How ZoTrus Bridges the Gap Between Digital Certificates and Real-World Applications

From Certificate Management Automation to Cryptographic Application Automation

November 9, 2026

Digital certificates have been around for decades. Certificate Authorities (CAs) issue certificates, Public Key Infrastructure (PKI) provides the foundation of digital trust, and cryptographic technologies such as RSA, ECC, and SM2 are widely available. Post-quantum cryptography is also moving toward practical deployment. Yet, for many individuals and organizations, using digital certificates in everyday applications remains complicated.

Having a certificate does not mean knowing how to use it. Users still need to understand certificate requests, certificate formats, install certificates, configure applications, manage private keys, and perform cryptographic operations manually. Organizations face even greater challenges. They must manage large numbers of certificates, integrate cryptographic capabilities into existing business systems, maintain security infrastructure, and keep up with evolving cryptographic standards and compliance requirements.

The fundamental problem is not the absence of digital certificates or cryptographic technologies. It is the gap between having cryptographic resources and actually using them effectively in real-world applications. Digital certificates provide the foundation of trust. But the real problem is that trust cannot be easily and consistently delivered to everyday applications.

1. Where Does the Gap Between Certificates and Applications Exist?

The gap is not caused by a single technical problem. It involves several interconnected challenges.

(1) Certificate Management Gap

A digital certificate is not a one-time product. It has a complete lifecycle, including:

- Certificate application and identity validation
- Certificate issuance and deployment
- Certificate renewal and replacement
- Certificate revocation

© 2026 **ZoTrus Technology Limited**

- Certificate and private key management

As certificate lifetimes become shorter, certificate quantities increase, and cryptographic requirements evolve, manual management becomes increasingly difficult and inefficient. Without automation, certificate management can become a significant operational burden.

(2) Cryptographic Application Gap

Even when users possess valid digital certificates, their applications may not know how to use them automatically. For example:

- Email clients need proper S/MIME configuration to sign and encrypt messages.
- Document applications need to integrate digital signing, signature verification, encryption, and decryption.
- Web services need certificates to be correctly deployed and maintained for HTTPS connections.

The availability of certificates does not automatically translate into practical cryptographic capabilities.

(3) Infrastructure Integration Gap

Organizations often have existing CAs, HSMs, identity management systems, security gateways, and business applications. However, these systems may operate independently, without an automated mechanism to coordinate certificate management and cryptographic operations.

Integrating cryptographic capabilities into existing business environments can require considerable development, deployment, and maintenance resources.

(4) Usability Gap

Cryptographic technologies are inherently specialized. But ordinary users should not need to become cryptography experts to benefit from digital trust. Users want their emails to be signed and encrypted automatically, their documents to be signed and verified conveniently, and their websites to have HTTPS secure connections without having to manage certificates manually.

Cryptography should become a natural part of the application workflow, not another technical task imposed on users.

© 2026 **ZoTrus Technology Limited**

2. ZoTrus Approach: From Certificate Management Automation to Cryptographic Application Automation

ZoTrus was established to address this gap. Our approach is built on two complementary capabilities:

(1) Certificate Management Automation

Certificate Management Automation addresses how digital certificates are obtained, deployed, maintained, and managed throughout their lifecycle. It automates essential certificate operations, including:

- Certificate enrollment and issuance workflows
- Certificate deployment
- Automatic renewal and replacement
- Certificate lifecycle management
- Integration with CA services and existing infrastructure

ACME (Automatic Certificate Management Environment), defined in RFC 8555, is an important standardized mechanism for automating certificate management. However, certificate management automation is not limited to ACME. Different application environments may require different integration methods and management mechanisms.

(2) Cryptographic Application Automation

Cryptographic Application Automation addresses a different but equally important question: How can applications actually use digital certificates and cryptographic capabilities automatically? It integrates cryptographic operations into real-world application workflows, including:

- Digital signing and signature verification
- Encryption and decryption
- Certificate-based identity recognition
- Automated cryptographic operations
- Integration with existing applications and business systems

Certificate Management Automation makes certificates available and manageable. Cryptographic Application Automation makes those certificates useful in real-world applications. Together, these two

© 2026 **ZoTrus Technology Limited**

capabilities form the foundation of the ZoTrus technology approach.

