Tackle the upcoming two HTTPS revolutions in one go

HTTPS technology was invented by Netscape in 1994, using SSL certificates to encrypt data transmission from browser to server. This is a revolutionary invention, which has transformed the plaintext HTTP Internet into the ciphertext HTTPS Internet, making the Internet commercially valuable, making the laboratory's Internet technology popularized and used worldwide, and making Internet services that people cannot live without today. 31 years later, this technology is about to usher in a technological revolution - shortening the validity period of SSL certificates, and completely changing from manual application and deployment of SSL certificates to automatic application and deployment. The purpose of this technological revolution is to welcome the next real technological revolution - post-quantum cryptographic HTTPS encryption. Both technological revolutions require system upgrades and transformations, which are inevitable transformations. This article discusses whether there are feasible technical solutions to tackle the two upcoming technological revolutions in one go.

1. The technological revolution of SSL certificate management from manual to automatic

Since its inception, SSL certificates have been issued by CAs trusted by browsers. After obtaining the certificate, users manually deploy the SSL certificate on the Web server or gateway device, and then enable HTTPS encryption to ensure the security of website data transmission. This business process has remained unchanged for 31 years. However, in today's world of the Internet of Everything, everything connected needs to implement HTTPS encryption, so it is impossible to manually complete the application and deployment of SSL certificates, which requires a technological revolution.

In fact, this technological revolution began as early as 2015, when Mozilla led the Let's Encrypt to automatically issue and deploy SSL certificates. In 2019, the RFC 8555 Automatic Certificate Management Environment (ACME) standard was published, which has received positive responses and has been widely implemented around the world. Currently, 800 million of the 1.1 billion valid SSL certificates in the world are automatically issued and deployed, effectively ensuring the security of data transmission in the global Internet of Everything. In 2015, there were only more than two million valid SSL certificates in the world. In ten years, the number of SSL certificates issued has increased 550 times. This is the power of automation.

Since this technological revolution has already begun, why does the author say that this technological revolution is coming soon? Because even though more than 80% of HTTPS encryption has achieved automatic management of SSL certificates, this is not mandatory. People are still accustomed to the 31-year habit of manually applying for and deploying SSL certificates, which seriously hinders the popularization and application of SSL certificates. This requires a revolution!

On March 3, 2023, Google released the revolutionary plan "Move Forward, Together" - forcibly shortening the validity period of SSL certificates to 90 days and fully embracing the automatic management of SSL certificates, which is to revolutionize the traditional manual management of SSL certificates. However, just like any revolution will inevitably encounter opposition, this technological revolution was opposed by CAs and SSL certificate users, resulting in the fact that this revolution did not have a successful outline until May 16, 2025 - the formulation of international standards for shortening the validity period of SSL certificates in steps. This is a revolution of compromise among all parties and will be completed in three steps: shortening the validity period of SSL certificates to 200 days on March 15, 2026, 100 days on March 15, 2027, and 47 days on March 15, 2029.

This means that this technological revolution will arrive on March 15 next year. The purpose of this upcoming HTTPS technology revolution is to realize the automatic management of SSL certificates, from traditional manual management to automatic management. This requires SSL certificate users to take appropriate technical measures to complete system upgrades and transformations to realize automatic management of SSL certificates. China users need to realize the automatic management of dual-algorithm (RSA/SM2) SSL certificates, and complete the system commercial cryptographic transformation to support the SM2 algorithm, and realize the HTTPS encryption automation of the adaptive cryptographic algorithm.

2. The technological revolution from traditional cryptography to quantum-resistant cryptography

In order to cope with the future quantum computing that may break the cryptographic algorithms currently in use in seconds, new quantum-resistant cryptographic algorithms are needed that can protect data from attacks launched using current traditional computers and future quantum computers. These algorithms are Post-Quantum Cryptography (PQC).

