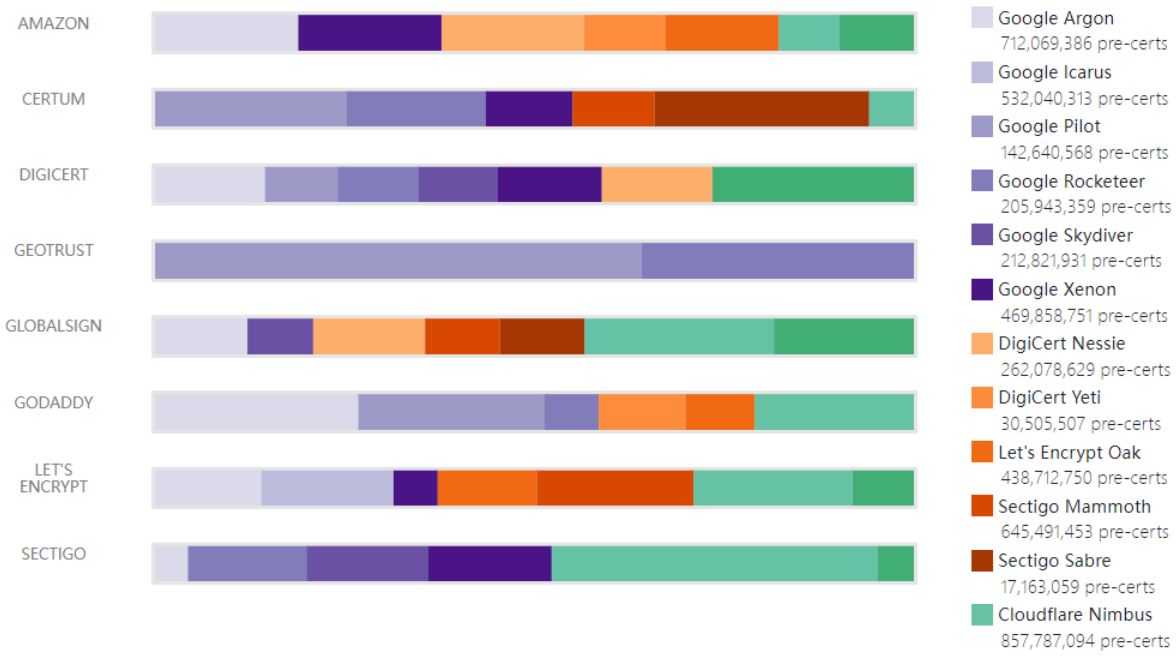
So, what does the international certificate transparency ecosystem look like? Who are the participants? Of course, the first is Google. The reason why Google can take the lead in making Certificate Transparency is of course inseparable from the influence and market share of Google Chrome. Google released the Certificate Transparency log system, which firstly occupied the moral high ground - "Transparency", and secondly, of course, using the influence of its browser has come up with a killer - if the SSL certificate issued by the CA does not support certificate transparency, Google Chrome will not trust it, and there will be a "Not secure" warning! Later, Apple browser – Safari also joined the camp to help certificate transparency, the same distrust warning if the SSL certificate does not support certificate transparency! Then came the support of the Microsoft Edge browser, and there is also a warning if the SSL certificate does not support Certificate Transparency! The global market share of these three major browsers ranks in the top 1, 2 and 3 respectively, with a total of 88%. The Firefox browser, which once had a share of 40%, did not support certificate transparency and fell to the fourth place (3%). This aspect may reflect the user's recognition and attention to certificate transparency. If the browser does not support certificate transparency, it means trusting the SSL certificate issued for malicious attacks. How can such a browser ensure the Internet security of browser users? Of course, users will ditch it! Browsers are the first important players in the Certificate Transparency ecosystem.



