200 days! 100 days! 47 days!

Today, the CA/Browser Forum officially approved the SC-081v3 ballot - Introduce Schedule of Reducing Validity and Data Reuse Periods. Starting from March 15, 2026, the validity period of globally trusted SSL certificates will be shortened from the current one year to 200 days, 100 days and 47 days in three phases, and it is planned to be shortened to 10 days in the end! This article talks about what this huge change means to all stakeholders. Is it a crisis or an opportunity? It can be said that they are both. It depends on how everyone understands and responds to this huge change.

1. Why is SSL certificate validity period getting shorter and shorter? What impact does this have on the entire digital security industry?

The validity period of SSL certificates has been shortened from the early 5 years to 3 years, 2 years, and then to 1 year. The core demand for this continuous shortening of the validity period is to ensure the security of HTTPS encryption. Shortening the validity period of the certificate means shortening the life span of the private key, which means shortening the attacker's time and attack window, thereby minimizing the risk of potential threats and ensuring that the global Internet security infrastructure remains up to date.

Google first proposed to shorten the validity period of SSL certificates from the current one year to 90 days, aiming to promote ecosystem agility and easy transition to quantum-resistant algorithms. As a result, the CA/Browser Forum began a long discussion on the proposal, and Apple proposed an updated proposal to shorten the validity period of SSL certificates to 47 days on October 10, 2024 , and gave a phased implementation plan: shortened to 200 days on September 15, 2025, shortened to 100 days on September 15, 2026, and shortened to 47 days on April 15, 2027. This proposal ballot to shorten the validity period of certificates was passed on April 13, 2026, two years after Google first proposed it. The passed proposal was postponed for half a year compared to Apple's proposal, and the validity period of 47 days was postponed for two years: shortened to 200 days on March 15, 2026, shortened

to 100 days on March 15, 2027, and shortened to 47 days on March 15, 2029. This is a compromise solution for all stakeholders, but in any case, the boot that has been shouted for two years has finally fallen! Some users said that "the wolf has finally come."

The development of this standard represents a major turning point for the digital security industry: in an era of rapidly evolving cyber threats, static security measures with a validity period of one year are no longer sufficient, and agility and proactive risk management must be at the core of modern security strategies. CAs, corporate security teams, and IT administrators must reconsider this core point to ensure that critical information infrastructure can handle the increased pace of certificate renewals, maintain operational efficiency, and not affect the normal operation of business systems.

In addition to the technical impact, this shift also reflects that all industries are moving towards a security-first mindset. The reluctance to shorten the validity period of certificates is rooted in convenience, but convenience is no longer the main driver of security decisions. The implementation of the 47-day validity period SSL certificate policy is not just the formulation of a technical standard, but a signpost for the development of digital security. It marks the key to reducing risks, increasing agility, and promoting more resilient Internet security. Although the challenges are great, the long-term benefits of the implementation of this policy will far outweigh the current challenges, reinforcing the principle that security must always be put first in the era of the Internet of Things and AI.

2. What do the 200-day, 100-day, and 47-day certificate policies mean to users? How to respond?

For website owners, that is, SSL certificate users, 200 days means that from March 15, 2026, if you still use the manual certificate application and deployment method, you must do it twice a year! This is acceptable for one website, but is it unbearable for 10, 100, 1,000 or even 10,000 websites!
For SSL certificate users, 100 days means that starting from March 15, 2027, if you still manually apply for and deploy certificates, you will have to do it four times a year! It is already difficult to manage one website, let alone 10, 100, 1,000 or even 10,000 websites. Automatic certificate management is a must!

For SSL certificate users, 47 days means that you must complete the automatic management of SSL certificates for all website systems in 4 years. No matter how many websites you have, even if you only manage one website, you cannot do it 10 times a year! After completing the automatic management of SSL certificates, they can then calmly deal with the subsequent 10-day validity policy. Therefore, all website owners must start preparing to implement automatic SSL certificate management from now on, must begin planning, researching, and make procurement budgets, and must complete automatic management of SSL certificates before March 15, 2026. Only in this way can we ensure the uninterrupted and reliable operation of the website system and meet the compliance requirements of security protection, and relevant laws and regulations.