3. How ZoTrus Bridges the Gap in Practice

ZoTrus Technology has spent more than 5 years truly implementing certificate management automation and cryptography application automation in three practical application areas: website security, email security (including Chat Security based on email system), and document security.

(1) Website Security: Making SSL Certificate and HTTPS Automatic

HTTPS is essential for protecting communication between websites and their visitors. However, deploying and maintaining SSL/TLS certificates across multiple websites and servers can be operationally demanding.

ZoTrus provides automated certificate management and HTTPS deployment capabilities to simplify this process. Key capabilities include:

- ACME-based automatic certificate enrollment and renewal.
- Support for RSA, ECC, SM2 and Hybrid PQC cryptographic algorithms.
- Automated SSL certificate deployment.
- Support for different CA services and certificate management environments.
- Integration of HTTPS automation with gateway-based security capabilities.
- Built-in Web Application Firewall (WAF) protection in the ZoTrus HTTPS Automation Gateway.

ZoTrus HTTPS Automation Gateway combines SSL certificate automation with gateway-based security protection, helping organizations deploy and maintain secure websites more efficiently.

The goal is to make SSL certificate management and website protection an automated part of web infrastructure.

(2) Email Security: Making S/MIME certificate and S/MIME Automatic

S/MIME provides standardized mechanisms for digital signatures and encryption for email security. However, practical deployment often requires certificate enrollment, installation, configuration, and

© 2026 **ZoTrus Technology Limited**

ongoing management.

For ordinary users, these steps can become barriers to adopting email security. For organizations, managing S/MIME certificates and cryptographic operations across existing email infrastructure can be even more challenging.

ZoTrus addresses these challenges through ZTmail. ZTmail provides automated S/MIME capabilities for email and chat, including:

- Automated S/MIME certificate enrollment and lifecycle management.
- Automatic digital signing and encryption of outgoing emails.
- Automatic verification of signed emails.
- Automatic decryption of encrypted emails.
- Certificate-based sender identity recognition and UI display.
- Support for individual users, small and medium-sized businesses, and enterprise environments.

ZTmail offers two implementation paths:

- **ZTmail App**

A user-oriented application that makes S/MIME encryption and digital signatures accessible to individuals and small businesses, without requiring them to manage complex certificate operations manually.

- **ZTmail Gateway**

An enterprise solution that integrates with existing email infrastructure through SMTP and IMAP proxy capabilities, automating S/MIME operations while supporting centralized certificate and identity management.

By combining certificate management automation with automated cryptographic operations, ZTmail makes secure email communication part of the normal email workflow.

The goal is to make S/MIME practical, accessible, and automatic for everyone.

(3) Document Security: Making Digital Signing and Encryption Part of the Workflow

Digital signatures are essential for establishing document authenticity and integrity. Document encryption also helps protect sensitive information from unauthorized access. However, traditional

© 2026 **ZoTrus Technology Limited**

document signing and encryption workflows can involve separate applications, manual certificate selection, complex configuration, and additional operational steps.

ZoTrus Sign brings certificate-based digital signing and cryptographic operations into document workflows. Its capabilities include:

- Automated document certificate enrollment and lifecycle management.
- Digital signing of local documents.
- Digital signing of email attachments.
- Digital signature verification and signer identity display.
- Document encryption and decryption.
- Trusted timestamping.
- Long-Term Validation (LTV) support.
- Cloud signing based on the Cloud Signature Consortium (CSC) standard.

One distinctive feature of ZoTrus cloud signing is that the original document does not need to be uploaded to the cloud signing platform. Instead, ZTmail App generates a document hash and submits it to the cloud signing service for signing, then the signed hash goes back to ZTmail App to complete the digital signature locally. This approach helps protect document privacy and confidential business information while enabling cloud-based signing.