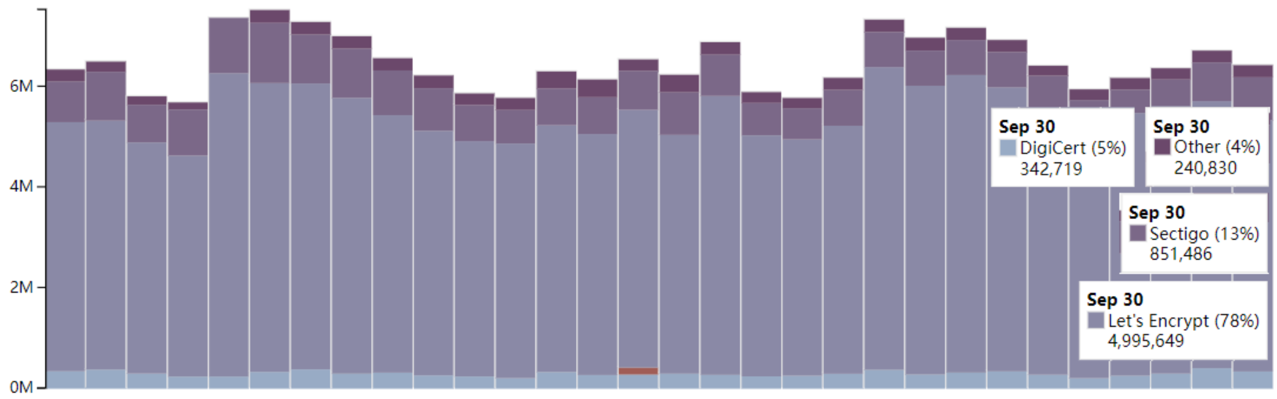
The second important participant in the Certificate Transparency ecosystem is of course the operator of the Certificate Transparency log system. There must be a certificate transparency log system first. This is the source, and Google must take the lead. Google has not only developed a certificate transparency log system, but also made the system completely open source, this encourages everyone to play together and encourage multiple deployments and operations the certificate transparency log system to provide certificate transparency log service for CA operators. Google Chrome requires that each SSL certificate must have one SCT from Google's own certificate transparency log system, and the other one or two must be other non-Google-operated certificate transparency log systems to show fairness and non-exclusiveness. At present, in addition to Google itself, the certificate transparency log system participants certified and trusted by Google Chrome include: Cloudflare, the world's leading CDN distribution service provider, and 4 well-known CA operators: Sectigo, DigiCert, Let's Encrypt and TrustAsia. CA operators operate the certificate transparency log system is not only for itself, but also open to other CAs.

The following picture shows the statistics of the usage of each CT system published by the Cloudflare Certificate Transparency website. Google CT system has 2.274 billion precertificates, Cloudflare has

857 million, Sectigo has 662 million, DigiCert has 567 million, Let's Encrypt has 438 million copies.



