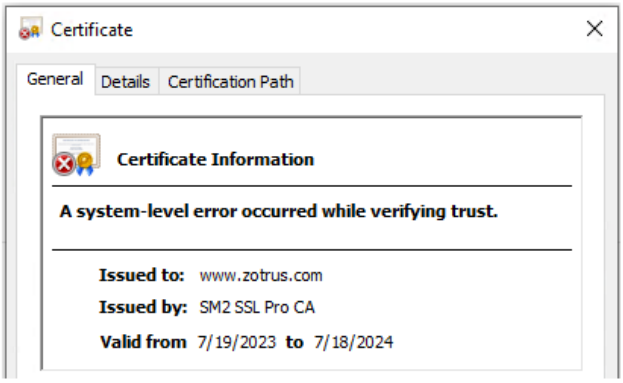
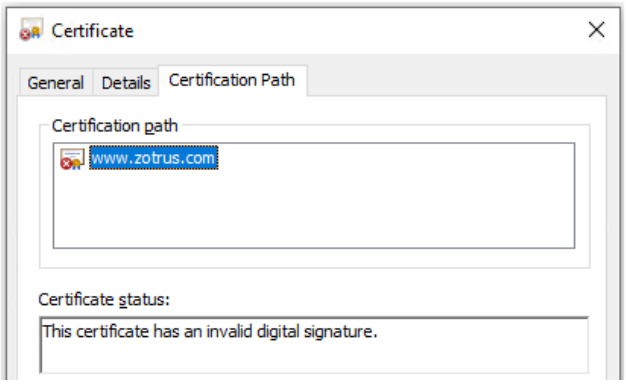
ZT Browser Patches the SM2 Algorithm for Windows

This is a big event that benefits the people in China and in the world, so the author must write an article to talk about it. In this article, readers will first be asked to take a look at how Windows currently displays the SM2 SSL certificate, and then take a look at how Windows displays the SM2 SSL certificate after installing the latest version 2401 of ZT Browser released today, and finally talk about the importance of this matter - benefiting the global Internet security.

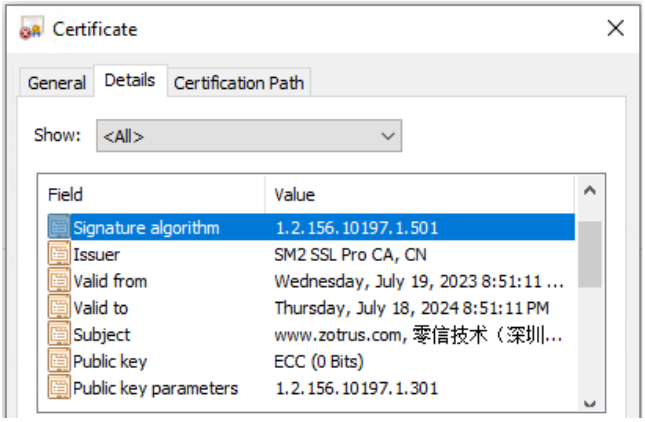
1. How does Windows display the SM2 SSL certificate?

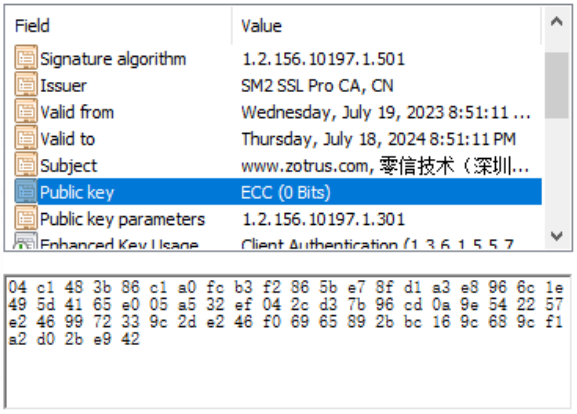
Windows does not support the China Commercial Cryptography Algorithm-SM2, which every Chinese can understand since it is not a made-in-China operating system, and even everyone can accept this reality with peace of mind. Since April 4, 2019, when the author created the first SM2 algorithm SSL root CA certificate, the author has been thinking that how good it would be if Windows could support SM2 algorithms. 5 years have passed, the author did not see that Windows supports the SM2 algorithm, click on the SM2 SSL certificate, although the certificate viewer can normally display the certificate binding domain name, issuer and certificate validity information, but because the SM2 algorithm cannot be recognized, it still shows "A system level error occurred while verifying trust", see below left figure. This message is very accurate, it is indeed Windows does not support the SM2 algorithm at the system level. As shown in the figure on the right below, click “Certification Path”, only the domain name bound to this SSL certificate can be displayed, but the certification path is not displayed, and the certificate status is "This certificate has an invalid digital signature". This is definitely a false positive! This SM2 SSL certificate must have a valid digital signature, but Windows cannot verify this digital signature.





