The 90-day SSL certificate countdown begins, am I ready?

This is a question every IT people must ask himself! Including website owners, website administrators, CA owners, Internet service providers, cloud service providers, etc.

The validity period of the SSL certificate is now 365 days. Google Chrome updated its Root Program Policy on March 3, the most important one is the validity period of the SSL certificate will shorten to 90 days! Of course, the global CAs have a lot of opinions on this, thinking that this is a "market-disrupting move", but they cannot refute Google's reasons for proposing this plan. This is a promotion to improve the agility of the entire ecosystem, a revolution in security, stability, and simplicity. To shorten the validity period of SSL certificates to 90 days is intended to promote and accelerate the automatic certificate management of the entire ecosystem, the entire ecosystem supports ACME (Automated Certificate Management Environment, RFC8555).

This plan has a resounding theme - "Move Forward, Together", which lists six benefits of implementing automatic certificate management:

- promote ecosystem agility,
- increase resiliency for CA owners and website owners alike,
- help website owners address scale and complexity challenges related to certificate issuance,
- drive innovation through ongoing enhancements and support from an open community,
- ease the transition to quantum-resistant algorithms, and
- better position the Web PKI ecosystem to manage risk.

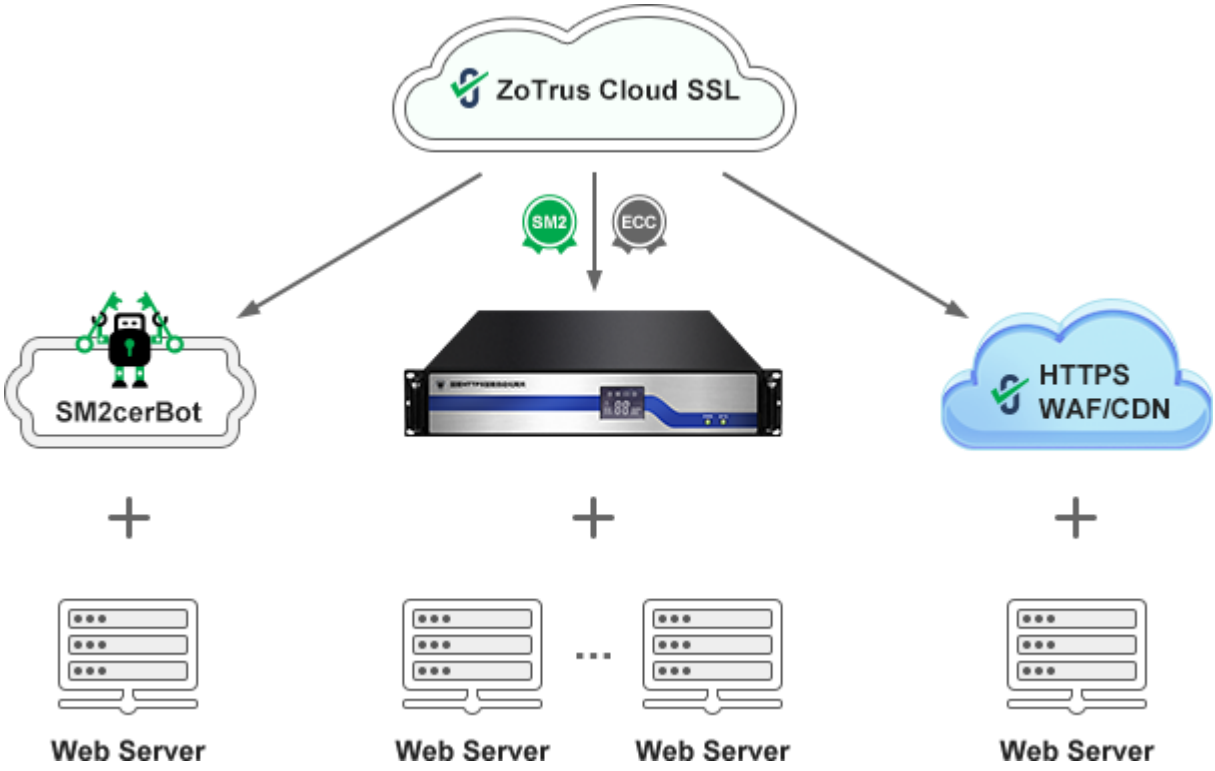
These six benefits are indeed very attractive and irresistible, how to do? The author thinks that this is not just a matter of the CA operators but should arouse the great attention of every SSL certificate user (website owner). 90 days means that I used to only need to enter the computer room once a year and install the SSL certificate once, but now I need to enter the computer room once a quarter and enter