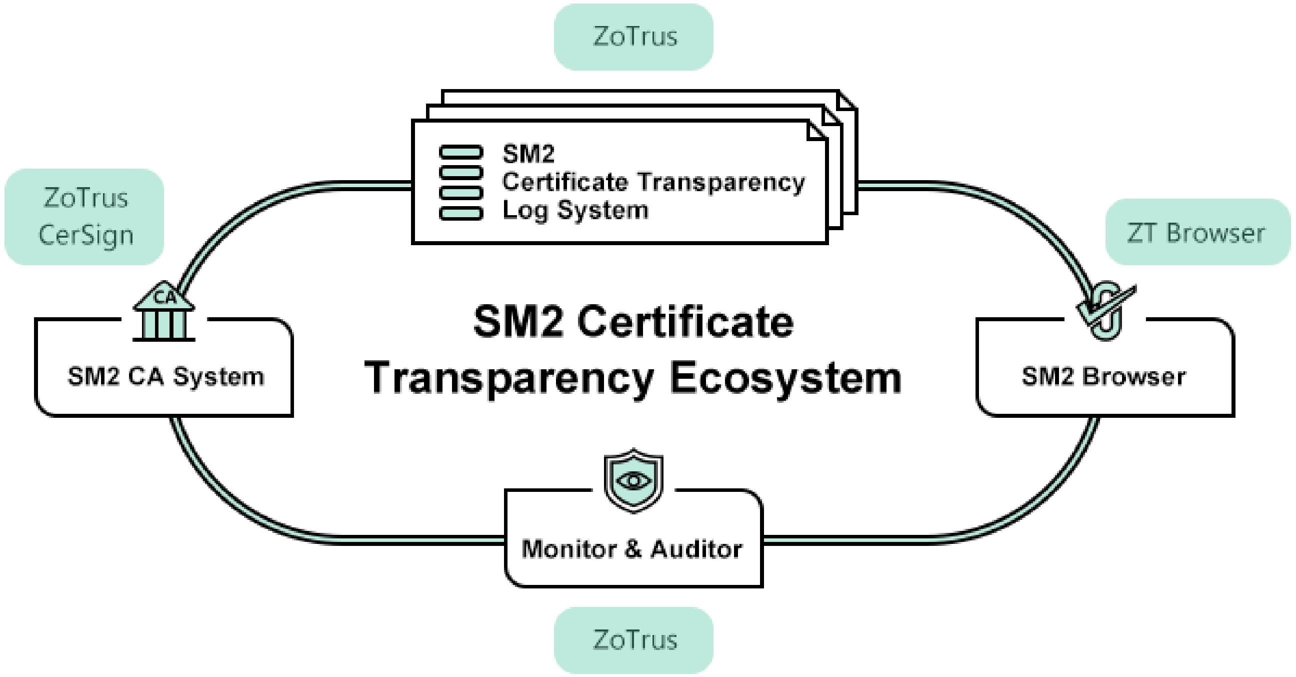
The CA operator is the third participant. It is both the service object and the supervised object of the certificate transparency ecosystem. At present, all CA operators that issued SSL certificates around the world have already supported certificate transparency, and each SSL certificate issued has already been submitted to the above certificate transparency log system certified and trusted by Google for transparency. The following figure is a histogram of the global SSL certificate issuance volume logged in the Certificate Transparency log system every day in September. The global issuance volume on September 1 was 6,344,370, and on September 30, it was 6,430,684, and the highest issuance volume was 7,527,091 on September 6th.



The last important participant is the monitor and auditor. The responsibility of this party is to ensure that all SSL certificates that have embedded SCT data are visible in the certificate transparency log system, and to observe suspicious certificates in the log. Users can subscribe to these services to receive timely notifications. Some service providers provide SSL certificate online query services, some such as social media providers - Facebook provides a monitoring service for its users - every time a CA operator issues an SSL certificate for a monitored domain name, user will receive Facebook notifications or Webhook API callback notifications. These services can help website owners discover suspicious certificates in a timely manner and effectively protect the legitimate rights and interests of website owners.

3. SM2 Certificate Transparency ecology, makes its debut.

Since the international certificate transparency ecosystem only supports the international algorithm RSA and ECC SSL certificates, and does not support China algorithm SM2 SSL certificate, in order to ensure the security of China SM2 SSL certificate, we must also establish a SM2 certificate transparency ecosystem. So, what is the status of China SM2 certificate transparent ecological construction? The SM2 Certificate Transparency Ecosystem was exclusively proposed by ZoTrus Technology, and it debuted on the day before the National Day. Two blockbuster products related to the SM2 Certificate Transparency Ecosystem were released globally, including the world's first certificate transparency log system that supports SM2 algorithm - ZoTrus SM2 Certificate Transparency Log System and the world's first browser that supports SM2 Certificate Transparency - ZT Browser. The world's first SM2 CA system that can issue SM2 SSL certificate embedded SM2 SCT data has been developed and is under internal testing, it will be officially released for issuing SM2 SSL certificate for public soon. As for monitors and auditors, ZoTrus Certificate Transparency Log System has provided a certificate transparency log data query API based on the RFC6962 standard for public query by interested parties and plans to provide online query services in SM2CT official website.



