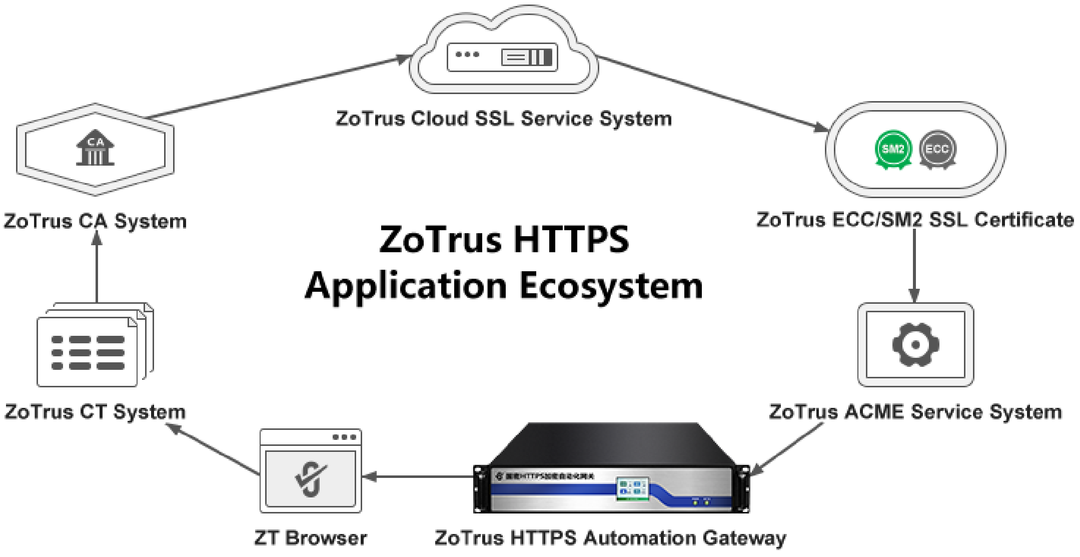
Building the post-quantum cryptography HTTPS application ecosystem

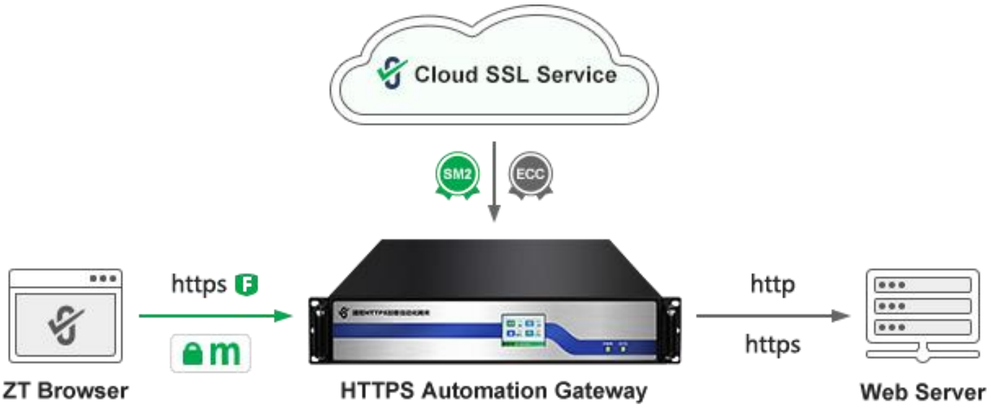
ZoTrus Technology today released the news of the “PQC HTTPS Full Ecosystem Product Readiness Timeline." This article details the details of this full ecosystem product to help users understand post-quantum cryptography HTTPS encryption technology and fully understand that only by implementing automatic management of dual-algorithm SSL certificates now, can ensure seamless upgrade to post-quantum cryptography HTTPS encryption in the future. The two are closely related.

