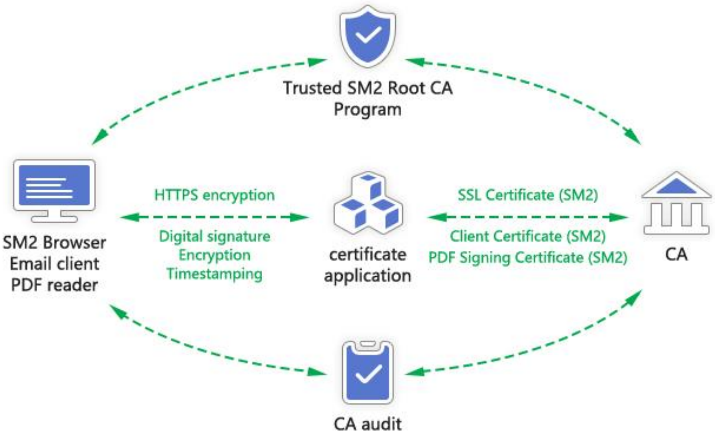
Popularize the application of SM2 SSL certificate, Starting from popularizing the use of SM2 browser

The conflict between Russia and Ukraine has led to the revocation of many SSL certificates for Russian government and banks, which has sounded the alarm for China Internet security, especially the security of China critical information infrastructure. The implementation of the "China Cryptography Law" is far-sighted, article 27 of the Law requires that China critical information infrastructure must be protected by commercial cryptography. However, as for how to use commercial cryptography for protection, there are no clear implementation policies. At present, each cryptographic product manufacturer can only justify his own explanation that the use and deployment of their products can meet the compliance requirements of the "Cryptography Law". This article provides our views and ideas on the cryptography compliance of SSL certificate and HTTPS encryption.

SSL certificate is the bottom plate product of Internet security (according to the barrel theory), HTTPS encryption is the core base technology of Internet security, and the Internet used cleartext transmission protocol when it was invented and came out, not only the widely used Web protocol - HTTP protocol is cleartext transmission, which is the Internet's largest traffic, and the second largest email MIME protocol is also cleartext transmission including SMTP protocol and IMAP protocol. These insecure cleartext transmission protocols have been continuously improved into encrypted transmission protocols, namely HTTPS protocol, and S/MIME protocol. The "S" in the names of these protocols means "Secure".

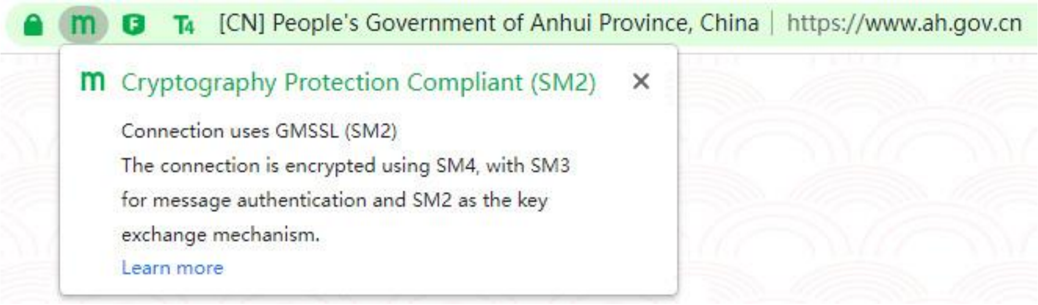
At present, the widely used HTTPS encryption protocol and SSL certificate both use RSA algorithm and ECC algorithm, which is a foreign algorithm. In order to protect China Internet security and information system security, China has launched its own cryptographic algorithm, which is the SM2 algorithm, including the SM3 algorithm for message authentication and the SM4 algorithm for encryption. The SM2 algorithm issued SSL certificate called “SM2 SSL certificate”, this is for making the difference from the RSA and ECC algorithm issued SSL certificate.

To implement HTTPS encryption, must have a CA to issue SSL certificate, have a browser trusts the root certificate that issues the SSL certificate, a Web server supports the algorithm used to issue this SSL certificate, and a browser that supports this algorithm can be used to realize HTTPS encryption. That is to say, only browsers (including mobile Apps), SSL certificates and web servers support the SM2 algorithm, can SM2 HTTPS encryption be realized, which is to establish a SM2 algorithm certificate application ecology. As early as the "2018 Cyberspace Trust Summit" (December 17-18, 2018) sponsored by the China Electronics and Information Industry Development Research Institute under the guidance of the Cybersecurity Coordination Bureau of the Cyberspace Administration of China and the State Cryptography Administration of China, the author put forward the proposal of "China Cyberspace Trusted Ecological Construction Framework", this is a complete ecological concept for the application of SM2 algorithm certificates. Now, it still seems very forward-looking. The author is also very happy to see that due to the implementation of the "Cryptography Law", this ecological concept has become reality that it is being accelerated in China.