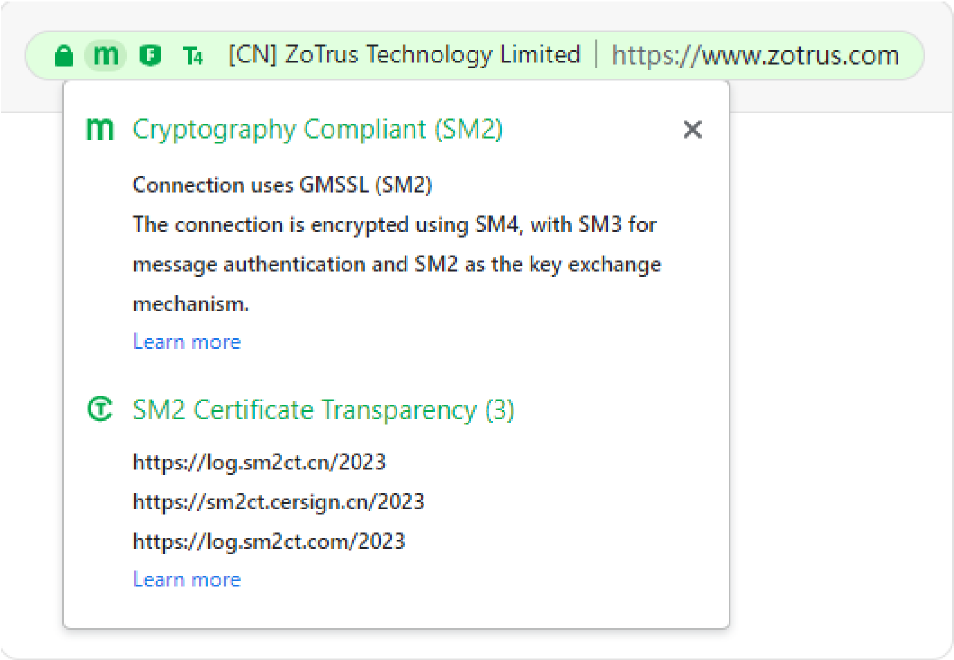
The author believes that readers can see that China's SM2 certificate transparency ecology has just started. ZoTrus Technology exclusively creates related products and services for the entire ecology, but only one company cannot truly establish an ecosystem. It is hoped that China can build a national-level SM2 certificate transparent log system and raise the SM2 certificate transparency logging to the same height and importance as the website domain name filing. The author also hope that more companies can also provide the SM2 certificate transparency log service, more browsers that support SM2 SSL certificate will support the SM2 certificate transparency, and all CA operators that can issue the SM2 SSL certificate will support the SM2 certificate transparency as soon as possible. It is hoped that more companies can provide monitoring and auditing services for SM2 SSL certificates, because the certificate transparency ecosystem requires multiple systems and services related to certificate transparency to work together, so as to play a greater role in the development of SM2 SSL certificate and SM2 https encryption, thus effectively protecting China cyberspace security.

4. Real experience of the SM2 certificate transparent ecology

Readers who want to know and experience the SM2 certificate transparency ecological product can download and install ZT Browser and use the ZT Browser to visit the official website of ZoTrus: https://www.zotrus.com, and experience the SM2 certificate transparency ecology for yourself to see what a transparency ecology looks like.

4.1 Experience how the browser that supports SM2 certificate transparency displays the SM2 certificate transparency

As shown in the figure below, clicking the SM2 encryption icon (**m**) in the address bar of the ZT Browser will show that this website is encrypted with SM2 algorithm, and it is Cryptography Compliant. The second part is to show that the SM2 SSL certificate deployed on this website supports SM2 Certificate Transparency and embeds the SCT data of 3 SM2 Certificate Transparency log services and displays the Service URLs of the three Certificate Transparency log services. Please note that these URLs are the SM2 certificate transparency log service system URLs, which cannot be accessed through browsers, but the URLs without /2023 can be accessed using browsers, and they will redirect to the official website of SM2 certificate transparency (sm2ct.cn or sm2ct.com). You can click the “learn more” below to learn more about the meaning of the SM2 certificate transparency icon.



