2026, Seize the Momentum to Win the Market

January 4, 2026

2026 is destined to be an extraordinary year, as March 15th will officially end the **32**-year history of using a year as the SSL certificate issuance cycle, switching to a 200-day issuance cycle, and further to 47 days on March 15th, 2029. This is one of the major events in global internet security in 2026, and I define 2026 as the "**Year One of HTTPS Automation**".

The second major event is that, starting March 1st, the validity period of code signing certificates will be shortened to one year and three months (450 days). This will officially end the **30-**year history of issuing code signing certificates with multiple-year validity periods. This is one of the major events in global software security in 2026, and I define 2026 as the " **Year One of Code Signing Automation**".

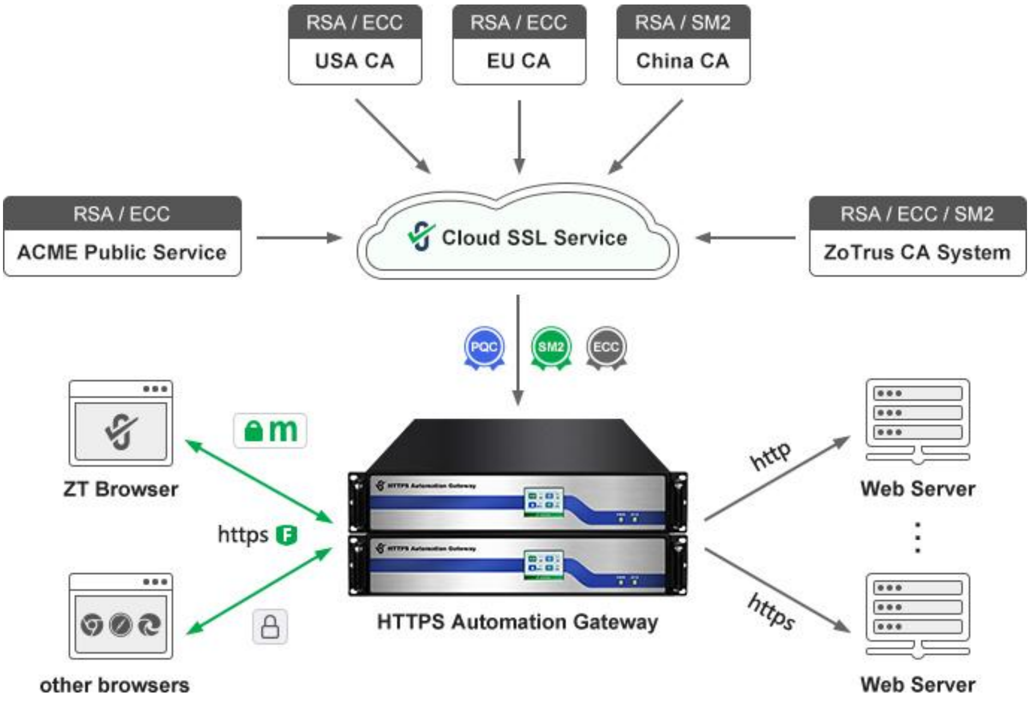
What do these two events mean? They mean the necessity of automating digital certificate applications. ZoTrus Technology began its foray into certificate application automation on its founding day in 2021. After four years, in December 2025, it perfectly completed an HTTPS automation management solution that simultaneously supports commercial cryptography algorithm and post-quantum cryptography algorithm, in anticipation of 2026, the inaugural year of HTTPS automation. ZoTrus Technology strategic goal for 2026 is to capitalize on this momentum and win over the HTTPS automation market and the code signing automation market.

1. The website security solution has been completed and is poised to win the market in 2026.

ZoTrus website security solution is an HTTPS automation solution. HTTPS ensures secure communication between browsers/apps, websites, APIs, and services, and SSL certificates are the core component for implementing HTTPS encryption. When the author was still busy with CA operations, its core business was, of course, selling SSL certificates. However, when the author founded ZoTrus Technology, the author realized that users needed HTTPS encryption, not just SSL certificates, and that SSL certificate automation had become an unstoppable trend. This is because the Internet of

