Early delivery of HTTPS products supporting two hybrid PQC algorithm

December 12, 2025

On August 8, 2025, ZoTrus Technology released its ecosystem product readiness timeline for post-quantum cryptography HTTPS encryption. The plan was for ZT Browser and ZoTrus Gateway to support hybrid key encapsulation mechanism combining ECC+MLKEM and SM2+MLKEM algorithms by December 2025, enabling HTTPS encryption using hybrid PQC algorithm. This project was completed ahead of schedule and delivered for use today, fully demonstrating ZoTrus Technology's forward-looking research capabilities and product implementation capabilities in the field of post-quantum cryptography. It provides strong technical support and widespread application support for early adoption of two hybrid PQC algorithm HTTPS encryption to ensure global Internet security, providing more hybrid PQC algorithm migration solutions, enhancing the resilience and security of the TLS ecosystem.

1. What are the two core PQC products that were delivered ahead of schedule?

The two core products of the hybrid PQC algorithm HTTPS encryption are ZT Browser and ZoTrus HTTPS Automation Gateway. ZT Browser is the client for hybrid PQC algorithm HTTPS encryption, and ZoTrus HTTPS Encryption Automated Gateway is used in server side for hybrid PQC algorithm HTTPS encryption. Both sides seamlessly realize the hybrid PQC algorithm HTTPS encryption application with zero modification to the original web server.

Users only need to upgrade ZT Browser to version V2601. Users who have already deployed ZoTrus HTTPS Automation Gateway only need to upgrade their system software to support it. Both support two hybrid PQC algorithms HTTPS encryption completely free of charge, meeting users' application needs for post-quantum cryptography migration. This is the unique advantage of ZoTrus Technology in creating a complete ecosystem of post-quantum cryptography HTTPS encryption products.

2. Why is it so important to implement HTTPS using hybrid PQC algorithm?

97% of global internet traffic is now encrypted with HTTPS, and 84% of traffic in mainland China is also encrypted with HTTPS. However, this traffic previously used traditional cryptographic algorithms such as RSA/ECC/SM2 to achieve HTTPS encryption. Future quantum computers can easily crack these encryptions. To prevent data security threats of "harvest now, decrypt later", 51% of global Internet traffic has now implemented hybrid PQC algorithm HTTPS encryption to ensure the continued security of HTTPS encrypted traffic in the quantum era.

The so-called hybrid PQC algorithm uses a combination of traditional cryptographic algorithms and post-quantum cryptographic algorithms to protect the shared key during the key encapsulation stage of the HTTPS encryption implementation process. Its working principle is to use traditional cryptographic algorithms (ECC or SM2) and the PQC algorithm (MLKEM) in parallel during the HTTPS handshake. This is a very strategically wise solution. First, it can hedge risks; even if vulnerabilities are found in the PQC algorithm in the future, the traditional cryptographic algorithm will still be effective. Second, it can achieve a smooth transition, ensuring compatibility with legacy systems and greatly reducing the risks of PQC migration. Third, it provides a pragmatic PQC migration path, reflecting a robust strategy for moving from the present to the future, lowering the technical threshold and uncertainty of adopting PQC, and making rapid deployment possible.

3. What are the innovative aspects of ZoTrus Hybrid PQC algorithm for HTTPS encryption?

The currently implemented hybrid PQC algorithm globally uses the X25519MLKEM768 algorithm, and ZoTrus innovative solution supports dual hybrid PQC algorithms by default on both side products. It uniquely boasts the following six major technological innovations:

(1) It not only supports the ECC algorithm hybrid PQC algorithm - X25519MLKEM768, but it is also the world's first to exclusively support SM2 algorithm hybrid PQC algorithm - SM2MLKEM768.

(2) Not only does it support the SM2MLKEM768 algorithm, but it also joined forces with the Alibaba TongsuoSSL open-source project to successfully apply to the international organization-IANA for TLS Supported Groups code point - 4590, making SM2MLKEM768 one of the four post-quantum cryptographic hybrid protocols in the international standard TLS protocol group. This is a global passport for the widespread application of the SM2MLKEM768 hybrid PQC algorithm.

(3) Not only does ZT Browser support the SM2MLKEM768 algorithm, but the server-side product, ZoTrus HTTPS Automation Gateway, also supports the SM2MLKEM768 algorithm, providing users with a one-stop solution without having to find support from multiple vendors.

(4) ZT Browser and ZoTrus HTTPS Automation Gateway support SM2MLKEM768 based on RFC 8998 (ShangMi (SM) Cipher Suites for TLS 1.3). It supports TLS 1.3 protocol using SM2 SSL certificates and SM2 algorithms to implement HTTPS encryption. ZoTrus is the world's first to support both the SM2 algorithm and SM2 hybrid PQC algorithm-SM2MLKEM768 in key exchange using the TLS 1.3 protocol.

(5) Not only does it achieve hybrid PQC algorithm HTTPS encryption, but ZoTrus HTTPS Automation Gateway also achieves automatic management of dual-algorithm (ECC+SM2) SSL certificates required for HTTPS encryption through collaboration with ZoTrus Cloud SSL Service System. This is also a globally unique one-stop solution, which does not just provide a PQC gateway or PQC browser.

(6) It not only supports hybrid PQC algorithms for HTTPS encryption, but also hybrid PQC algorithms for HTTPS + WAF protection. It is the world's only company to provide users with a one-stop China commercial cryptography compliance and PQC migration solution for HTTPS encryption and WAF protection.

4. The next step in the PQC ecosystem product readiness timeline is expected to be early.

The forementioned hybrid PQC algorithm is implemented during the HTTPS handshake process, using a hybrid algorithm to protect the shared key. The SSL certificate used for HTTPS encryption remains a traditional cryptographic algorithm (RSA/ECC/SM2) SSL certificate. According to ZoTrus Technology's post-quantum cryptography HTTPS encryption full ecosystem product readiness timeline released on August 8, 2025, the next PQC product will be launched in September 2026, enabling the issuance of hybrid PQC algorithm SSL certificates and supporting PQC algorithm HTTPS encryption with these hybrid algorithm SSL certificates.

The author anticipates two possible scenarios: either the product is implemented and delivered to users ahead of schedule, or this stage may be skipped, with direct entry into the next stage — issuing pure PQC algorithm SSL certificates and supporting HTTPS encryption with pure PQC algorithm SSL certificates. This is a major issue concerning the global Web PKI ecosystem's migration path from traditional cryptographic algorithm root CA certificates to hybrid PQC algorithm root CA certificates and then to pure PQC algorithm root CA certificates. The author is actively participating in international discussions on this topic. ZoTrus Technology will release the latest next-step PQC ecosystem products in a timely manner based on the global Web PKI industry consensus. Please continue to follow ZoTrus Technology's updates.

Richard Wang

December 12, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 104 articles in English (more than 142K words) and 243 articles in Chinese (more than 719K characters in total).