The things about SM2 SSL certificate

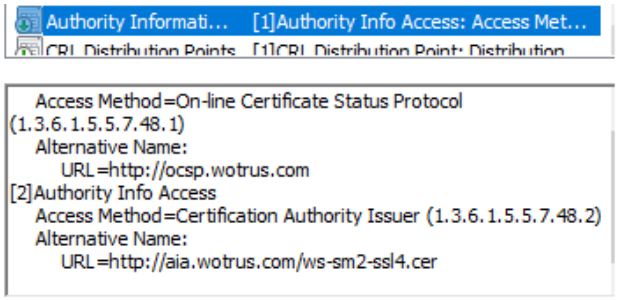
The first product released by ZoTrus Technology is ZT Browser, one of the biggest highlights is to support the SM2 SSL certificate to realize the SM2 HTTPS encryption. ZT Browser is developed based on the open-source project Chromium. The most important change is to add full support for SM2 SSL certificate, which support the SM2/SM3/SM4 algorithms and two SM2 standard specifications of "GM/T 0024 SSL VPN Technical Specifications" and "GB/T38636-2020 Information Security Technology Transport Layer Cryptography Protocol (TLCP)". Of course, the more important thing is to include the SM2 root certificates. This article will talk about this matter.

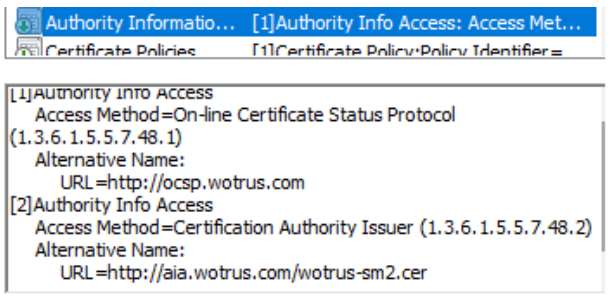
In order to allow browser users to fully experience the ZT Browser's support for the SM2 SSL certificate, we plan to include the SM2 root certificate of several CAs that have issued many SM2 SSL certificates when the browser is officially released. In the process of the application for the SM2 root certificate submitted by various CA operators, we found that there are still many issues in the SM2 SSL certificate issued by these CA operators, and there is still a lot of room for improvement. I hope this article can help to improve the technical level of the SM2 SSL certificate related parties, including the CA operators issuing the SM2 SSL certificate, the user deploying the SM2 SSL certificate, the SM2 browser manufacturer, etc. Everyone works together to improve the quality of SM2 SSL certificate's technical level and application level.

The first issue is the end user certificate and the issuing CA certificate do not have AIA information.

AIA is the abbreviation of Authority Info Access, which means the certificate issuer information access URL, which is used to tell the browser which issuing CA issued this certificate, and where to download the issuer certificate to verify whether the user certificate is really issued by this issuing CA, this information must be included in the end user certificate so that the browser can get the certificate issuer's public key to verify the end user certificate. Of course, the issuing CA must also have AIA information, so that the browser can verify whether the issuing CA is issued by an included trusted

root certificate. As shown in the figure below, the left picture is the end user certificate AIA of WoTrus CA that have AIA info, and the right picture is the AIA of issuing CA.





We regret to see that there are many end user certificates issued by CA operators that applied for inclusion by ZT Browser do not have AIA info, and the issuing CAs also do not have, so even if the root certificate is included and trusted, the browser cannot display it as trusted certificate because it cannot be verified. Some end user certificates have AIA information but cannot be accessed. Please make sure that the AIA URL is accessible, and the issuing CA certificate is correct.

Second issue is the end user certificates do not have a validation level identification OID.

International standards define the OIDs of 4 different certification validation levels of SSL certificates, DV SSL certificate OID: 2.23.140.1.2.1, IV SSL certificate OID: 2.23.140.1.2.3, OV SSL certificate OID: 2.23.140.1.2.2, EV SSL certificate OID: 2.23.140.1.1, these OIDs in the policy of the SSL certificate can make the browser know the validation level of the SSL certificate by reading these OIDs, and can display different UI according to different validation level such as EV SSL Certificates display a green address bar and organization name.

However, we found that only the SM2 SSL certificates issued by some CAs have these OIDs, and most of the SM2 SSL certificates do not contain these OIDs. Perhaps it is not appropriate to use these OIDs, because these OIDs defined by CA/Browser Forum clearly stated that these OIDs are only applicable to SSL certificates issued in accordance with relevant international standards, and the current SM2 algorithm has not been incorporated into CA-related international standards. That said, it should be inappropriate to use these OIDs for SM2 SSL certificate, although the CA/Browser Forum may not say something.