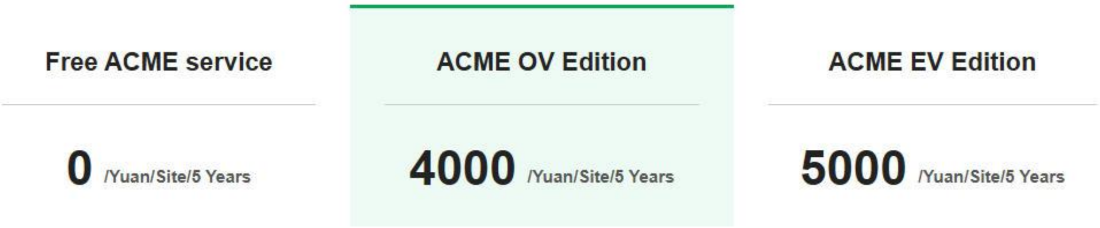
Things (IoT) requires HTTPS encryption, and manually applying for and deploying SSL certificates is impossible to achieve secure IoT. The author clearly saw the power of SSL certificate automation in the growth of Let's Encrypt, the initiator of automatic SSL certificate management. The name Let's Encrypt itself speaks volumes — users need HTTPS encryption, not just SSL certificate! They need automatic implementation of HTTPS encryption, not automatic management of SSL certificate.

ZoTrus HTTPS automation solution is a dual-algorithm SSL certificate automation management solution tailored to the specific needs of China. It's an innovative solution integrating commercial cryptography HTTPS encryption upgrades, automatic SSL certificate management upgrades, and post-quantum cryptography migration, helping customers complete three essential technical upgrades with a single minor upgrade. This is a client-to-cloud solution with two essential "clients": First, the ZT Browser, an HTTPS client supporting both commercial cryptography algorithm and post-quantum cryptography algorithm, completely free, clean, and ad-free. Existing browsers on the market cannot meet the three essential technical upgrade requirements. The other “client” is the ZoTrus HTTPS Automation Gateway, a new type of gateway specifically designed for HTTPS encryption, supporting both commercial cryptography algorithm and post-quantum cryptography algorithms and enabling automatic dual-algorithm SSL certificate management. Existing gateway products on the market cannot meet the three essential technical upgrade requirements. Furthermore, to achieve automatic SSL certificate management, the ZoTrus Cloud SSL Service System is also required. This server provides dual-algorithm SSL certificate issuance services for ZoTrus HTTPS Automation Gateway. Existing certificate automation services on the market cannot meet the three essential technical upgrade requirements. International automatic certificate management services can only provide RSA/ECC algorithm SSL certificates and can only provide automatic certificate issuance services for a single issuing CA. China not only needs RSA/ECC algorithm SSL certificates but also SM2 algorithm SSL certificates, and it also needs to support multiple CA issuance channels. This is not only to cope with the very uncertain international environment, but also to provide customers with reliable SSL certificate issuance, because single CA issuance cannot guarantee a reliable supply of SSL certificates.



This is ZoTrus HTTPS automation solution, meticulously crafted over four years. It's a globally unique and innovative solution that perfectly addresses the challenges of commercial cryptography HTTPS encryption upgrade, certificate automation upgrade, and post-quantum cryptography migration. This proprietary ecosystem offers a complete suite of products required for HTTPS encryption, including the SM2 certificate transparent log system (not listed in the figure above). Globally, it's the first to simultaneously support two hybrid PQC algorithms (SM2MLKEM768 and X25519MLKEM768) and three traditional cryptographic algorithms (SM2, RSA, and ECC). ZT Browser and ZoTrus HTTPS Automation Gateway prioritize the SM2MLKEM768 algorithm for HTTPS encryption, while also meeting the commercial cryptography compliance upgrade and post-quantum cryptography migration needs.

On March 15, 2026, the world officially entered the era of SSL certificate automation. ZoTrus Technology already possesses the production, deployment, and service capabilities for large-scale implementation of automatic SSL certificate upgrade and post-quantum cryptography migration. It not only can quickly provide HTTPS Automation Gateway products for critical infrastructure operators, but also plans to launch a completely free certificate automation service for SMEs and individual users in January. Similar to Let's Encrypt certificate automation service, the difference is that it automatically issues dual algorithm (ECC+SM2) SSL certificates. SM2 SSL certificates are trusted by all SM2 supported browsers, and ECC SSL certificates are trusted by all browsers. Furthermore, it offers fully open-source ACME client software, meeting the certificate automation application needs of SMEs and individual users for single or small groups of websites.



