ZoTrus Empowers Cryptography with Automation

Cryptography is the foundation of global Internet security. Every moment, cryptographic tools like HTTPS encryption, powered by TLS/SSL certificates, secure data as it flows from users' browsers and apps to servers, protecting the world's digital backbone. But the popularization of HTTPS encryption is inseparable from SSL certificate automation, and the same is true for email encryption, and there is only one way for other cryptography applications to become popular. ZoTrus addresses this challenge head-on by automating cryptography and making its presence clear. Let's dive into the details.

1. New Threats in the IoT and AI Era

The Internet of Everything (IoT) era thrives on data, uploaded to the cloud and exchanged constantly. This demands secure transmission channels. Traditional HTTP, transmitting data in plain text, is a glaring vulnerability: information can be intercepted or altered mid-journey. Imagine AI relying on tampered data - the consequences could be disastrous. Smart connected cars and autonomous driving face similar risks: if communication between vehicles, road networks, and the cloud isn't encrypted, data theft or manipulation could compromise security. In smart cities, cameras and sensors sending unencrypted HTTP data to the cloud invite equally grave dangers. Server-side "fortress" protection alone won't cut it, data security in transit is now non-negotiable.

2. Cryptography: The Only Solution

HTTPS encryption, built on TLS/SSL certificates, is the cornerstone of IoT security. It ensures data collected by devices reaches cloud servers secure and returns to users intact, critical for smart cars, AI reliability, and beyond. Software updates for IoT devices go further, requiring HTTPS channels to deliver upgrade packages with code signing certificates to digitally sign them. Devices verify these signatures and timestamps before installation, ensuring security without bulky antivirus systems.

Email security follows suit. IMAP and SMTP services must enable TLS encryption for transmission using TLS/SSL certificates, while email certificates provide end-to-end encryption, keeping content secure in cloud mailboxes. Digital signatures confirm sender authenticity and prevent tampering, certificate encryption safeguards emails throughout their lifecycle. For electronic documents, digital signatures verify the publisher's identity and integrity, while encryption restricts access to authorized readers, preventing leaks. Cryptography is the answer to these modern threats.

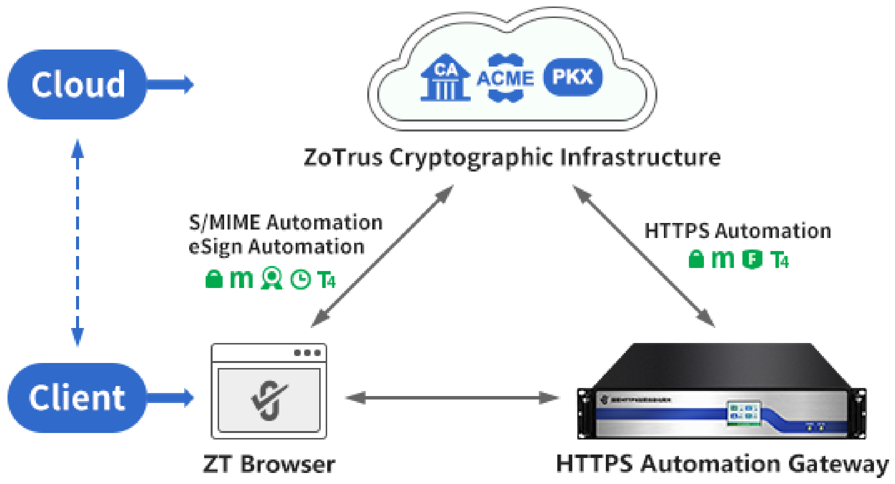
3. Why Automation Matters

HTTPS encryption, invented in 1994, only became widespread recently. Why the delay? Cryptography is powerful but complex. Deploying HTTPS requires SSL certificates, compatible web servers, and browsers, plus manual effort to apply for and install certificates from Certificate Authorities (CAs). For a few servers, this is manageable, but in the IoT era, where every device and app needs encryption, it needs many Web servers to collect and process the IoT data, manual processes collapse. Automation changed the game. Let's Encrypt, launched in 2015, offers free, automatic SSL certificates, claiming the largest market share in just three years. Since the Certificate Transparency log began in 2013, over 12 billion trusted TLS/SSL certificates have been issued, with more than 1 billion actives today - a scale only the IoT could drive.

Email encryption lags behind. Despite email's 54-year history and the S/MIME standard for email encryption is introduced in 1995, most of the 300 billion daily emails remain unencrypted plain text in cloud servers. TLS secures transmission is made, but content security needs to catch up. Document signing and code signing face the same hurdle: though valuable, think electronic contracts, manual certificate management limit their reach. Automation is the key to unlocking cryptography's full potential across these domains.

4. ZoTrus: Automation Meets Innovation

ZoTrus Technology delivers with a client-cloud integration model. The "client" includes ZT Browser and ZoTrus HTTPS Automation Gateway; the "cloud" is the ZoTrus Cloud Cryptography Infrastructure. Sensitive data stays on the client (ZT Browser) for privacy, while the Gateway automates HTTPS without requiring web server overhauls or ACME client installations. The cloud provides computing power and services to make it automated.



This synergy powers:

- **HTTPS Automation Service**: The Gateway auto-configures SSL certificates and enables HTTPS encryption with adaptive algorithms, no server tweaks needed.
- **S/MIME Automation Service**: ZT Browser handles email certificate automation, public key exchange and key management automation, and automates encryption, signature, and timestamp.
- **eSign Automation Service**: Beyond browsing PDF documents, ZT Browser verifies digital signatures in real time, auto-configures document signing and encryption certificates, and applies them for eSign automation.

5. Making Cryptography Visible

ZT Browser doesn’t stop at automation, it makes cryptography tangible with a groundbreaking UI:

For Websites (HTTPS):

- Padlock Icon: Signals HTTPS encryption in the address bar.
- SM2 Algorithm Icon: Highlights SM2 algorithm encryption.
- WAF Protection Icon: Indicates web application firewall protection.
- Trust Level Icon: Displays validated website trusted identity information.

For Emails (S/MIME):

- Padlock Icon: Marks encrypted emails.

- SM2 Algorithm Icon: Highlights SM2 algorithm encryption.
- Digital Signature Icon: Verifies sender identity and integrity.
- Timestamp Icon: Ensures trusted email sending time.
- Trust Level Icon: Shows validated sender trusted identity information.

For Documents (eSign):

- Padlock Icon: Confirms encryption.
- SM2 Algorithm Icon: Notes SM2 algorithm encryption.
- Digital Signature Icon: Validates publisher identity and document integrity.
- Timestamp Icon: Guarantees a trusted timestamp of signing.
- Trust Level Icon: Reflects validated publisher trusted identity information.

6. Empowering Trust Online

ZT Browser integrates a PDF reader and email client, automating HTTPS, email, and document security while showcasing their effects through a unique UI. By simplifying cryptography and making it visible, it transforms an abstract technology into a user-friendly reality. This dual innovation - automation and visibility, enhances online trust, paving the way for secure digital transactions worldwide.

Richard Wang

March 10, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 87 articles in English (more than 114K words)
and 204 articles in Chinese (more than 597K characters in total).