One of the most important applications in this ecology is the SM2 HTTPS encryption, and the first component to realize the SM2 HTTPS encryption is the SM2 browser. If the browser does not support the SM2 algorithm and the SM2 SSL certificate, then there is no application base even the CA is able to issue the SM2 SSL certificate. This is why the first product launched by ZoTrus Technology is the ZT Browser that fully supports the SM2 algorithm and the SM2 SSL certificate. This is a completely free SM2 browser that follows the general browser business mode. At the time of release, the SM2 root certificates of 8 CA operators and the National SM2 Root Certificate have been included and trusted.

ZT Browser is based on the open-source Chromium project, mainly adding support for SM2 algorithm and SM2 SSL certificate, and especially innovatively adding a SM2 encryption icon “m” in the address bar, click on the SM2 encryption icon, it displays " Cryptography Protection Compliant". This display is to put forward our understanding and interpretation of the compliance of the "Cryptography Law" in terms of HTTPS encryption protection. As long as the website deploys the SM2 SSL certificate trusted by ZT Browser, ZT Browser will give priority to using the SM2 algorithm to realize HTTPS encryption, that is the use of commercial cryptography for protection, which is to meet the compliance requirements of the "Cryptography Law", that is, to meet the compliance requirements of cryptography protection, the ZT Browser clearly informs website visitors that this website is a cryptography protection compliant, clear at a glance, and does not need more explanation, which is also an innovation.



[CN] People's Government of Anhui Province, China | https://www.ah.gov.cn

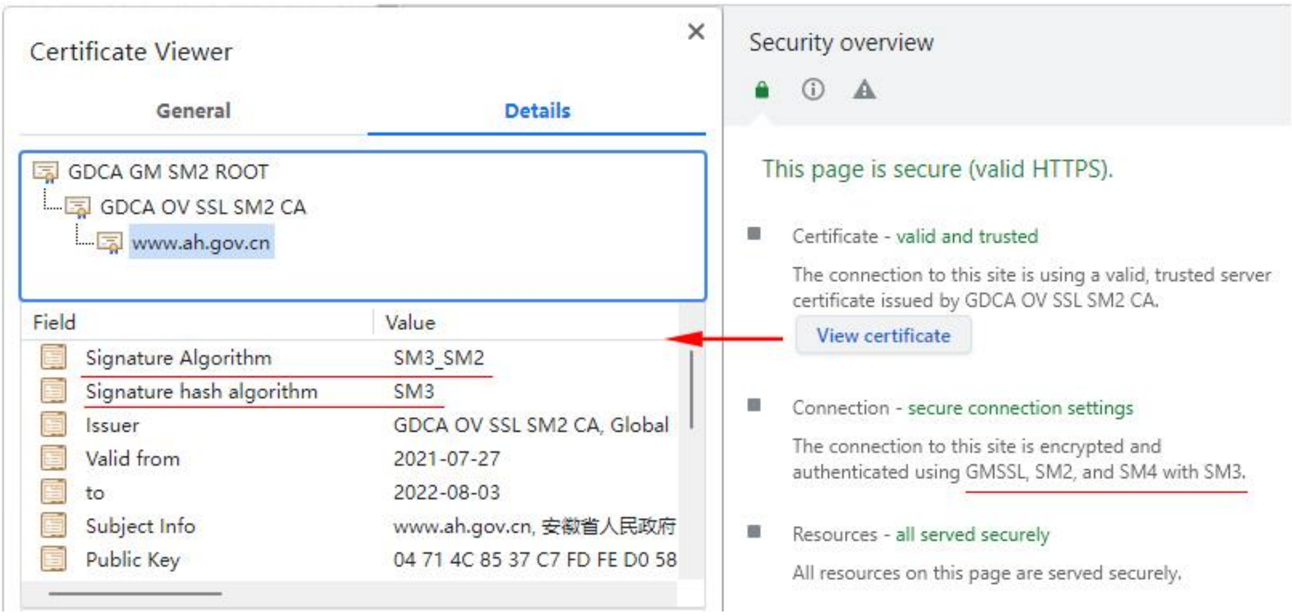
m Cryptography Protection Compliant (SM2) ×

Connection uses GMSSL (SM2)

The connection is encrypted using SM4, with SM3 for message authentication and SM2 as the key exchange mechanism.

Learn more

If we want to popularize the application of the SM2 SSL certificate, we must first popularize the use of the SM2 browser. Readers and friends are welcome to 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 m icon in the address bar. Welcome to experience the different SM2 https encryption!



Certificate Viewer

GDCA GM SM2 ROOT
GDCA OV SSL SM2 CA
www.ah.gov.cn

Field	Value
Signature Algorithm	SM3_SM2
Signature hash algorithm	SM3
Issuer	GDCA OV SSL SM2 CA, Global
Valid from	2021-07-27
to	2022-08-03
Subject Info	www.ah.gov.cn, 安徽省人民政府
Public Key	04 71 4C 85 37 C7 FD FE D0 58

Security overview

This page is secure (valid HTTPS).

- Certificate - valid and trusted

  The connection to this site is using a valid, trusted server certificate issued by GDCA OV SSL SM2 CA.

- Connection - secure connection settings

  The connection to this site is encrypted and authenticated using GMSSL, SM2, and SM4 with SM3.

- Resources - all served securely

  All resources on this page are served securely.

Richard Wang

June 17, 2022
In Shenzhen, China