SSL certificate validity period will be shortened to 47 days

This blog is released on December 9, 2024, updated on April 13, 2025:

According to the latest announcement from the CA/Browser Forum, the vote on Ballot SC-081v3: **Introduce Schedule of Reducing Validity and Data Reuse Periods** has been passed, and the schedule for shortening the validity period of SSL certificates is:

- From March 15, 2026, the validity period of the SSL certificate is shortened to 200 days.
- From March 15, 2027, the validity period of the SSL certificate is shortened to 100 days.
- From March 15, 2029, the validity period of the SSL certificate is shortened to 47 days.

One of the hot topics in the global Internet security community recently is the CA/Browser Forum ballot proposal by Apple on October 10 to shorten the validity period of SSL certificates to 45 days. The author wanted to write an article about it at that time but decided to wait and see the industry's reaction before talking about it. Two months have passed, and this matter has received strong reactions. So, it is time to write an article to talk about this matter.

1. Shortening the validity period of SSL certificates is inevitable, and the industry leaders are ready

The author have written two related articles before: "Google wants to "Move together" or "Remove" other CAs ?" and "The 90-day SSL certificate countdown begins, are you ready?". The author will not repeat them here, please refer to these two articles.

This article will talk about the latest situation. Google proposed to shorten the validity period of SSL certificates to 90 days in March last year. A year and a half later, Apple proposed a plan of 45 days! This is a step-by-step shortening process. It is planned to spend more than two years to gradually shorten the current certificate validity period from no more than 398 days to 45 days. The specific plan

is:

(1) From September 15, 2025, to September 14, 2026, the validity period of the SSL certificate is shortened to 200 days.
(2) From September 15, 2026, to April 14, 2027, the validity period of the SSL certificate is shortened to 100 days.
(3) Starting from April 15, 2027, the validity period of the SSL certificate will be shortened to 45 days.

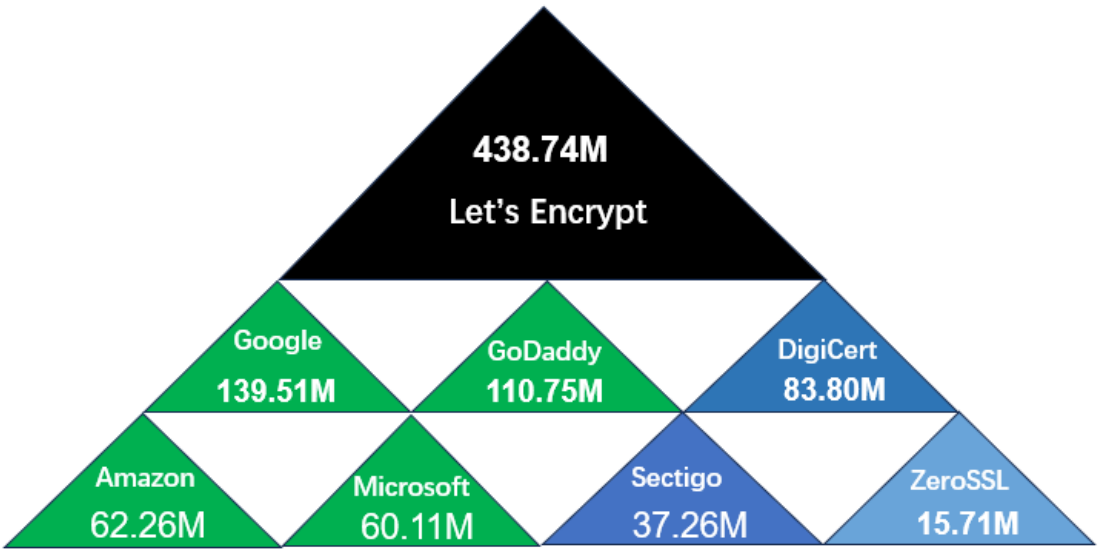
This proposal is slightly milder than Google's proposal to shorten the validity period from 398 days to 90 days. There is a gradual shortening process, but the final validity period is less than half of the 90 days proposed by Google. What does a 45-day validity period mean? Now certificates are applied for and installed once a year. If it is shortened to 45 days, certificates will have to be applied for and installed every month! It is estimated that operation and maintenance engineers will have to install certificates every day. This is why IT engineers around the world have come out to curse. Some people questioned Apple: In this proposal: Tell me you've never worked in IT without telling me you've never worked in IT. This is a popular Internet humorous saying from IT engineers. The author will not explain it. You can experience it for yourself.

In other words, the era of manually applying for and installing SSL certificates will come to an end on September 15 next year! Because the validity period of the SSL certificate is shortened to 200 days, that is, it has to be tossed at least twice a year, even if only a few websites can no longer be done manually, that is, there is only one way left: automation. Even if some people say that it is acceptable to install it once every six months, then only 100 days of SSL certificates can be issued on September 15, 2026, and it must be tossed at least 4 times a year, and it must be impossible to install the SSL certificate once a quarter. It's time to get ready for automatic certificate management ahead of time.

