S/MIME Certificate Automation: A New Growth Opportunity for CAs

November 16, 2026

The traditional SSL/TLS certificate market has changed dramatically. Free certificates and bundled services have taken over most of the basic DV certificate market, putting increasing pressure on traditional commercial CAs. Continuing to rely primarily on conventional SSL/TLS certificate sales is no longer a sustainable growth strategy. Where should CAs look for their next growth opportunity?

S/MIME certificate automation offers a promising answer.

1. The Opportunity: S/MIME Is Ready for Automation

1.1 The Standards Are in Place. The Implementation Gap Is the Opportunity.

S/MIME is a mature, internationally standardized technology for email digital signatures, sender identity validation, and message encryption. Yet its adoption remains far below its potential, largely because obtaining, installing, configuring, renewing, and managing S/MIME certificates is still too complicated for ordinary users and many organizations.

A significant step toward making S/MIME easier to deploy was the incorporation of ACME-based email certificate automation into the S/MIME Baseline Requirements. On July 2, 2025, the CA/Browser Forum published S/MIME Baseline Requirements version 1.0.10 following Ballot SMC012, incorporating RFC 8823, which defines ACME for S/MIME certificate issuance. This established a standardized approach for automating S/MIME certificate issuance and mailbox control validation.

However, the publication of a standard does not mean that every CA already operates an ACME Service for S/MIME. CA-side implementation, deployment, and operational readiness still require investment. Email clients and applications must also support the corresponding automation workflows.

This implementation gap is precisely where the opportunity lies. CAs do not need to wait until every part of the ecosystem has independently completed its ACME implementation. An alternative, practical route is already available: integrate existing CA system APIs with an external ACME automation service.

ZoTrus provides this automation and integration capability. Instead of requiring a CA to immediately build and operate a complete ACME Service for S/MIME, ZoTrus can connect its existing certificate issuance APIs to the ACME automation workflow and ZTmail applications. This allows a CA to take advantage of the existing S/MIME standards while significantly reducing the time and effort required to enter the automated S/MIME market.

© 2026 **ZoTrus Technology Limited**

1.2 Why Now?

Several factors make this an important opportunity for CAs:

- **A mature technology:** S/MIME already provides standardized digital signatures, identity validation, and email encryption.
- **A standardized automation framework:** RFC 8823 provides the ACME framework for S/MIME certificate issuance.
- **An underserved market:** The complexity of certificate management continues to prevent widespread S/MIME adoption.
- **Growing security awareness:** Individuals and organizations increasingly need trustworthy email identities and encryption protection for sensitive communications.
- **AI is changing the BEC threat landscape**: As AI becomes more widely used in email and attackers use it to produce highly convincing, personalized messages at scale, traditional content-based email security detection becomes more challenging. Cryptographic sender identity, supported by S/MIME digital signatures, gives recipients a way to validate the sender's identity and detect changes to signed content.
- **A proven automation precedent**: ACME played a major role in making SSL/TLS certificates widely accessible by automating certificate issuance and renewal. CAs that move early to S/MIME certificate automation can gain a similar first-mover advantage by helping shape the market as it develops.
- **An available implementation path:** ZoTrus can integrate existing CA APIs with automated certificate management and application workflows.

The market does not simply need more S/MIME certificates. It needs S/MIME certificates that ordinary users can actually obtain, configure, renew, and use. The history of SSL/TLS automation shows what standards-based automation can make possible. ACME helped turn certificate issuance and renewal into scalable, widely adopted services. CAs that participate early in S/MIME automation have an opportunity to gain first-mover advantage in the next stage of certificate-based digital trust.

2. The Solution: No CA System Changes, Fast to S/MIME Automation Market.

2.1 Keep Your Existing CA Infrastructure. Add S/MIME Automation.

The most important advantage of the ZoTrus partnership model is its simplicity. A CA does not need to change its existing CA system, redesign its certificate issuance processes, or immediately develop its own complete ACME Service for S/MIME. ZoTrus can work with the CA's existing APIs to provide the automation and integration layer.

The CA retains control over its existing business and certificate services, including:

(1) Certificate products, policies, and pricing.

© 2026 **ZoTrus Technology Limited**

(2) Customer relationships and sales channels.
(3) Identity validation and mailbox control validation.
(4) Certificate issuance and trust services.
(5) Existing CA infrastructure and operational processes.

ZoTrus provides the automation capabilities required to connect the CA's existing services with automated S/MIME applications.

2.2 What the CA Provides

The participating CA provides:

(1) Existing S/MIME certificate products and issuance capabilities.
(2) API access for certificate application, validation workflow interaction, issuance, and certificate retrieval, as supported by its existing systems.
(3) Its existing identity validation and certificate issuance procedures.
(4) Certificate policies, pricing, and customer support.