[CN] ZoTrus Technology Limited | https://www.zotrus.com

m 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 Transparency (3)

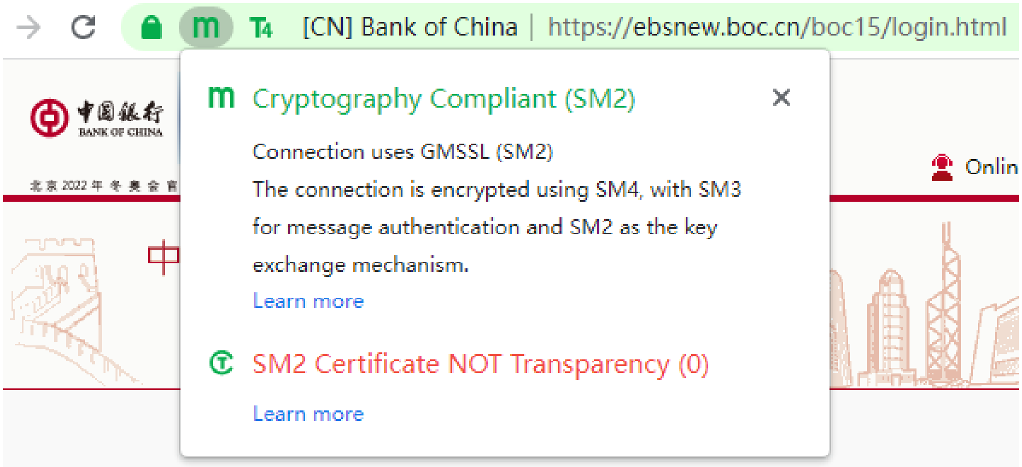
https://log.sm2ct.cn/2023

https://sm2ct.cersign.cn/2023

https://log.sm2ct.com/2023

Learn more

Let's use ZT Browser to access the personal online banking system of Bank of China: https://ebsnew.boc.cn/boc15/login.html, this is the only online banking website in China that has deployed a SM2 SSL certificate and is encrypted with SM2 algorithm. In the online banking system, click the SM2 encryption icon(**m**) in the address bar of the ZT Browser, it will show that this website is encrypted with SM2 algorithm, and is compliant with the Cryptography Law. The second part is to show whether the SM2 SSL certificate deployed on this website supports the SM2 Certificate Transparency, and it shows "SM2 Certificate NOT transparency", which means that the SM2 SSL certificate deployed by this website does not yet support the SM2 certificate transparency. At present, this is still a normal state, because there is no SM2 certificate transparency log system in China before that can be used by CA operators to obtain the SM2 SCT data. Now, China already has SM2 certificate transparency log service available, the author believes that the CA operators that issued this certificate will support the SM2 certificate transparency as soon as possible.



[CN] Bank of China | https://ebsnew.boc.cn/boc15/login.html

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.