The proposal is currently on the agenda for discussion. How likely is it that the ballot will be passed? That depends on how determined Apple is. In 2020, Google, Apple, and Let’s Encrypt jointly proposed to shorten the validity period of SSL certificates from 825 days to 398 days. The CA/Browser Forum voted that this ballot did not pass because most CAs voted against it. However, Apple unilaterally

decided to only trust one-year certificate, and other browsers followed suit, so that even if this ballot did not pass, it was implemented, and the validity period of SSL certificates was shortened from 2 years to the current 1 year. Therefore, everyone should still believe that this will definitely come, not shortened to 90 days, but eventually shortened to 45 days!

In response to this big event, leading CAs and cloud service providers have already taken action. DigiCert and Sectigo have both launched their own SSL certificate lifecycle management solutions. The SSL certificate prices listed on DigiCert's official website are based on how much per domain name per month, while Sectigo plans to charge per domain name per year, rather than per certificate per year. The world's leading cloud service providers all support ACME's automatic configuration of SSL certificates. The latest ranking of the world's top eight SSL certificate providers and the number of certificates issued are shown in the figure below. The number of valid SSL certificates worldwide is 975.41 million, and more than 90% of SSL certificates have been automated. This is the confidence of Apple and Google in pushing to shorten the validity period of SSL certificates. As for whether the validity period is 90 days or 45 days, it is not a problem. As long as automation is achieved, automated issuance and deployment of SSL certificate with any validity period can be achieved.



Ranking of the world's top eight SSL certificate providers and certificate issuance volume (2024.12.6)

2. China IT industry should attach great importance to it and prepare in advance

99.99% of websites in China are still heavily dependent on RSA SSL certificates, China must attach great importance to these changes in SSL certificate standards that affect the normal operation of all government websites, online banking systems, and all critical information infrastructures, and prepare countermeasures in advance to avoid the inaccessibility of these important website systems.

Some people may say: Isn't China promoting the popularization of SM2 SSL certificates? If the SM2 SSL certificates are popularized, will this problem disappear? No, to ensure the security of SM2 algorithm HTTPS encryption, the SM2 SSL certificates should also implement the corresponding certificate validity policy in sync with international standards.

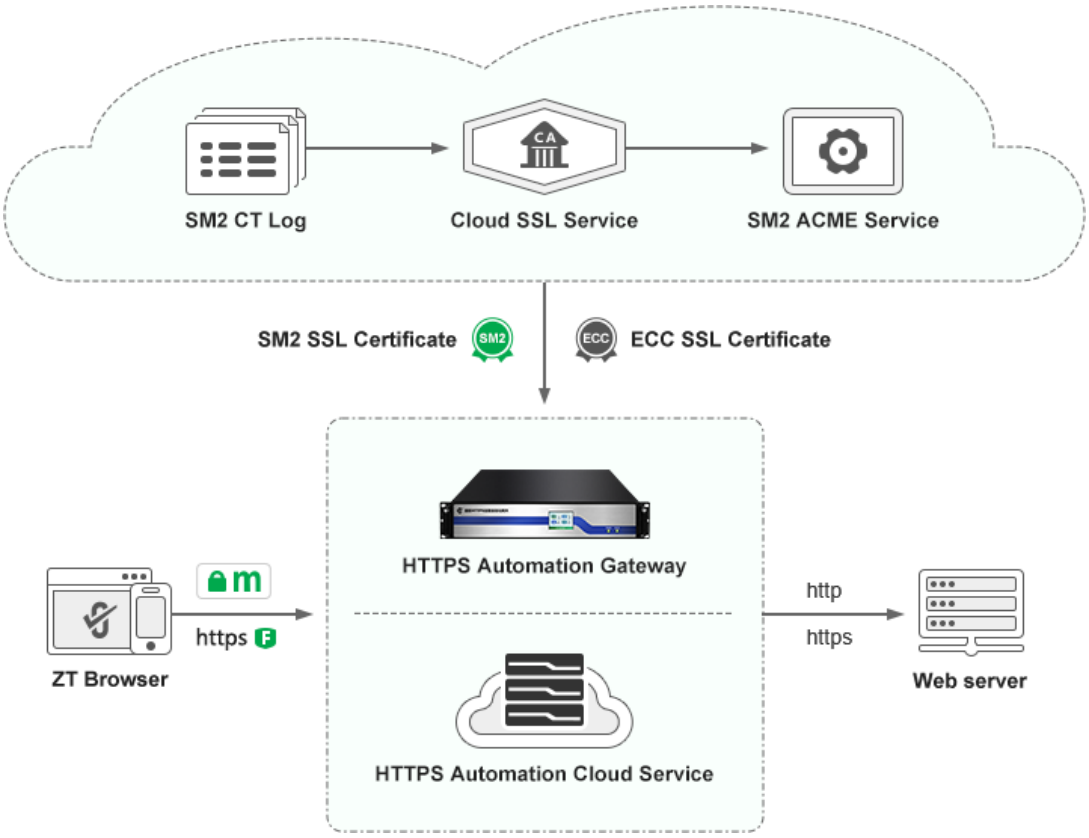
The purpose of shortening the validity period of SSL certificates is to further enhance the security of HTTPS encryption and prepare for the transition to quantum-resistant algorithms. The only feasible solution is to completely abandon the traditional method of manually applying for and deploying SSL certificates, and fully realize the automatic application and deployment of SSL certificates. For the SM2 HTTPS encryption reconstruction that is being promoted in China, it is necessary to promote the automatic application and deployment of SM2 SSL certificates. It is recommended that all SM2 algorithm reconstruction plans are the automatic solution that are directly implemented in one step, and the SM2 HTTPS encryption is automatically realized, instead of the traditional solution of manually deploying SM2 SSL certificates and installing SM2 algorithm modules.