1. Introduction to the traditional cryptography HTTPS Application Ecosystem

ZoTrus Technology has spent four years building the SM2 Certificate Automatic Management Ecosystem and the SM2 Certificate Transparency Ecosystem. These two ecological products have realized the automatic management of dual-algorithm (ECC/SM2) SSL certificates, that is, ZoTrus has created a traditional cryptography HTTPS application ecosystem. This ecosystem includes at least 7 major products: the RSA/ECC algorithm SSL certificates and SM2 algorithm SSL certificates that are issued by ZoTrus Cloud SSL Service System connecting to multiple RSA/ECC CAs and multiple SM2 CAs to realize multi-channel automatic certificate issuance. ZoTrus SM2 CA System is responsible for issuing dual algorithm (RSA/SM2) intranet SSL certificates. ZoTrus SM2 Certificate Transparency System is providing SM2 algorithm certificate transparency log services for CAs that issues SM2 SSL certificates. ZoTrus SM2 ACME Service System is providing dual-algorithm SSL certificate automatic application and issuance services for ZoTrus HTTPS Automation Gateway. ZoTrus HTTPS Automation Gateway is a hardware gateway product dedicated to https encryption of Web website systems, which has passed commercial cryptographic product certification and integrates multiple functions such as https encryption acceleration, https offloading and forwarding, SM2 algorithm module, WAF protection, load balancing, and two-way authentication. ZT Browser supports RSA/ECC/SM2 algorithms from the core layer and supports ECC and SM2 certificate transparency.

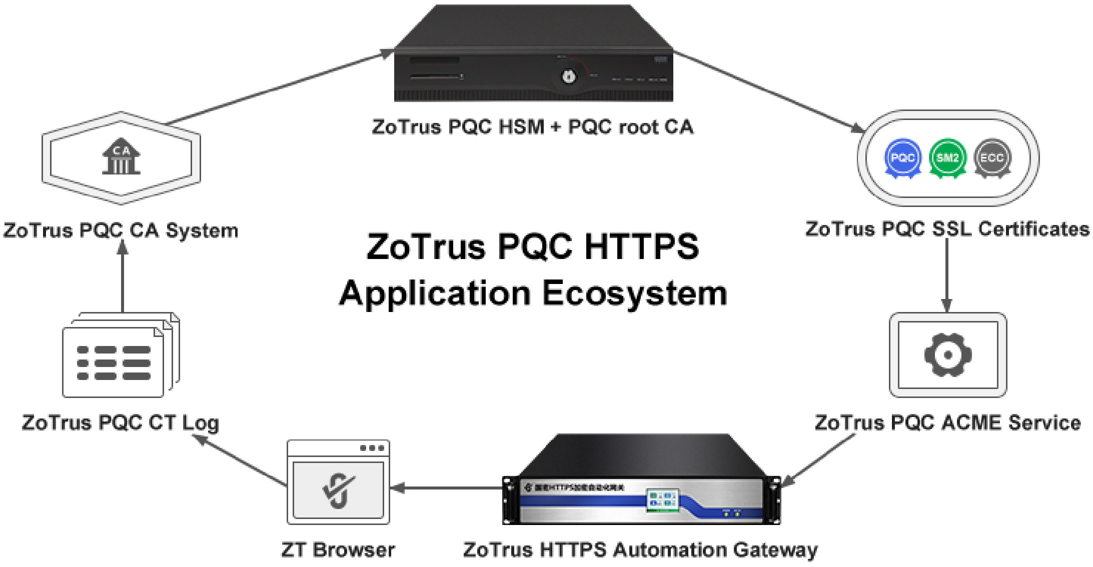

ZoTrus Cloud SSL Service System
ZoTrus CA System
ZoTrus ECC/SM2 SSL Certificate
ZoTrus HTTPS Application Ecosystem
ZoTrus CT System
ZoTrus ACME Service System
ZT Browser
ZoTrus HTTPS Automation Gateway
CA
SM2
ECC

The full HTTPS application ecosystem products created by ZoTrus Technology constitute a client-to-cloud integrated dual-algorithm SSL certificate automatic management solution with zero modification to the original Web server. ZT Browser is installed on the end user's computer, and the ZoTrus HTTPS Automation Gateway is deployed in front of the Web server in the user's computer room, automatically implementing HTTPS encryption and WAF protection with adaptive cryptographic algorithms. The automatically configured SSL certificates have achieved 90 days of validity in advance, and they will achieve 47 days of validity before December 2028, meeting the compliance requirements of international standards for continuously shortening the validity period of SSL certificates in advance.