Although the transition to post-quantum cryptography began before the advent of quantum computers, there is still a pressing threat. Attackers collect encrypted data now with the intention of decrypting the data after quantum technology matures. This is the security threat of "collect first-decrypt later". Because the value of many confidential data often lasts for many years, and some personal confidential data will accompany a person's life, it is crucial to start the transition to post-quantum cryptography now to prevent confidential data from being decrypted in the future. This threat model is one of the main reasons for the urgent transition to post-quantum cryptography.

To this end, the National Institute of Standards and Technology (NIST) of the United States released a draft for public comments on NIST IR 8547 "Transition to Post-Quantum Cryptography Standards" on November 12, 2024. The report describes NIST's expected approach to transitioning from cryptographic algorithms vulnerable to quantum attacks to post-quantum digital signature algorithms and key establishment schemes, identifies existing cryptographic standards vulnerable to quantum attacks and quantum-resistant cryptographic standards to which information technology products and services need to transition, and aims to promote cooperation with industry, standards organizations, and related institutions to promote and accelerate the adoption of post-quantum cryptography. NIST has listed a timetable for transitioning to PQC standards, with the goal of reducing quantum risks as much as possible by 2035. The currently widely used secure cryptographic algorithms RSA-2048 and ECC-256 will be **deprecated after 2030 and disallowed after 2035.** This is the death date of traditional cryptographic algorithms, requiring the industry to prepare for the migration of all related systems and products to PQC algorithms in advance.

This means the technological revolution that will be faced before December 31, 2029, is that HTTPS encryption must be migrated to quantum-resistant cryptographic algorithms, and all systems need to be upgraded to support post-quantum cryptographic HTTPS encryption. This is another upcoming technological revolution that users must face, and this technological revolution requires users to upgrade and transform existing systems to support post-quantum cryptographic algorithms.

3. Two technological revolutions require two system upgrades

One of the six benefits of automating SSL certificate management listed by Google in its "Move Forward, Together" plan is "easy transition to quantum-resistant algorithms." Indeed, the ultimate goal of the technological revolution to shorten the validity period of SSL certificates is to resist quantum attacks, because current cryptographic algorithms cannot resist the upcoming quantum computing. The main purpose of continuously shortening the validity period of SSL certificates is to achieve automatic updates of SSL certificates, providing the technical means to support post-quantum cryptographic algorithms for automatic updates, ensuring a seamless and unnoticed transition to quantum-resistant algorithms when conditions are mature. The ultimate goal of these two technological revolutions is still to support the second quantum-resistant technological revolution.

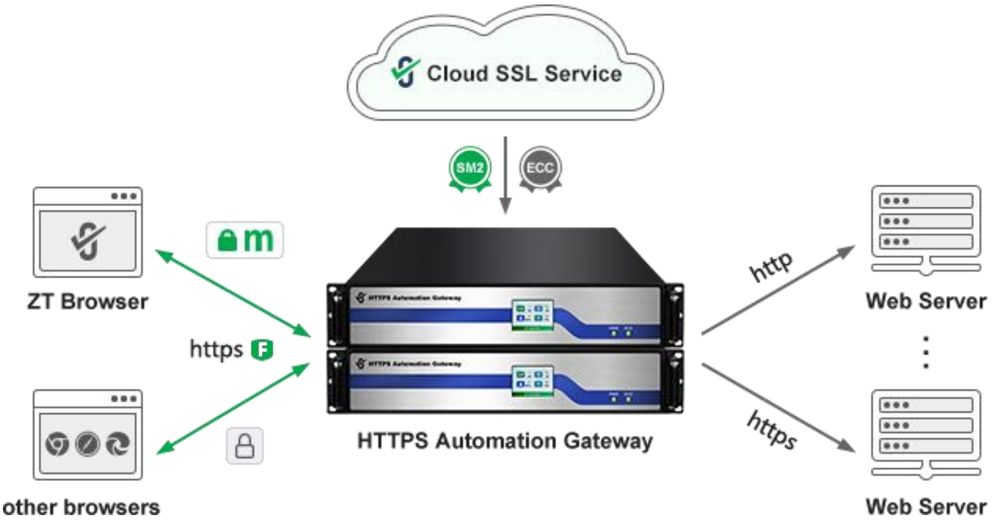
Shortening the validity period of SSL certificates is a revolution that SSL certificate users must face. This revolution will arrive on March 15, 2026, and will be completed on March 15, 2029. Abandoning traditional cryptographic algorithms and enabling post-quantum cryptographic algorithms is another revolution that SSL certificate users must face. This revolution will arrive on December 31, 2029, because the cryptographic algorithms currently in use must be abandoned in 2030, including the RSA-2024 algorithm, ECC-256, and SM2 algorithm.