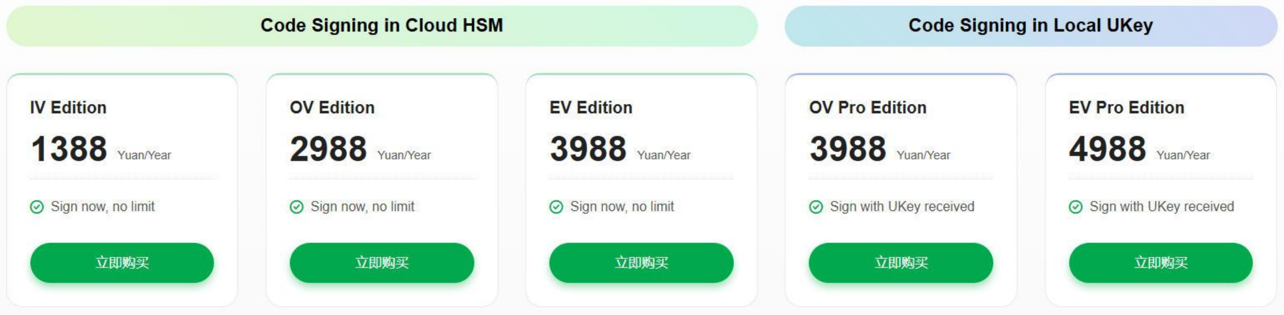
Free ACME service	ACME OV Edition	ACME EV Edition
0 /Yuan/Site/5 Years	4000 /Yuan/Site/5 Years	5000 /Yuan/Site/5 Years

ZoTrus Certificate Automation (ACME) Service has no limit on the number of websites or certificate applications, and dual-algorithm (ECC+SM2) DV SSL certificates are completely free. For users who need automated OV/EV SSL certificate management, professional edition and enhanced edition are available, with dual certificates (SM2 OV + ECC DV) starting at as low as RMB 800 per year, and dual certificates (SM2 EV + ECC DV) starting at as low as RMB 1000 per year. RSA/ECC OV/EV SSL certificates are also available.

2. **Application Security, Email Security, and Document Security solutions will all be delivered by 2026.**

After completing its website security solution, ZoTrus Technology shifted its R&D focus to application security, email security, and document security solutions, all based on the same philosophy — automating cryptography applications, automating code signing, automating email encryption, and automating document signing.

The application security solution — code signing cloud service — is expected to launch in January. It will be the first and only service in China to provide software developers with a domestically sourced, cloud-based code signing service. The code signing certificates required for the service are issued by two of the six CAs designated by the Microsoft Windows Hardware Partner Center: **Sectigo** and **SSL.com**. The biggest difference from code signing services provided by foreign CAs is that it does not charge based on the number of signed codes; it has a fixed annual fee and no limit on the number of code signatures. Of course, users can still purchase traditional USB Key certificates, but these will use China produced USB Key. After certificate issuance, users will not need to wait 10 days for the USB Key to be shipped from the US; instead, it will be delivered directly from Shenzhen via SF Express within 24 hours.



Code Signing in Cloud HSM			Code Signing in Local UKey	
IV Edition	OV Edition	EV Edition	OV Pro Edition	EV Pro Edition
1388 Yuan/Year	2988 Yuan/Year	3988 Yuan/Year	3988 Yuan/Year	4988 Yuan/Year
✓ Sign now, no limit	✓ Sign now, no limit	✓ Sign now, no limit	✓ Sign with UKey received	✓ Sign with UKey received
立即购买	立即购买	立即购买	立即购买	立即购买

The email security solution — the email encryption service — is expected to launch in the third quarter. This solution, an email client built into ZT Browser, has been under development for three years. After completing website security and application security solutions, R&D efforts will focus on completing internal testing in the second quarter and global release in the third quarter. This is the world's only free, automatic configuration solution for dual-algorithm email certificates, automating email encryption, digital signatures, and timestamping for email security. The basic edition is completely free, while the professional edition provides trusted sender identity validation service, proving the trusted identity of each email and enhancing online trust.