The CA remains the certificate issuer and retains responsibility for its certificate issuance decisions and trust services.

2.3 What ZoTrus Provides

ZoTrus provides:

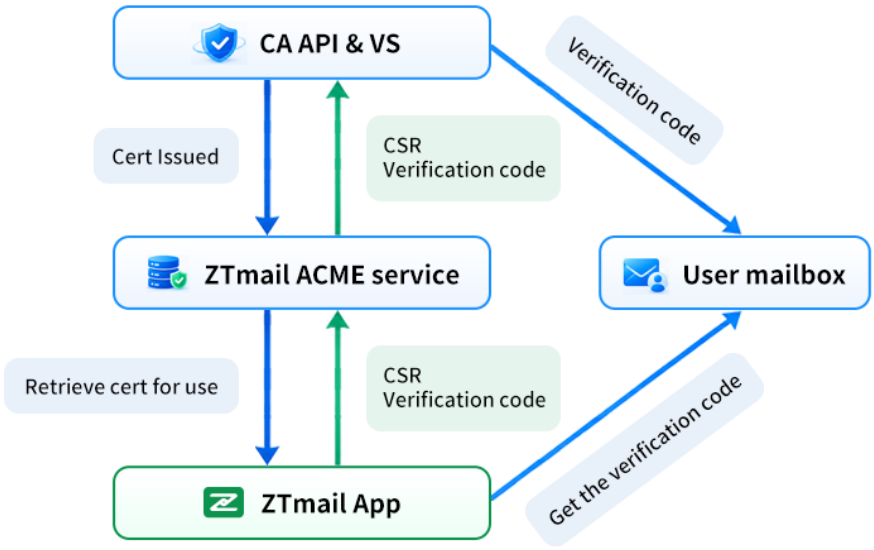
(1) API integration with the CA's existing certificate services.
(2) An ACME automation service for S/MIME certificate management.
(3) Automated CSR submission and certificate request handling.
(4) Integration with the CA's validation workflow, including verification information and challenge handling according to the CA's policies and API capabilities.
(5) Certificate retrieval and delivery to the requested application.
(6) Automated certificate configuration and lifecycle management through ZTmail.

The exact integration workflow can be adapted to each CA's existing API capabilities and certificate issuance policies, the solution does not require every CA to adopt an identical validation process and certificate issuance.

2.4 How Integration Works

The overall workflow is straightforward as shown as following figure:

© 2026 **ZoTrus Technology Limited**

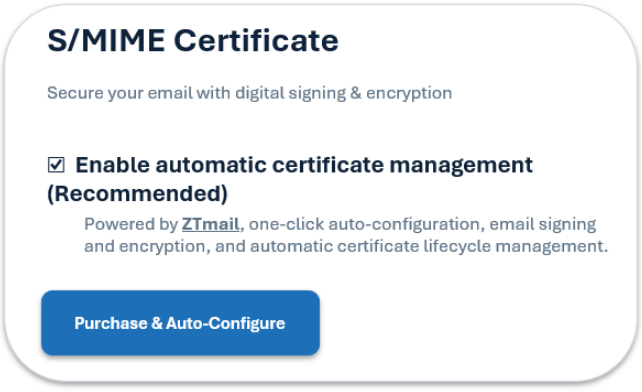


(1) The user initiates an S/MIME certificate request through ZTmail App.
(2) ZTmail App submits the certificate request and CSR to the ZTmail ACME Service.
(3) The ZTmail ACME Service connects to the CA through its existing traditional API.
(4) The CA performs the required validation and sends a verification code to the user's mailbox.
(5) ZTmail App retrieves the verification email, extracts the verification code, and submits it to the ZTmail ACME Service.
(6) The ZTmail ACME Service submits the verification code to the CA through its traditional API.
(7) The CA completes the certificate issuance process in accordance with its own policies.
(8) The ZTmail ACME Service retrieves the issued certificate by API and returns it to ZTmail App.
(9) ZTmail App automatically configures the certificate for email signing and encryption.

The user does not need to manually handle complicated certificate installation and configuration procedures. The objective is to turn certificate application and issuance into a usable, automated email security experience.

2.5 Add One Option to Your Existing S/MIME Certificate Sales Page

A participating CA can retain its existing S/MIME certificate products and sales process while adding a simple option to its certificate purchase page like this:



© 2026 ZoTrus Technology Limited

Customers who select this option can use ZTmail to automate certificate configuration and lifecycle management. The CA continues to sell its own certificates under its own brand, policies, and pricing. ZoTrus supplies the automation and application integration behind the service. This creates a new service offering without requiring a major redesign of the CA's existing business model.

2.6 Turn Standards into Market Opportunities, Without Waiting.

CAs can enter the automated S/MIME market now, using their existing APIs and infrastructure, rather than waiting until they have independently developed and deployed a complete ACME Service for S/MIME. ZoTrus provides the integration and automation layer. ZTmail App and ZTmail Gateway bring automated certificate management and practical S/MIME capabilities into real email workflows.