This is a big event that concerns the entire IT industry. All applications that require SSL certificates to implement HTTPS encryption need to be upgraded and transformed to support automatic certificate management, including e-government systems, online banking systems, all other critical information systems, SSL VPN devices, WAF devices, WAF cloud services, CDN services, email services, IoT devices, all kind of gateway devices, etc. Otherwise, a large number of systems will be interrupted due to the expiration of SSL certificates and non-renewal. This big event must be taken seriously, and sufficient technical preparations must be made in advance.

3. ZoTrus Technology provides dual-algorithm SSL certificate automatic management solution

ZoTrus Technology focuses on dual-algorithm SSL certificate automatic management solutions, providing a complete line of HTTPS encryption automation products. It not only realizes the automatic management of RSA algorithm SSL certificates, but also realizes the automatic management of SM2 algorithm SSL certificates, to realize HTTPS encryption automation with zero modification of the original Web server and adaptive encryption algorithm. This is very import for these Web servers that cannot install ACME client software.

ZoTrus HTTPS encryption automation solution is a client-cloud integrated cryptographic application automation solution based on ZoTrus Cloud Cryptographic Infrastructure. Its core product is the ZoTrus HTTPS Automation Gateway. Unlike international automatic certificate management solution, it does not require to install ACME client software on the Web server, which is unrealistic in important e-government systems, online banking systems, and other critical information systems. Users do not need to install SM2 algorithm support module, do not need to install SSL certificates, do not need to purchase and apply for SSL certificates from CAs. All they need to do is deploy the ZoTrus HTTPS Automation Gateway in front of the original Web server. The ZoTrus HTTPS Automation Gateway automatically connects to the ZoTrus Cloud SSL Service System to complete the application and retrieval of dual-algorithm SSL certificates, and the ZoTrus Cloud SSL Service System connects to international CAs and China CAs to obtain globally trusted ECC algorithm SSL certificates and cryptographic compliant SM2 algorithm SSL certificates, implement dual SSL certificate deployment, and automatically implement HTTPS encryption and WAF protection.



The second core product is ZT Browser, which is currently the world's only completely free, high-performance browser based on the Chromium that supports SM2 algorithms, SM2 SSL certificates, and SM2 certificate transparency. It is a free supporting product for the ZoTrus HTTPS Automation Gateway. These two core products enable all websites to implement SM2 and RSA dual algorithm HTTPS encryption without any modification in Web server.

ZoTrus HTTPS Automation Gateway supports free automatic configuration of dual SSL certificates (SM2 OV SSL Certificate + ECC DV SSL Certificate) for up to 255 websites. It has achieved automatic update every 80 days and issuance of 90-day validity certificates. It supports daily certificate updates, which means that it already supports shortening the validity period of SSL certificates to 2 days, not just 45 days!

For users who only have a small number of websites that need to implement SSL certificate automation, they can purchase ZoTrus HTTPS Automation Cloud Service. This is an innovative cloud service that based ZoTrus HTTPS Automation Gateway on the cloud sharing it with up to 255 websites. Users do not need to purchase and deploy gateway hardware. They only need to do two domain name resolutions to automatically implement HTTPS encryption and WAF protection with adaptive encryption

algorithms. It also automatically configures each website with a dual-algorithm 90-day validity period SSL certificate that is automatically updated every 80 days.

The 45-day new policy is coming, which is not scary, because ZoTrus Technology has made sufficient technical preparations and can fully supply ZoTrus HTTPS Automation Gateway to realize HTTPS encryption automation and automatically realize WAF protection in HTTPS mode. For government websites, bank websites and all critical information system operating organizations, it is necessary to plan, prepare in advance, directly adopt the automatic certificate management solution, and realize the HTTPS encryption automation and WAF protection automation in one step. Only in this way can they avoid responding to the situation passively at that time, and avoid affecting the reliable operation and uninterrupted service of important information systems due to the expiration of SSL certificates. The 45-day new policy is not scary, and advance preparation is the key. Choose the right technical solution and realize automatic certificate management without reconstruction.

Richard Wang

December 9, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 82 articles in English (more than 105K words) and 195 articles in Chinese (more than 559K characters in total).