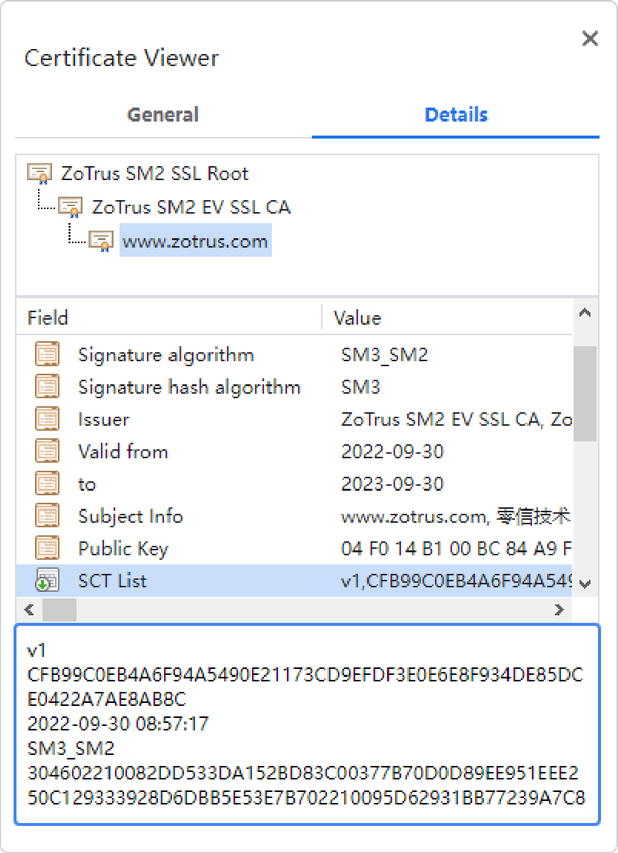
Learn more

SM2 Certificate NOT Transparency (0)

Learn more

4.2 Experience what a SM2 SSL certificate that supports SM2 certificate transparency look like.

As shown in the figure below, click the padlock icon to view the SM2 SSL certificate, click the details to scroll down to see the SCT List that is the same as the RSA/ECC SSL certificate, and display the SCT data of the three SM2 certificate transparency log service embedded in the certificate , where "SM2_SM2" is displayed in the fourth row, indicating that the signature algorithm of the SCT data is the SM2 algorithm. International Certificate Transparency SCT data will appear as "SHA256 ECDSA". This SM2 SSL certificate is issued by the world's first SM2 CA system that can issue SM2 SSL certificate embedded the SM2 SCT data. It is the fourth SM2 SSL certificate in the world that embedded the SM2 certificate transparency SCT data, the first one is the SM2 SSL certificate issued to the test website - sm2test.zotrus.cn.

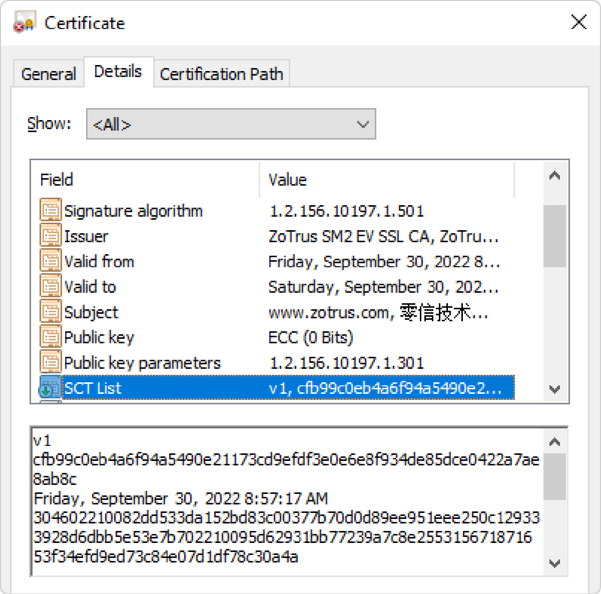


Certificate Viewer

ZoTrus SM2 SSL Root
ZoTrus SM2 EV SSL CA
www.zotrus.com

Field	Value
Signature algorithm	SM3_SM2
Signature hash algorithm	SM3
Issuer	ZoTrus SM2 EV SSL CA, Zo
Valid from	2022-09-30
to	2023-09-30
Subject Info	www.zotrus.com, 零信技术
Public Key	04 F0 14 B1 00 BC 84 A9 F
SCT List	v1,CFB99C0EB4A6F94A54!

```
v1
CFB99C0EB4A6F94A5490E21173CD9EFDF3E0E6E8F934DE85DC
E0422A7AE8AB8C
2022-09-30 08:57:17
SM3_SM2
304602210082DD533DA152BD83C00377B70D0D89EE951EEE2
50C129333928D6DBB5E53E7B702210095D62931BB77239A7C8
```