Continue to check the certificate details, as shown in the left figure below, the "Signing algorithm" field shows OID: 1.2.156.10197.1.501, and the "Public key parameters" field also shows OID: 1.2.156.10197.1.501, instead of displaying the algorithm name "sha256RSA" and RSA (2048 bits) like the RSA algorithm SSL certificate. Since the SM2 algorithm is also an elliptic curve algorithm (ECC), Windows can recognize the public key of the SM2 SSL certificate as the ECC algorithm, but because it cannot recognize the elliptic curve parameters, the public key length shows 0 bits, but it is actually 256 bits, and the data of each byte can be displayed correctly, as shown in the figure on the right.





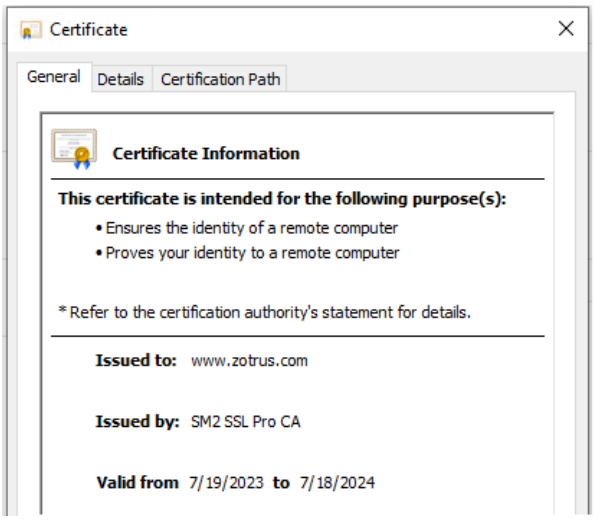
2. After ZT Browser patches Windows, how will the SM2 SSL certificate be displayed?

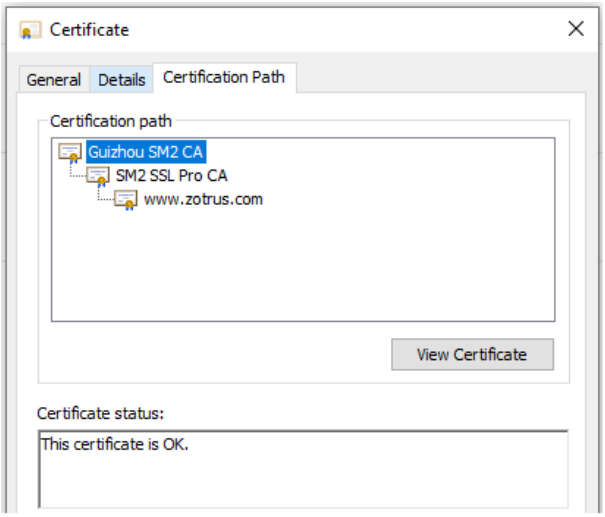
In June 2021, the author re-started his business, and in the past three years, the author has led the R&D team to create three commercial cryptography application ecosystems: the SM2 Certificate Transparent Ecosystem, the SM2 certificate automatic management ecosystem, and the intranet SSL certificate application ecosystem, and created the indispensable core products in these three ecosystems, including: ZT Browser, ZoTrus SM2 Certificate Transparency Log, ZoTrus Cloud SSL Service System, ZoTrus SM2 Certificate Automation Service System, ZoTrus SM2 HTTPS Automation Gateway,

ZoTrus SM2 HTTPS Automation Cloud Service, CerSign SM2 SSL certificate and RSA/ECC SSL certificate (Internet SSL certificate and intranet SSL certificate), etc. However, the most widely used Windows system does not support the SM2 algorithm, and the SM2 SSL certificate and the USB Key SM2 client certificate issued by China CAs cannot be displayed normally, which has always been a major event in the author's mind.