In fact, this policy is a great benefit for website administrators and security administrators. As long as the automatic management of SSL certificates is implemented, they will be more relaxed and no longer have to worry about updating SSL certificates for many web servers every year. Especially for users who need to complete the SM2 HTTPS encryption transformation, the once-and-for-all solution is micro-change. Just deploy the HTTPS Automation Gateway in front of the existing web server. One-time investment, deploy two gateways at a time, and you can automate HTTPS encryption and WAF protection for up to 255 website systems. Free automatic certificate configuration meets the 100-day validity period of the dual-algorithm SSL certificate stipulated in 2027 in advance, and the gateway hardware system and SSL certificate are all included for 5 years. It is safe and worry-free for 5 years, and you no longer need to worry about applying for and deploying SSL certificates. Of course, more websites and website systems with larger traffic need to deploy more HTTPS Automation Gateways.

3. What do the 200-day, 100-day, and 47-day certificate policies mean to digital security service providers? How should they seize the opportunity?

For digital security service providers, including system integrators, cloud service providers, CA Agencies, etc., this is a huge new business opportunity. This is no longer a small business selling SSL certificates for a few thousand Yuan, but a big business of hundreds of thousands, millions, or even hundreds of millions of Yuan! Because all users need to complete this upgrade, this industry will be a large industry of hundreds of billions of Yuan. Especially with the mandatory requirements of

Cryptography transformation and IPv6 transformation that must be completed in China, this is a rare market opportunity for technology transformation that kills two birds with one stone.

For system integrators, this market opportunity has two business models. One is to sell the HTTPS Automation Gateway to help users easily complete the SM2 HTTPS encryption transformation, complete the WAF protection transformation, and complete the IPv6 transformation. For provincial or national government cloud platforms, in addition to selling HTTPS Automation Gateways, you can also sell the E-government Cloud SSL Service System to help government users automate the issuance of dual-algorithm SSL certificates for government systems from the government-specific SSL intermediate root certificates. All government systems are limited to deploying government-specific SSL certificates, completely eliminating SSL middleman attacks and not being affected by SSL certificate supply cuts.

Another business model of system integrators is to provide users with SSL certificate automation management services, invest in the purchase of HTTPS Automation Gateways, deploy them in the user's computer room, and charge annually according to the number of websites enabled. The charging pricing can refer to the current dual-algorithm SSL certificate charging. According to rough estimates, the return on investment of this service model greatly exceeds the return on investment from selling gateway hardware. This business model is a win-win solution. Government cloud platform does not need to purchase HTTPS Automation Gateways and still pay the service provider according to the current SSL certificate fees for each website. The amount of money paid is based on the number of websites activated, and the initial investment is small. The service provider's investment not only gets a high return, but also saves the engineer HR cost that no need to help customers to install SSL certificates. Just click the mouse to activate the HTTPS encryption and WAF protection services for users.

For commercial cloud platform vendors, it is essential to learn from the successful experiences of international giants like Google Cloud, Amazon Cloud, and Microsoft Cloud. By building their own cloud SSL service system or directly integrating with the ZoTrus Cloud SSL Service System, they can quickly provide automatic management services for dual-algorithm SSL certificates to all cloud host users, CDN users, and WAF users. They can deploy multiple HTTPS Automation Gateways in the

cloud to offer HTTPS Automation Cloud Service to users.

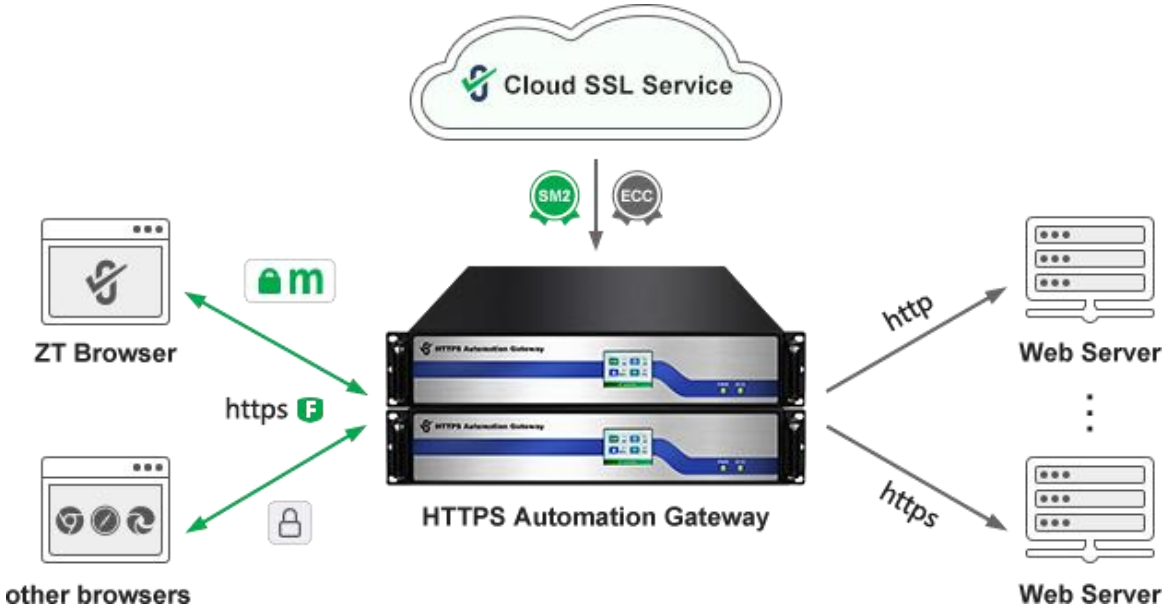
For CAs, it is necessary to promptly establish automation capabilities for issuing dual-algorithm SSL certificates and for automatic deployment. This will allow them to not only automatically configure dual-algorithm SSL certificates for their own HTTPS Automation Gateways but also to provide automatic management services for dual-algorithm SSL certificates to other gateway vendors. This shifts the focus from merely selling SSL certificates to offering solutions for automatic SSL certificate management. ZoTrus Technology has spent four years developing a dual-algorithm SSL certificate issuance system and an automatic management solution, which can help CAs swiftly acquire these two core capabilities, thus entering the vast market for automatic SSL certificate management in the quickest way possible.