the computer room 4 times a year. The author clearly tells everyone today that 90 days is not the end! Soon after 90 days is achieved, it will be 60 days, 30 days, 20 days, 10 days and so on. In fact, this is not terrible. As long as the automatic issuance and deployment of SSL certificates is realized, you will no longer care about the validity period of the certificate! Our SM2 ACME test website (https://sm2test.cersign.cn) is set to automatically issue and renew a new SSL certificate every day without any problems. Automation will definitely make it easier for you to remember to renew the SSL certificate in time than before, and there will never be a situation where the normal operation of the website system will be affected because of forgetting to renew the SSL certificate. This is not a bad thing! Take this step, the sea and the sky will be brighter, and you will completely get rid of the troubles of SSL certificate and enjoy the worry-free https encryption.

How to take this step? how to prepare before the upcoming 90-day SSL certificate countdown to zero? As early as 2021, ZoTrus Technology began to develop the fully automatic https encryption solution, and it automatically realizes SM2 https encryption! The author has participated in many times CA/Browser Forum face-to-face meetings since 2013, and deeply understand that international industry elites are planning and promoting automatic certificate management. The author firmly believe that the future of SSL certificates is automation, SSL certificate will be relegated from unattainable star products to the second tier, because what users need is https encryption, and they don't want to care or bother to manage SSL certificates.

The beautiful answer sheet handed over by ZoTrus Technology is a complete solution, a solution that can meet the needs of various users, a solution that is not just to install an ACME client software on the server – SM2 ACME client - SM2cerBot, there is also a solution that does not need to install software on the server, because some important servers cannot install third-party software. This is a solution for zero change of the original server: deploying the SM2 HTTPS Auto Gateway (hardware) or enabling the SM2 HTTPS Auto Cloud Service. The deployment of SM2 HTTPS Auto Gateway is very suitable for application scenarios where a large number of servers need to automatically deploy SSL certificates to realize https encryption, dual gateways support up to 255 websites. The SM2 HTTPS Auto Cloud Service is very suitable for users who do not want or cannot deploy hardware gateway devices in front of the servers. It only needs to do 3 domain name resolutions to realize https encryption automatically and adaptive encryption algorithm. The three innovative solutions of ZoTrus

Technology not only realize the automatic management of the RSA/ECC SSL certificates, but also realize the automatic management of the SM2 SSL certificates, and seamlessly realize the web server and other related systems SM2 transformation to support SM2 algorithm and SM2 SSL certificate to realize SM2 https encryption.



The three innovative solutions of ZoTrus Technology are all client-cloud integrated solutions, and they are all automatically connected to the ZoTrus Cloud SSL System through the SM2 ACME protocol, and automatically configure the SM2 SSL certificates and ECC SSL certificates, automatic deployment of dual SSL certificates, automatic renewal of dual SSL certificates, enabling websites to automatically implement https encryption with adaptive encryption algorithms. The ZT Browser that support SM2 algorithms and SM2 Certificate Transparency automatically uses SM2 algorithm realizes the SM2 https encryption, and other browsers that do not support SM2 algorithm and SM2 Certificate Transparency automatically use the RSA/ECC algorithm to realize https encryption, which allows users to enjoy https encryption services without worry, and users do not need to worry about the annoying SSL certificate will expire at some day! Even if Google will reduce the validity period of the SSL certificate to 1 day in the future, it will be able to deal with it freely!

The 90-day SSL certificate countdown has begun! The only thing we need to think about is which solution to adopt and start implementing it early, because we don't know when the countdown will end!

Richard Wang

April 21, 2023
In Shenzhen, China