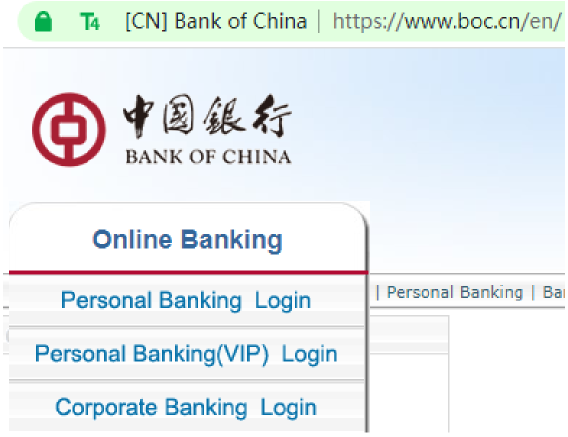
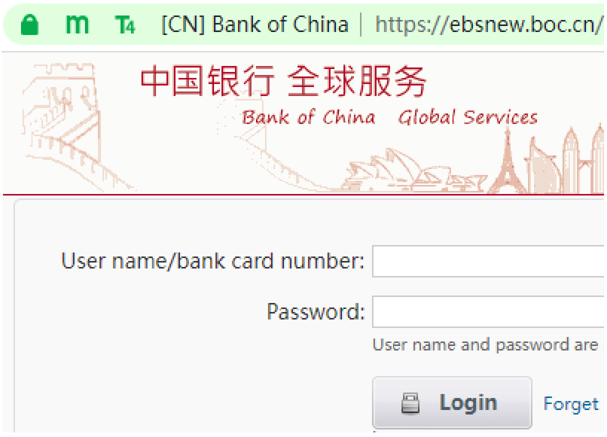
China online banking start to use SM2 algorithm https encryption

When I visited Bank of China’s personal online banking on the weekend, I found that HTTPS encryption has become a SM2 https encryption. ZT Browser address bar shows that the SM2 encryption icon **m** is displayed. I recommend readers download ZT Bowser to verify it, as shown in the right picture below.



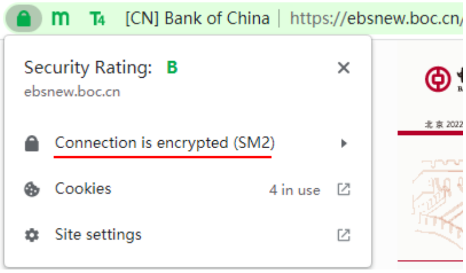
T4 [CN] Bank of China | https://www.boc.cn/en/



m T4 [CN] Bank of China | https://ebsnew.boc.cn/

中国银行 全球服务
Bank of China Global Services
User name/bank card number:
Password:
User name and password are
Login
Forget

Click the padlock icon to see "Connection is encrypted (SM2)". Click to view the certificate to see that this is a SM2 algorithm SSL certificate issued by CFCA on July 12, 2022, which is trusted by ZT Browser. And if the reader uses a Google Chrome that does not support SM2 SSL certificate to visit personal online banking, the padlock icon will also be displayed. Click to view the certificate to see that this is an RSA algorithm SSL certificate, see below the right picture.



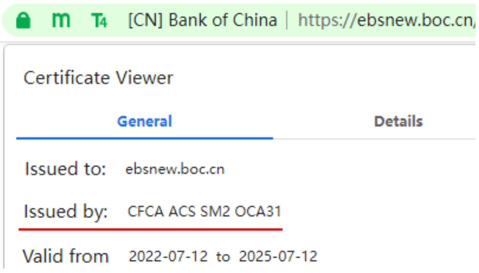
m T4 [CN] Bank of China | https://ebsnew.boc.cn/

Security Rating: B

ebsnew.boc.cn

Connection is encrypted (SM2)

Cookies 4 in use



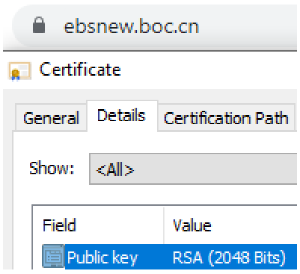
m T4 [CN] Bank of China | https://ebsnew.boc.cn/