Certificate

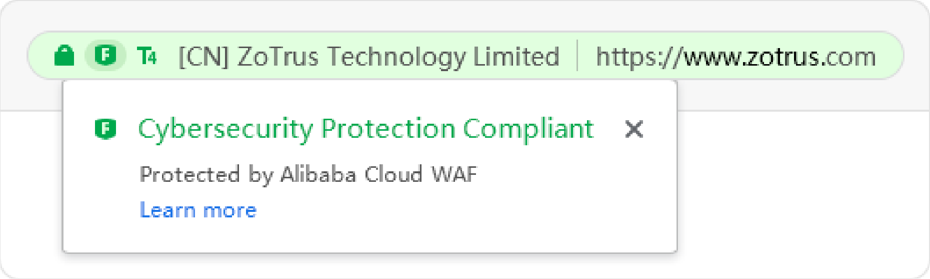
Show: <All>

Field	Value
Signature algorithm	1.2.156.10197.1.501
Issuer	ZoTrus SM2 EV SSL CA, ZoTru...
Valid from	Friday, September 30, 2022 8...
Valid to	Saturday, September 30, 202...
Subject	www.zotrus.com, 零信技术...
Public key	ECC (0 Bits)
Public key parameters	1.2.156.10197.1.301
SCT List	v1, cfb99c0eb4a6f94a5490e2...

```
v1
cfb99c0eb4a6f94a5490e21173cd9efdf3e0e6e8f934de85dce0422a7ae
8ab8c
Friday, September 30, 2022 8:57:17 AM
304602210082dd533da152bd83c00377b70d0d89ee951eee250c12933
3928d6dbb5e53e7b702210095d62931bb77239a7c8e2553156718716
53f34efd9ed73c84e07d1df78c30a4a
```

4.3 Experience zero reconstruction of SM2 https encryption and cloud WAF protection

As shown in the figure below, clicking the cloud WAF protection icon (F) will show that this website is protected by Alibaba Cloud WAF, and display "Cybersecurity Protection Compliant". ZoTrus official website uses the world’s first website security cloud service using SM2 SSL certificate that supports SM2 certificate transparent SCT data to realize SM2 https encryption automatically. This is a zero-reconstruction website security cloud service based on Alibaba Cloud CDN+WAF service created by ZoTrus Technology, which fully automatically configures the SM2 SSL certificate to realize SM2 https encryption, cloud WAF protection, CDN high-speed content distribution service, multi-dimensional protecting of website security.