For network security equipment manufacturers and cryptographic equipment vendors, if their relevant security devices and cryptographic devices (such as gateways and WAFs) require SSL certificates, it is time to embrace SSL certificate automation. They should provide automatic management services for dual-algorithm SSL certificates based on the China ACME standard. As the leading organization in formulating the China ACME standard, ZoTrus Technology can assist network security and cryptographic vendors in rapidly achieving automatic management capabilities for their devices regarding dual-algorithm SSL certificates, reliably issuing globally trusted RSA/ECC SSL certificates and SM2 SSL certificates through multiple channels, and quick entry into the large market for automatic SSL certificate management.

4. ZoTrus is already prepared to support automatic renewal of dual-algorithm SSL certificates every day

As early as it was founded in 2021, ZoTrus Technology had already identified the general development trend of SSL certificate automation management, invested heavily in the research and development of SM2 SSL certificate automation management ecological products, and took the lead in formulating the cryptographic industry standard "Automatic Certificate Management Specifications". In November 2023, at the 25th China International High-Tech Fair, it launched a client-to-cloud integrated SSL certificate automation management solution. The core product is the ZoTrus HTTPS Automation

Gateway, the first dual algorithm (RSA/SM2) HTTPS Automation Gateway in China that has passed the Commercial Cryptographic Product Certification. It supports the automatic application and deployment of dual-algorithm SSL certificates for up to 255 websites, and it integrates a high-performance WAF protection system to provide users with automatic HTTPS encryption and WAF protection services. The completely free SM2 algorithm supported browser - ZT Browser is a supporting product for the automatic management of SM2 SSL certificates. It gives priority to the use of SM2 algorithms to implement HTTPS encryption and supports SM2 certificate transparency.



Currently, many government agencies, universities, banks and other companies have deployed ZoTrus HTTPS Automation Gateway to realize the automatic management of SSL certificates. The default automatic configuration is the 90-day valid ECC DV SSL certificate and SM2 OV SSL certificate, which meets the user's global trust and cryptography compliance needs. Not only does it meet the 100-day certificate validity policy starting on March 15, 2027 in advance, but it also automatically supports the requirements for changing the validity period of SSL certificates, that is, before March 15, 2029, it will automatically configure a dual-algorithm SSL certificate with a validity period of 47 days for users without user settings.

What is even more worthy of praise is that the ZoTrus Cloud SSL Service System supports multi-channel issuance of RSA/ECC SSL certificates and SM2 SSL certificates, which effectively ensures that no matter what problems the CA encounters in the future or supply chain interruptions caused by

changes in the international situation, it will not affect the ZoTrus Cloud SSL Service System's automatic configuration of dual-algorithm SSL certificates for the HTTPS Automation Gateway. This is a global and exclusive innovative SSL certificate supply chain security measure provided by ZoTrus Technology, which completely solves the problem that a single CA supply chain cannot guarantee the security of SSL certificate supply, thereby effectively ensuring the uninterrupted service of HTTPS encryption of user websites. This is very worthy of users' high attention when evaluating and selecting SSL certificate automation management service providers.

Richard Wang

May 16, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 92 articles in English (more than 123K words) and 213 articles in Chinese (more than 632K characters in total).