How to do? First of all, it is hoped that the State Cryptography Administration can define 4 OIDs from the OID architecture used by the National SM2 Root as soon as possible to define the validation level of the certificate. Of course, this may not be able to solve the thirst of the near future. Therefore, ZT Browser Trusted Root Program defines 4 OIDs for different validation levels. CA operators can use these OIDs for free to identify different validation level of SSL certificates, specifically: DV SSL certificate: 1.2.156.157933.11, corresponding to the CA/Browser Forum OID: 2.23.140.1.2.1; IV SSL certificate: 1.2.156.157933.12, corresponding to the CA/Browser Forum OID: 2.23.140.1.2.3; OV SSL certificate: 1.2.156.157933.13, corresponding to the CA/Browser Forum OID: 2.23.140.1.2.2; EV SSL certificate: 1.2.156.157933.14, corresponding to the CA/Browser Forum OID: 2.23.140.1.1. With these OIDs, browsers can accurately identify the validation level of the SM2 SSL certificate, so that different user interfaces can be displayed correctly.

Third issue is end user certificate has no Enhanced Key Usage, no revocation list (CRL and OCSP), no subject alternative name.

These are problems that shouldn't be there, but unfortunately some CA issued SM2 SSL certificate do not have Enhanced Key Usage (EKU), which is a must: server authentication (1.3.6.1.5.5.7.3.1) and Client authentication (1.3.6.1.5.5.7.3.2), only with these two EKUs can this certificate be proved to be an SSL certificate, so this is a must.

Of course, the revocation list is also necessary. It can be only CRL or only OCSP. There must be one or both, so that the browser can verify whether the certificate is valid and whether it is revoked. The subject alternative name is also required, otherwise the browser will not be able to obtain the domain name information bound to the certificate normally and will not be able to display the SSL certificate correctly.

The fourth issue is the user deploys the SSL certificate without the issuing CA certificate.

This problem is that the CA operator needs to remind users that when deploying the SM2 SSL certificate, they must include the issuing CA certificate in the web server, so that the browser can get the issued CA certificate when shaking hands with the web server and does not need to get it from

the AIA URL, to quickly verify whether the SSL certificate is trusted. If some CAs cannot add AIA URL to end user certificates in a short time, end users must be required to install the issuing CA certificate when deploying SSL certificate, which is also a temporary remedy. It is recommended that CA provide users with the commonly used web server certificate files binding the issuing CA certificates. For example, the Nginx web server just superimposes the issuing CA certificate and the user certificate. Please note: There is no need to add the root CA certificate and adding it will increase the data of the SSL handshake, reduce the communication efficiency, and increase the server bandwidth consumption.

Today, I talked about above four things, and 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. It is hoped that the four issues mentioned in this article will attract the attention of CA operators that issue SM2 certificates and users who use SM2 SSL certificates. Improving these issues will help browsers to quickly verify whether the certificate is trusted and correctly display the certificate's identity validation level, while also improving the browser user experience.

Since 2018, the author proposed to vigorously promote the application of the SM2 SSL certificate, and it is a dual-algorithm and dual certificate deployment adaptive encryption solution, which was called the "dual system" at that time. The deployment volume has grown from scratch, from small to large, and has been developing rapidly. Here I recommend 5 websites that have deployed the SM2 SSL certificate. You can download the ZT Browser to experience what the SM2 encryption is like: The first website is the official website of the Jiangxi Provincial Government website: https://www.jiangxi.gov.cn, the second website is the Anhui Provincial Government website: https://www.ah.gov.cn, the third website is the Shanghai Cryptographic Administration Bureau website: https://mgj.sh.gov.cn, the fourth website is the official website of Credit China (Jiangxi): https://www.creditjx.gov.cn. These four websites are all deploying SM2/RSA dual-SSL certificate for adaptive encryption, using ZT Browser to visit will use the SM2 algorithm encryption preferentially, but using other browsers don’t have this effect. The fifth website is the online banking service of Bank of China: https://ebssec.boc.cn, which is a website that only deploys the SM2 SSL certificate. If you are using a browser that don’t supports SM2 algorithm, the browser will prompt "Accidentally terminated the connection", don't think this is a problem with the website, it is because

the browser you are using does not support SM2 algorithm. Please use the ZT Browser to visit, it will be able to be accessed, and ZT Browser will display an icon in the address bar and prominently indicates that this website is encrypted with the SM2 algorithm.

Finally, the author hopes that the State Cryptography Administration can release the CA baseline requirement for SM2 SSL certificate in a timely manner and regulate the issuance and use of the SM2 SSL certificate. And I hope that all parties involved in the SM2 SSL certificate can work together, make good use of the SM2 SSL certificate, and jointly contribute to the popularization of the application of the SM2 SSL certificate, so that the SM2 SSL certificate can truly play the greatest role in ensuring China Internet security, and then effectively promote the international acceptance and use of the SM2/SM3/SM4 algorithm that has become an international standard, and jointly promote the early incorporation of the SM2 algorithm into the international standards related to SSL certificates, so that users can freely choose SSL certificates with RSA/ECC/SM2 algorithms as soon as possible like currently freely choosing RSA/ECC algorithms without deploying two SSL certificates with different algorithms. I firmly believe that this day will come, and I look forward to it coming soon through everyone's efforts.

Richard Wang

June 1, 2022
In Shenzhen, China