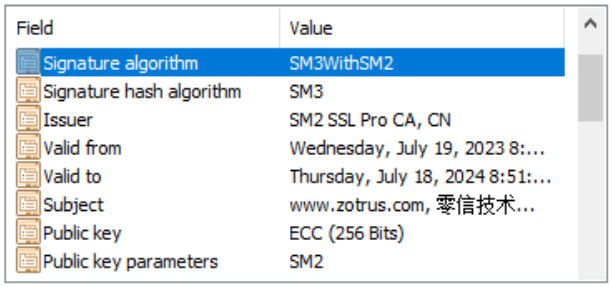
It wasn't until ZT Browser released the 2311 version that supported the SM2 client certificate authentication for USB Key certificates that the author decided to develop a Windows patch, so that Windows can support the verification of SM2 algorithm certificates, and can display SM2 algorithm certificates normally like RSA algorithm certificates, and can make the browser pop up SM2 certificates to complete two-way authentication like RSA client certificates, instead of the current USB Key manufacturers programming and implementing them themselves or not at all.

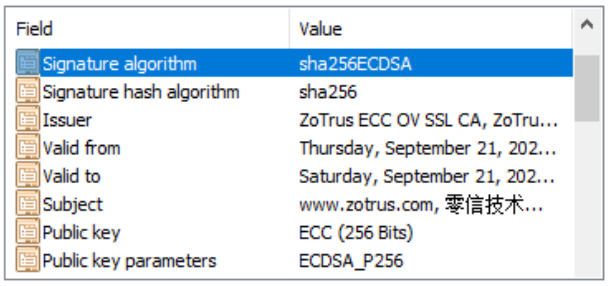
Today, ZT Browser released version 2401, starting from this version, ZT Browser will automatically patch Windows after installation, so that Windows can complete the SM2 algorithm certificate verification and normal display like supporting RSA/ECC algorithm certificates, as shown in the figure on the left below, Windows can display the general information of the certificate normally, and will not prompt the failure to verify the trust relationship. As shown in the figure on the right below, the Certification Path is displayed normally, and the certificate status shows "This certificate is OK". Please note that this is the certificate verification information displayed by the certificate viewer after Windows supports the SM2 algorithm, not prompted by ZT Browser, which has displayed the SM2 SSL certificate normally in the browser when it is released.



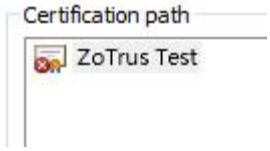


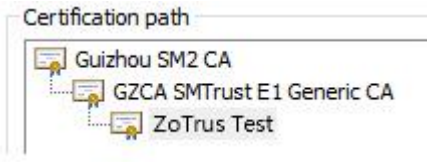
Continue to view the certificate details, as shown in the figure on the left below, the Signature algorithm is "SM3WithSM2", the Signature hash algorithm is SM3, the Public key is ECC (256 bits), and the Public key parameters is SM2, all of which are correct. For ECC algorithm SSL certificate, the details are shown in the figure on the right below, it can be seen that Window can display the SM2 algorithm SSL certificate like the ECC algorithm SSL certificate, which are all ECC (256 bits) public keys, and the public key parameters are displayed as SM2 and ECDSA_P256 respectively, because the only difference between the SM2 algorithm and the ECDSA_P256 algorithm is that different elliptic curve parameters are used.