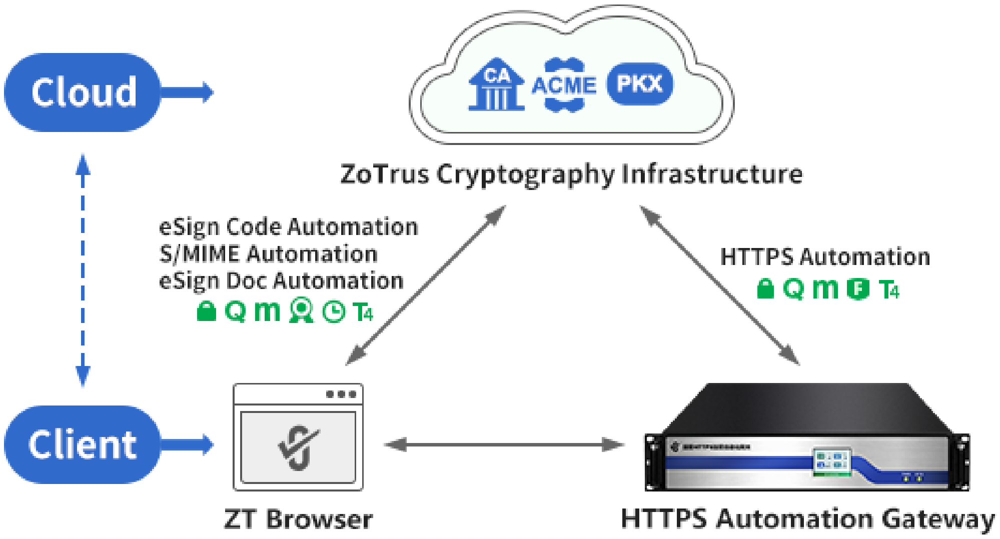
The document security solution — document signing service — is expected to launch in the fourth quarter. This is a complete document security service following the real-time validation of digital signatures in PDF documents and the display of the signer's trusted identity by the ZT Browser's built-in PDF reader. It offers free, automatic configuration of dual-algorithm document signing certificates. The professional edition provides globally trusted e-signing services and trusted identity validation services, proving the trusted identity of each document and enhancing online trust. And a free e-contract signing service is offered based on encrypted email. Contracts to be signed and those already signed are stored in encrypted emails in the user's own inbox, completely overturning the current insecure method of storing signed contract documents in e-contract signing service providers.

3. ZoTrus Technology, a leader in cryptography application automation.

The main cryptographic products that ensure global Internet security are four types of digital certificates: SSL certificates ensure secure communication between the client (browser/app) and the server; code signing certificates ensure the security of software running on the client and server; email certificates ensure secure email communication; and document certificates ensure document security.

However, traditional cryptographic applications are disconnected from users' actual application needs. Users need to apply for certificates from CAs and then painstakingly configure them for use in various application software systems. CAs only issue certificates, while application software developers only use them. The intermediate work is left to users to handle manually, which is the bottleneck of cryptographic applications. This is why the RSA cryptographic algorithm, invented in 1977, has not been widely adopted even after 50 years. The new situation is that this still-unpopular cryptographic algorithm will be abandoned in four years because it is insecure in the face of quantum computing. Therefore, to prevent the "harvest now, decrypt later" security threat, it is now necessary to adopt post-quantum cryptographic algorithms. The only solution is to follow the principle of cryptographic agility and automate the application of various digit certificates, that is, to automate cryptographic applications.

ZoTrus Technology has completed the R&D and large-scale production capacity building of its SSL certificate application automation solution, with many technical indicators being unique and leading globally. Code signing certificate application automation is also about to be launched, and email certificate application automation and document signing certificate automation will both be completed and launched on the market in 2026.



ZoTrus will provide more advanced HTTPS encryption automation management solutions and related products and services in 2026, working together with users to welcome the arrival of the year one of HTTPS automation. This will help customers complete commercial cryptography transformation, certificate automation transformation and post-quantum cryptography migration in one technical upgrade, ensuring the continued security of customers valuable data resources in the present and the quantum era.

Richard Wang

January 4, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 107 articles in English (more than 152K words) and 247 articles in Chinese (more than 731K characters in total).