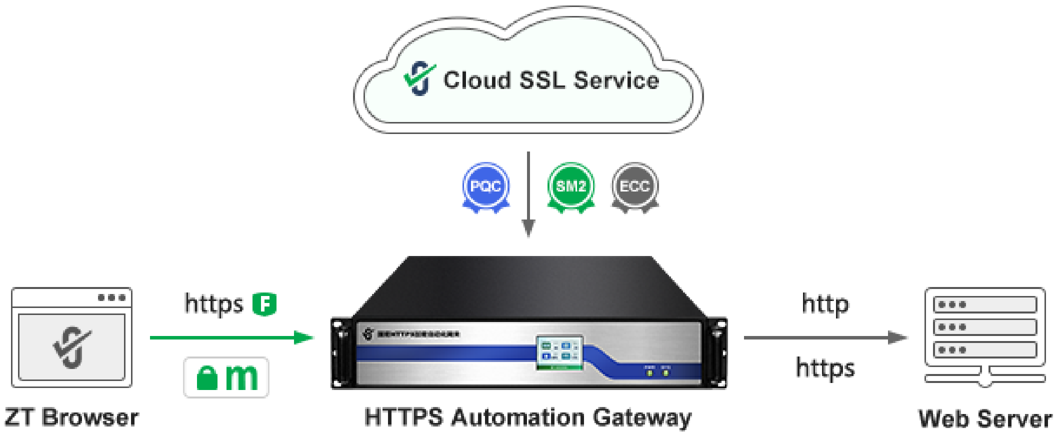
2. Introduction to the Post-Quantum Cryptography HTTPS Application Ecosystem

The post-quantum cryptography HTTPS application ecosystem is another ecosystem that ZoTrus Technology is vigorously building for the smooth migration of HTTPS encryption from traditional cryptography to post-quantum cryptography. This ecosystem includes at least seven major products: ZoTrus PQC HSM and the PQC algorithm root CA certificates generated in this HSM. ECC algorithm + MLDSA hybrid algorithm SSL certificates, SM2 algorithm + MLDSA hybrid algorithm SSL certificates, and pure PQC algorithm SSL certificates are all issued by ZoTrus PQC CA System. ZoTrus PQC CT System provides PQC algorithm certificate transparency log services for CAs issuing PQC SSL certificates. ZoTrus PQC ACME System provides dual-algorithm SSL certificate automatic certificate application and issuance services for ZoTrus HTTPS Automation Gateway. ZoTrus HTTPS Automation Gateway provides HTTPS encryption and WAF protection services that support ECC+MLKEM and SM2+MLKEM hybrid PQC algorithms and pure PQC algorithms. ZT Browser supports multiple cryptographic algorithms such as ECC / SM2 / ECC+MLKEM / SM2+MLKEM / MLDSA+MLKEM and supports ECC / SM2 / PQC algorithm certificate transparency.


ZoTrus PQC HSM + PQC root CA
ZoTrus PQC CA System
ZoTrus PQC SSL Certificates
PQC
SM2
ECC
ZoTrus PQC HTTPS Application Ecosystem
ZoTrus PQC CT Log
ZoTrus PQC ACME Service
ZT Browser
ZoTrus HTTPS Automation Gateway

The full PQC HTTPS application ecosystem products created by ZoTrus Technology constitute a client-to-cloud integrated multi-algorithm (ECC/SM2/PQC) SSL certificate automatic management solution with zero modification to the original Web server. ZT Browser is installed on the end user's computer, and ZoTrus HTTPS Automation Gateway is deployed in front of the Web server in the user's computer room, automatically implementing HTTPS encryption and WAF protection of adaptive cryptographic algorithms. The automatically configured traditional algorithm SSL certificates and

PQC algorithm SSL certificates are 47-day validity certificates. Users only need to automatically upgrade ZT Browser to support the PQC algorithm, and the ZoTrus Gateway deployed in the user's computer room will automatically upgrade to support the PQC algorithm, allowing the user system to seamlessly migrate to post-quantum cryptography without any feeling. The upgrade to support post-quantum cryptography is completely free, and users no longer need to spend money, worry about post-quantum cryptography migration.