The technological revolution on March 15, 2026, requires users to implement the upgrade and transformation of SSL certificate automatic management technology in advance, and completely abandon the traditional manual management of SSL certificates. The technological revolution on December 31, 2029, requires users to implement post-quantum cryptographic support for HTTPS encryption in advance, which also requires users to complete system upgrades. SSL certificate users, that is, all website operators and administrators, must come up with an action plan to complete the 2026 technological revolution as soon as possible. And they also need to consider how to complete the 2029 technological revolution in advance, rather than just considering the 2026 technological revolution. The two revolutions are related and are both for the purpose of ensuring the security of HTTPS encryption.

4. ZoTrus innovation achieves a micro-transformation to complete the necessary technological transformation for two technological revolutions

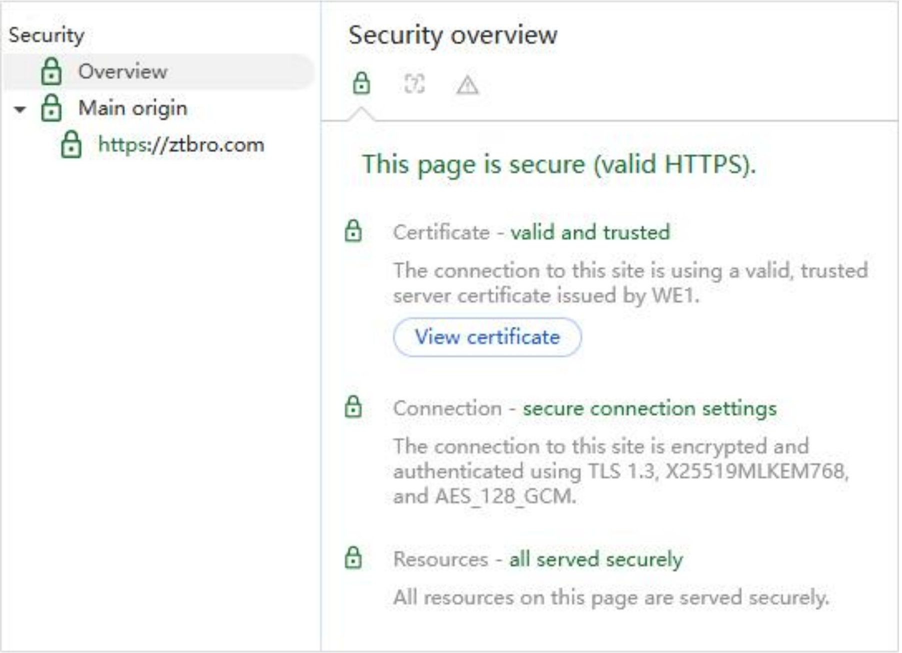
When ZoTrus Technology was founded four years ago, it positioned itself as a provider of SSL certificate automatic management solutions for users, and it provided automatic management of both SM2 and RSA/ECC SSL certificates. Because at that time, the world had already begun to popularize the use of SSL certificate automatic management technology, but China is still basically blank. Given that the SM2 SSL certificate automatic management cannot apply the international SSL certificate automatic management solution, because the commercial cryptographic system is generally not supported in various systems at present, in order to realize the SM2 HTTPS encryption automation, it is not only necessary to realize the automatic management of the SM2 SSL certificate, but also to automatically complete the SM2 algorithm support upgrade and transformation.