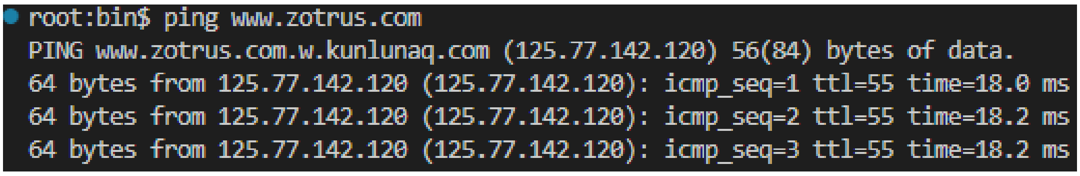


[CN] ZoTrus Technology Limited | https://www.zotrus.com

Cybersecurity Protection Compliant

Protected by Alibaba Cloud WAF

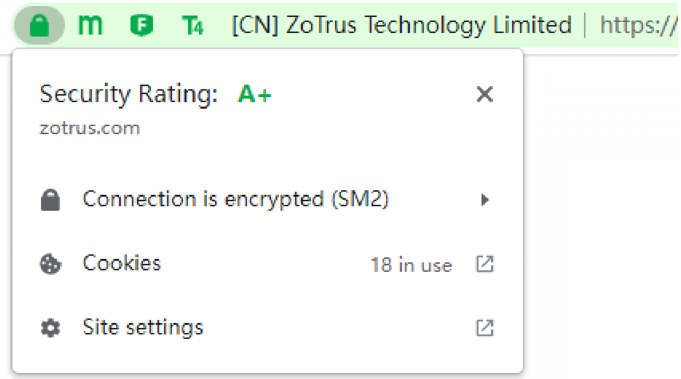
Learn more



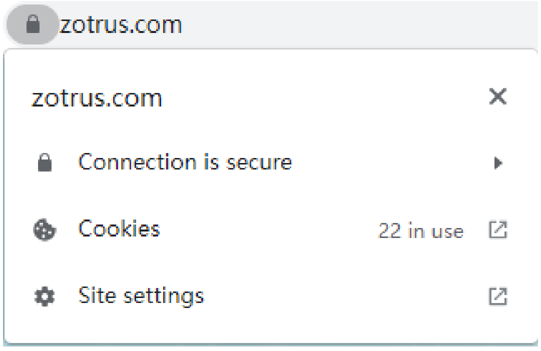
```
root:bin$ ping www.zotrus.com
PING www.zotrus.com.w.kunlunaq.com (125.77.142.120) 56(84) bytes of data.
64 bytes from 125.77.142.120 (125.77.142.120): icmp_seq=1 ttl=55 time=18.0 ms
64 bytes from 125.77.142.120 (125.77.142.120): icmp_seq=2 ttl=55 time=18.2 ms
64 bytes from 125.77.142.120 (125.77.142.120): icmp_seq=3 ttl=55 time=18.2 ms
```

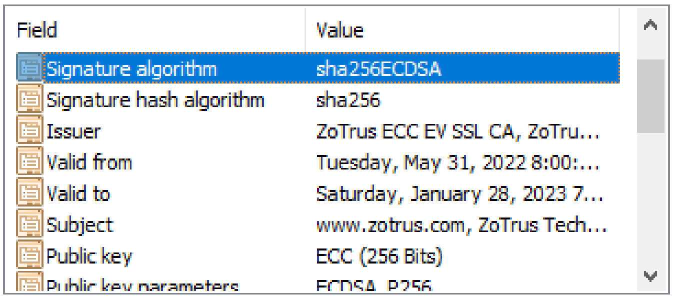
4.4 Experience what the dual-certificate adaptive encryption algorithm https encryption looks like.

Some readers may say: very good, the official website of ZoTrus has deployed SM2 SSL certificate that supports SM2 certificate transparency to implement SM2 https encryption, but if I use a Google Chrome that does not support SM2 algorithm, can I still access ZoTrus official website? Of course, you can. As shown in the left figure below, this is a screenshot of using ZT Browser to access the ZoTrus official website, click the padlock icon, it displays "Connection is encrypted (SM2)", which means that the connection with the server adopts the SM2 algorithm to realize https encryption. As shown in the middle picture below, this is a screenshot of using Google Chrome to access the official website of ZoTrus. Click the padlock icon, and it displays "Connection is secure". If you continue to view the certificate, you can see that this is an ECC SSL certificate. That is to say, the dual-algorithm dual-SSL certificate deployed on the ZoTrus official website will implement https encryption according to the user's browser to realize auto-adaptive encryption algorithms. This is the best https encryption deployment practice, which guarantees the website's cryptography compliance requirements, guarantees that the website will not be affected by the revocation of the RSA/ECC SSL certificate under unforeseen and uncontrollable circumstances, and guarantees the maximum compatible, allowing all browsers to achieve a seamless https encryption experience.



[CN] ZoTrus Technology Limited | https://
Security Rating: A+
zotrus.com
Connection is encrypted (SM2)
Cookies
18 in use
Site settings





Field	Value
Signature algorithm	sha256ECDSA
Signature hash algorithm	sha256
Issuer	ZoTrus ECC EV SSL CA, ZoTru...
Valid from	Tuesday, May 31, 2022 8:00:...
Valid to	Saturday, January 28, 2023 7...
Subject	www.zotrus.com, ZoTrus Tech...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256

Richard Wang

October 06, 2022
In Shenzhen, China