3. Post-quantum cryptography HTTPS application ecosystem product readiness timeline

Based on the internationally agreed timetable for post-quantum cryptography migration, ZoTrus Technology has developed a timetable for the readiness of the entire ecosystem of post-quantum cryptography HTTPS application. As shown in the figure below, it will be completed in 7 steps.

The specific product readiness for each step is as follows:

(1) By December 2025, ZT Browser and ZoTrus Gateway will support ECC+MLKEM and SM2+MLKEM dual-algorithm hybrid key encapsulation mechanisms to achieve hybrid PQC algorithm HTTPS encryption.

(2) By March 2026, ZoTrus CA will create ECC+MLDSA and SM2+MLDSA dual-algorithm hybrid root CA certificates and sub-CA certificates for issuing PQC hybrid algorithm SSL certificates.

(3) By September 2026, ZT Browser and ZoTrus Gateway will support dual-algorithm PQC hybrid algorithm SSL certificates and adaptive 4 algorithms to implement PQC algorithm

HTTPS encryption.

(4) By December 2026, ZoTrus CA will create pure PQC algorithm (ML-DSA) root certificate and sub-CA certificates for issuing pure PQC algorithm SSL certificates.

(5) By July 2027, ZT Browser and ZoTrus Gateway will support pure PQC algorithm SSL certificates to implement PQC algorithm HTTPS encryption.

(6) By December 2028, ZT Browser and ZoTrus Gateway will support China PQC algorithm SSL certificates to implement China PQC algorithm HTTPS encryption.

(7) By December 2029, ZoTrus Technology will have completed the development of a full ecosystem of HTTPS encryption PQC algorithm products, supporting international and China PQC algorithms, and helping customers achieve seamless PQC HTTPS encryption migration.

4. Only by achieving ACME can seamlessly migrate to PQC

As can be seen from the introduction to the post-quantum cryptographic HTTPS application ecosystem that ZoTrus Technology is building, in order to achieve a seamless and smooth migration to post-quantum cryptography HTTPS encryption, it is necessary to first implement the automatic management of dual-algorithm SSL certificates, which is one of the six major benefits of implementing automatic SSL certificate management listed by Google in the "Moving Forward, Together" plan is "easy transition to quantum-resistant algorithms".

As can be seen from the timetable for the full-ecosystem product readiness of ZoTrus Technology's post-quantum cryptography HTTPS applications, all work is completed by ZoTrus Technology in the cloud, enabling ZoTrus HTTPS Automation Gateway deployed on the user side to automatically apply and deploy the issued PQC hybrid algorithm SSL certificates and pure PQC algorithm SSL certificates required for each stage. This is a client-to-cloud solution, and it is also the unique advantage of ZoTrus Technology in creating full-ecosystem products. Users do not need to seek support from multiple suppliers. They only need to start implementing automatic management of dual-algorithm SSL certificates now and deploy ZoTrus HTTPS Automation Gateway. At that time, users can automatically implement post-quantum cryptography HTTPS encryption, easily complete the migration of HTTPS encryption to post-quantum cryptography, and effectively ensure the uninterrupted HTTPS encryption security of all business systems.

All users must act now to complete the technological revolution of automatic SSL certificate management as soon as possible and make technical preparations for seamless migration to post-quantum cryptography HTTPS encryption.

Richard Wang

August 8, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 98 articles in English (more than 133K words)
and 223 articles in Chinese (more than 666K characters in total).