SSL certificate automatic deployment,
### ensure uninterrupted https encryption of business system

Deploying SSL certificates has become a must for various business systems, and SSL certificate have a validity period, once expired, they cannot be used, which will definitely affect the normal operation of business systems. Let's first look at a real case that happened in December 2018, the mobile operator O2's mobile data management system crashed due to the expiration of the SSL certificate in Ericsson telecom equipment, which made its own 32 million customers and customers of other operators around the world could not use mobile communication services normally, and the business was interrupted for more than 20 hours before being restored. In this case, O2 sued Ericsson for millions of dollars. It can be seen how important it is to maintain the continuous validity of the SSL certificate required for key businesses, but it is a very big challenge for large organizations that need to maintain hundreds of web servers, facing the huge risk of unexpected expiration of SSL certificate, and the results of system failures and these failures may paralyze the system for a period of time will bring irreparable losses to the business and reputation of the enterprise.

With the in-depth implementation of "Cryptography Law", it has become must for deploying SM2 SSL certificate for critical information infrastructure systems. This brings new challenges to IT administrators because the deployment of the SM2 SSL certificate must first upgrade the web server to support the SM2 algorithm. And in order to be compatible with all browsers, it is necessary to deploy a globally trusted SSL certificate at the same time. It is indeed a big challenge to upgrade the system and deploy dual algorithm SSL certificate, especially if you want to manage thousands or even tens of thousands of web servers in the e-government cloud platform. This cannot understand why a large number of e-government websites have not yet deployed SSL certificate, because deploying SSL certificates for thousands of websites is not an easy job, especially if it cannot affect the normal operation of existing systems that are running, let alone not to mention the need to renew and redeploy SSL certificates after they expire!

　　　　　　(C) 2023 **ZoTrus Technology Limited**

How to do? The only way is to automate certificate management. Fortunately, there is already an international standard for automatic certificate management - RFC 8555 (ACME). At present, there are already many CA operators that support the ACME standard in the market, and they have been a great success, because ACME automatic deployment completely free IT administrators from the tedious certificate application and deployment work, and due to the realization of automation, the risk of business interruption caused by human error and forgotten certificate renewal is greatly reduced or even eliminated.

However, International ACME standard does not support automatic deployment of SM2 SSL certificate, only support the international algorithm SSL certificates. How to do? The SM2 ACME Service launched today is to solve the problem of automatically deploying the SM2 SSL certificate. Of course, it also support the ECC SSL certificate that it is deployed at the same time, so that the website can automatically implement the adaptive encryption algorithm of https encryption to support all browsers. ZT Browser that support SM2 algorithm and SM2 Certificate Transparency automatically use SM2 algorithm to realize SM2 https encryption, and other browsers that do not support SM2 algorithm and SM2 Certificate Transparency use ECC algorithm to realize https encryption.

The SM2 ACME Service is jointly created by CerSign Technology and ZoTrus Technology, which completely solves the problem of automatic management of the SM2 SSL certificate and the ECC SSL certificate. Users only need to install the SM2 ACME client - SM2cerBot once, and it can automatically apply for and deploy a globally trusted ECC SSL certificate, a SM2 signing SSL certificate, and a SM2 encrypting SSL certificate, and automatically install the SM2 algorithm module to support the implementation of SM2 https encryption, one-click automatic deployment of dual-algorithm dual SSL certificates. It not only supports a completely free 90-day free SSL certificate, but also supports EV SSL certificate, OV SSL certificates and DV SSL certificates with a validity period of 1 year. These SSL certificates are all automatically configured dual-algorithm certificates. Welcome to download the SM2cerBot for free and enjoy the SM2 ACME service.
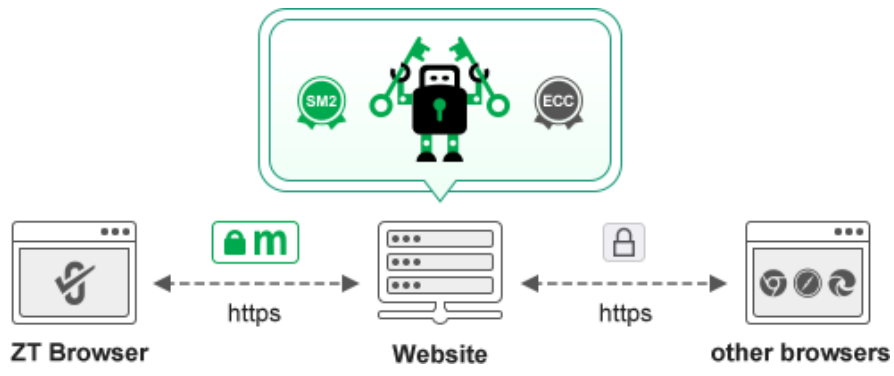
Richard Wang

Jan 06, 2023
In Shenzhen, China