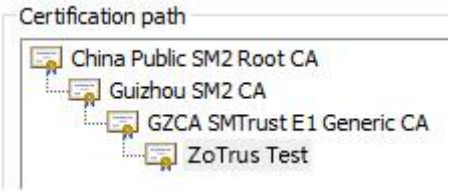




Of course, not only can it display the SM2 SSL certificate, but it can also display the USB Key certificate issued by China CA normally, as shown in the figure on the left below, which is the display of the user certificate issued by the Guizhou CA before the patching, and the certificate chain cannot be displayed normally. After installing ZT Browser, as shown in the figure below, the three-level certificate chain of the user certificate can be displayed normally, and the two-way authentication of the SM2 certificate can be normally supported. If the user computer does not have the Guizhou CA SM2 root CA certificate installed, the 4-level certificate chain with the China Pubic SM2 Root CA as the top-level root is displayed, as shown in the following figure on the right.







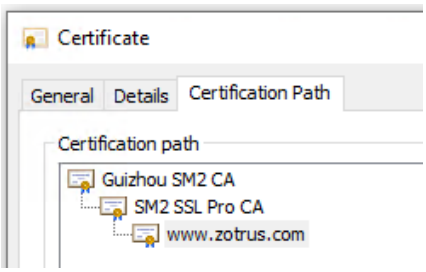
3. What is the greatest significance of Windows supporting the SM2 algorithm?

ZT Browser has patched the SM2 algorithm support patch for Windows, which not only greatly facilitates Chinese users to view SM2 algorithm digital certificates, including SM2 SSL certificates,

SM2 client certificates, SM2 email certificates, SM2 code signing certificates and SM2 document signing certificates, but more importantly, it allows Windows to handle SM2 algorithm certificates like RSA/ECC algorithm digital certificates. Take full advantage of the powerful certificate application capabilities of Windows to support various SM2 algorithm certificate applications, such as the most commonly used two-way authentication. That's one of the significances.

The second significance is that it greatly facilitates global users to know and understand SM2 algorithm digital certificates, especially SM2 SSL certificates, because if users see a certificate Windows displayed as "A system level error occurred while verifying trust" and "This certificate has an invalid digital signature", the first feeling is that there is a problem with this certificate, so as to increase vigilance and will not pay attention to this certificate, which is not conducive to let global users to know the SM2 algorithms.

ZT Browser users have covered users in more than 100 countries and regions around the world, after ZT Browser patches the SM2 algorithm for Windows this time, global users can not only know the SM2 algorithm SSL certificate in the address bar of ZT Browser, but also make Windows display the certificate chain and certificate details normally after downloading this certificate, which is very convenient for global users to know and understand SM2 algorithm SSL certificate. It is conducive to the global application of this cryptographic algorithm, which has become an ISO standard, so that global users have a new choice other than the RSA algorithm, and this provides an optional China cryptographic algorithm scheme for global Internet users, so that the SM2 algorithm and RSA algorithm work together to ensure global Internet security.



4. Welcome to use ZT Browser to let your computer perfectly supports the SM2 algorithm

With its excellent performance, rich functions and comprehensive support for SM2 algorithms, ZT

Browser has not only won the love of Chinese users, and it also become the No. 1 market share SM2 browser in China market. Moreover, due to the world's exclusive support for green address bar for EV SSL certificate, the display of website WAF protection icon, the support for real-time verification of PDF document digital signatures and the display of the signer's trusted identity, the special display of certificate transparency and other features, it has been welcomed by users in more than 100 countries and regions around the world, and the number of global users is rising rapidly.

The author strongly recommends that all new and old users download and install the latest 2401 version of ZT Browser, instead of upgrading the old version, so that Windows can perfectly support the SM2 algorithm, perfectly view the SM2 algorithm digital certificates, and perfectly realize the two-way authentication of the SM2 client certificate. And since Windows has perfectly supported the SM2 algorithm digital certificate, it is expected that more global software developers will develop more applications of SM2 certificates, and jointly contribute to the popularization of the SM2 algorithm, so that global users have more choices of cryptographic algorithms and use SM2 algorithm to ensure global Internet security.

Richard Wang

May 16, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.