By integrating document signing into the email workflow and supporting local document operations, ZoTrus makes digital signatures more accessible in everyday work.

The goal is to make document signing, encryption, and verification a natural part of document handling.

4. From Individuals to Enterprises: Two Paths to Cryptographic Automation

Different users have different requirements for deploying cryptographic capabilities. Individuals and small businesses need simple applications that work with minimal configuration. Large organizations need centralized management, integration with existing infrastructure, and control over cryptographic operations.

ZoTrus addresses these requirements through two complementary implementation paths.

© 2026 **ZoTrus Technology Limited**

(1) Application-Based Automation

For individuals and smaller organizations, applications such as ZTmail App provide ready-to-use cryptographic capabilities. Users can perform email and document security operations without having to understand the underlying certificate management and cryptographic processes.

(2) Gateway-Based Automation

For enterprises, the ZoTrus Gateway approach integrates cryptographic capabilities into existing infrastructure. Instead of requiring organizations to replace their current business applications, the gateway operates alongside existing systems to automate certificate management and cryptographic operations.

Supporting components include:

- HTTPS Automation Gateway
- ZTmail S/MIME Automation Gateway
- Document Cryptographic Automation Gateway
- Enterprise Key Management System (EKMS)
- Timestamping Service System

This approach allows organizations to introduce cryptographic automation while preserving their existing business workflows and infrastructure investments.

Different deployment paths. One consistent objective: make cryptographic applications automatic.

5. Preparing for the Evolution of Cryptography

Cryptographic technologies continue to evolve. RSA and ECC have provided the foundation for modern digital security. SM2 supports China's commercial cryptographic requirements. Meanwhile, the development of post-quantum cryptography is creating new requirements for future-proof cryptographic infrastructure. Supporting multiple algorithms is only part of the challenge. Applications and infrastructure must also be able to adapt as cryptographic standards and security requirements change.

© 2026 **ZoTrus Technology Limited**

ZoTrus embraces cryptographic agility through its support for multiple cryptographic algorithms and evolving application requirements. The technology direction includes:

- RSA, ECC, and SM2 cryptographic support.
- International and Chinese commercial cryptographic standards.
- Post-quantum cryptography readiness.
- Hybrid cryptographic mechanisms.
- Adaptable certificate management and cryptographic application workflows.

Cryptographic agility is not simply about supporting more algorithms. It is about making cryptographic evolution manageable for real-world applications.

ZoTrus believes that cryptographic automation is essential to making future cryptographic technologies practical and accessible.

6. ZoTrus Vision: Making Cryptography Accessible, Automatic, and Practical

The digital world has already established the foundations of cryptographic trust through digital certificates, CAs, PKI, and standardized cryptographic technologies. But these foundations should not remain isolated technical resources. They should work seamlessly within the applications people use every day. This is why ZoTrus focuses on connecting certificate management with real-world cryptographic applications.

ZoTrus vision is built around three principles:

(1) Make Cryptography Accessible

Make professional cryptographic capabilities available to ordinary users and organizations, without requiring specialized technical knowledge.

(2) Make Cryptographic Applications Automatic

Automate certificate management and cryptographic operations so that digital signing, encryption, decryption, and verification become natural parts of application workflows.

(3) Make Digital Trust Visible and Actionable

© 2026 **ZoTrus Technology Limited**

Help users and systems recognize trusted identities, verify digital signatures, and understand the security protections behind their communications and documents.

Digital certificates are the foundation. Automation makes them useful. Applications make digital trust real. ZoTrus, Cryptography for Trust, Automation for Security, AI for Productivity.

ZoTrus are committed to making cryptographic application automation accessible to everyone, helping bridge the gap between digital certificates and the applications that depend on them.

Richard Wang

November 9, 2026
In Shenzhen, China

Follow ZTmail at X (Twitter) for more info.
The author has published 142 articles in English (more than 206K words) and 301 articles in Chinese (more than 913K characters in total).

© 2026 **ZoTrus Technology Limited**