Certificate Viewer

Issued to: ebsnew.boc.cn

Issued by: CFCA ACS SM2 OCA31

Valid from 2022-07-12 to 2025-07-12



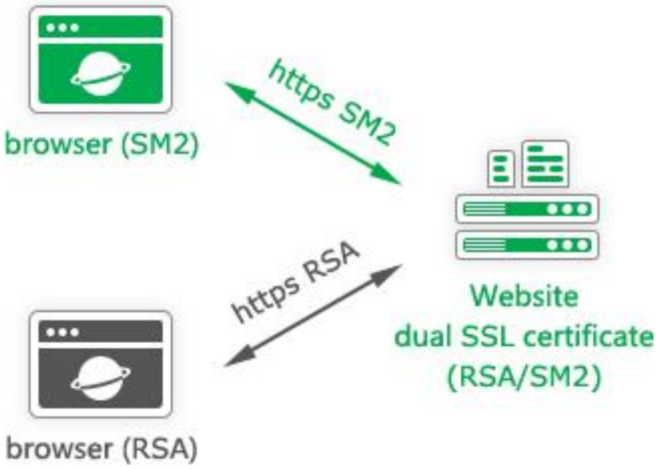
ebsnew.boc.cn

Certificate

Show: <All>

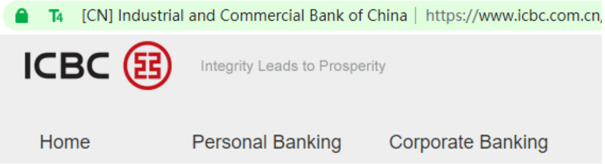
Field	Value
Public key	RSA (2048 Bits)

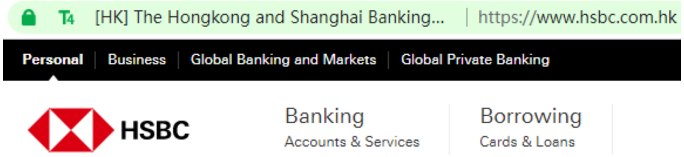
This illustrates that the personal online banking system of Bank of China is deployed with a dual SSL certificate, which realizes the dual algorithm self-adaptive HTTPS encryption. This is the best solution for the SM2 compliance and global trust, because the online banking system cannot restrict what the browser is required to use. Do not underestimate the huge role of this dual certificate deployment. Not only does the deployment is Cryptography Law compliance, but more importantly, this dual SSL certificate will play a great role at a certain time. For example, when the Russia-Ukraine conflict occur, many Russia's banks' online banking used RSA SSL certificate were revoked and the user could not access the online banking system normally. The dual SSL certificate adopted by Bank of China can easily cope with such emergencies! Because even if the RSA SSL certificate deployed by online banking is revoked or "no-supply", because the online banking system deployed SM2 SSL certificate, as long as the browser used by users is to support the SM2 algorithm and prioritize using SM2 algorithm for https encryption, then it is not aware that the RSA SSL certificate has been revoked, because the actual encrypted communication does not use this RSA SSL certificate but use SM2 SSL certificate to achieve HTTPS encryption communication!



This year is the last year of "The Cryptography Application and Innovation Development Plan for Financial and Important Fields (2018-2022)", this plan clearly requires efforts to promote the comprehensive application of cryptography in finance and important fields including the reconstruction and upgrade of financial information infrastructure and new financial services industry cryptography application in electronic payment such as online banking, mobile payment, barcode payment. The "cryptography application" mentioned here of course refers to the application of SM2 algorithm. The author is glad to see that the Bank of China's online banking system HTTPS encryption has realized the SM2 encryption application, which not only meets the requirements of the cryptography compliance, but also can truly effectively prevent the SSL certificate risk of online banking system.

Therefore, the author must praise the Bank of China. And the author also strongly recommends that readers and friends must use browsers to support SM2 algorithm to avoid the use of online banking cannot be available. It is recommended to download and use the completely free SM2 browser – ZT Browser, which not only prefer the SM2 encryption, but also display the green address bar with the bank name, so that users can recognize the authentic bank website at a glance to avoid losses in the fake bank website.


[CN] Industrial and Commercial Bank of China | https://www.icbc.com.cn,


[HK] The Hongkong and Shanghai Banking... | https://www.hsbc.com.hk

Richard Wang

August 1, 2022
In Shenzhen, China