In order to help SSL certificate users easily complete the system upgrades and transformations that must be completed in the upcoming technological revolution to shorten the validity period of SSL certificates, ZoTrus Technology's innovative solution is a micro-transformation, zero business interruption solution. One gateway simultaneously completes the automatic management of dual-algorithm SSL certificates and SM2 algorithm support transformation, while the original Web server does not need any transformation. This is a client-to-cloud integration solution. Users only need to deploy the ZoTrus HTTPS Automation Gateway in front of the original Web server. The ZoTrus Gateway automatically connects to the ZoTrus Cloud SSL Service System to automatically complete the automatic application and deployment of dual-algorithm SSL certificates with a validity period of 47 days, automatically implement HTTPS encryption and WAF protection, and it is an adaptive encryption algorithm. The free ZT Browser implements SM2 algorithm HTTPS encryption, while other browsers that do not support the SM2 algorithm implement RSA/ECC algorithm HTTPS encryption.



The innovative solution proposed by ZoTrus Technology for the technological revolution of shortening the validity period of SSL certificates can not only help SSL certificate users easily cope with the upcoming technological revolution in 2026, but ZoTrus Technology is already researching the automatic implementation of post-quantum cryptographic HTTPS encryption. This is the advantage of ZoTrus in creating a full range of products for the automatic management ecosystem. As long as ZT Browser and ZoTrus Gateway support post-quantum cryptographic HTTPS encryption, users only need to upgrade ZT Browser for free, and ZoTrus Gateway only needs to automatically complete the software upgrade for free, so that users can complete the post-quantum cryptographic HTTPS encryption upgrade and transformation work without feeling.

As shown in the figure below, ZT Browser's English official website has realized the HTTPS encryption of the post-quantum cryptography (ML-KEM768) hybrid key agreement mechanism of the ECC algorithm SSL certificate, and the SM2 algorithm SSL certificate PQC hybrid key agreement mechanism is also in full swing. It is expected that by the end of the year, both ZT Browser and ZoTrus HTTPS Automation Gateway will support SM2DH-MLKEM768, and it takes the lead in realizing HTTPS encryption of SM2 PQC hybrid key agreement mechanism, which is the unique advantage of ZoTrus Technology's full ecological products.



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by WE1.

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519MLKEM768, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

This means if users choose the micro-transformation solution of the SSL certificate automation management technology revolution from ZoTrus Technology, they can complete the technical transformation work of the quantum cryptography HTTPS encryption technology revolution for free and automatically in the future. This is a perfect solution to kill two birds with one stone. It is far-sighted and completes the necessary two technical revolutions and technical transformations with one investment, saving money and workforce. This is the unique advantage of ZoTrus Technology, which considers and arranges for users in advance, helping users to easily deal with current and future HTTPS encryption security threats.

5. Since two technological revolutions are necessary, let's complete them at once.

Just as Google has said that it is pushing to shorten the validity period of SSL certificates in order to ease the transition to quantum-resistant cryptography, since it is necessary to complete two HTTPS encryption technology revolutions, we should think about the second technological revolution when planning the first technological revolution, plan the technological transformations required for the two technological revolutions together, and choose advanced technical solutions that can be completed in one go, rather than treating the symptoms without addressing the root cause. Only in this way can we find the best solution that saves investment and reduces the burden of upgrades and transformations.

The technological revolution of shortening the validity period of SSL certificates will arrive on March 15, 2026, and end on March 15, 2029. The technological revolution of post-quantum cryptographic

HTTPS encryption will arrive on December 31, 2029. These two technological revolutions are what all website operators must deal with and must undergo transformation. Choosing to complete both revolutions at once is the only correct choice.

Richard Wang

July 14, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 96 articles in English (more than 131K words) and 219 articles in Chinese (more than 652K characters in total).