3. Business Value: Minimum Investment, Maximum Return

For a CA, the value of this partnership goes beyond adding another certificate product. It creates an opportunity to expand certificate sales while reducing the operational complexity traditionally associated with S/MIME.

3.1 New Revenue Opportunities

By offering automated S/MIME certificate services, CAs can reach customer segments that have historically found S/MIME too complicated to adopt. Potential customers include:

(1) Individual users who want trustworthy email identities.
(2) Professionals who need digitally signed and encrypted email.
(3) Small and medium-sized businesses.
(4) Enterprises seeking standardized email security.
(5) Organizations with regulatory, compliance, or confidentiality requirements.

Automation makes S/MIME more accessible, helping convert previously untapped demand into actual certificate sales.

3.2 Lower Technical Support Costs

One of the major obstacles to S/MIME adoption is the technical support burden associated with certificate installation, configuration, renewal, and troubleshooting. Automation can reduce many of these manual tasks. By allowing ZTmail App and gateway to manage certificate configuration and lifecycle operations, the participating CAs can potentially reduce support requests and operational costs while improving customer experience.

© 2026 **ZoTrus Technology Limited**

3.3 Better Customer Experience and Retention

Customers are more likely to continue using a certificate service when it works reliably within their daily email workflow. Automated certificate management reduces the need for users to understand complicated PKI procedures. This can improve customer satisfaction, increase renewal opportunities, and strengthen long-term customer relationships.

3.4 Market Differentiation

As basic SSL/TLS certificates become increasingly commoditized, CAs need to differentiate themselves through services that deliver more value than certificate issuance alone. Automated S/MIME services provide a practical opportunity to demonstrate that a CA can deliver not only trusted certificates, but also an easier way for customers to use them.

3.5 A New Market Without Building Everything from Scratch

Most importantly, CAs can enter this market without first investing in an entirely new application platform or independently building every component of the automation ecosystem. By leveraging existing APIs and the ZoTrus platform, a CA can focus on what it already does best: identity validation, certificate issuance, and trust services.

ZoTrus handles automation and application integration. The strategy is to minimize additional investment while opening a new market and creating additional certificate revenue.

4. A Win-Win Partnership: CA and ZoTrus

The partnership is designed around complementary capabilities rather than competition. Each participant focuses on its core strengths.

4.1 The CA: Certificate Issuance and Trust

The CA remains the trusted certificate issuer. It provides certificate products, identity validation, issuance services, certificate policies, and the associated trust infrastructure. It retains its brand, pricing, customer relationships, and control over certificate issuance.

4.2 ZoTrus: Automation and Integration

ZoTrus provides the technology that connects CA services with real-world applications. Its two core capabilities are:

(1) Certificate Management Automation.

© 2026 **ZoTrus Technology Limited**

(2) Cryptographic Application Automation.

For S/MIME, ZoTrus connects existing CA APIs to automated certificate management workflows and integrates those workflows with email applications. ZoTrus is not intended to replace the CA or become a competing certificate issuer. It acts as an automation and integration layer that helps CAs deliver more value through their existing certificate services.

4.3 ZTmail: Bringing S/MIME into Everyday Communication

ZTmail turns certificate automation into practical services for users and organizations.

- **ZTmail App: For Individuals and SMBs**

ZTmail App makes S/MIME easier to use by automating certificate management and integrating digital signing, signature verification, encryption, and decryption into everyday email workflows.

- **ZTmail Gateway: For Enterprises and Organizations**

ZTmail Gateway provides enterprise-level S/MIME automation through SMTP and IMAP proxy integration with existing email infrastructure. It enables organizations to automate email signing, verification, encryption, decryption, and certificate management without requiring users to change their existing email clients.

Together, ZTmail App and ZTmail Gateway provide two implementation paths for bringing automated S/MIME services to individuals, businesses, and enterprises.

4.4 A Larger Market Benefits Everyone

The partnership is not a zero-sum business model. It is designed to expand the overall S/MIME certificate market:

(1) CAs gain more certificate customers and new revenue opportunities.
(2) ZoTrus expands its open certificate automation ecosystem.
(3) ZTmail reaches more users and organizations through the participating CAs.
(4) End users gain access to practical, automated email security.

The more CAs participate, the more choice customers have. The more applications support automated S/MIME, the more valuable the entire ecosystem becomes.

5. Building an Open S/MIME Automation Ecosystem

ZoTrus intends to work with CAs around the world to build an open, interoperable S/MIME automation ecosystem. We welcome cooperation with both established international CAs and regional certificate authorities. The partnership model is designed to be non-exclusive. Each CA can retain its own brand, certificate products, pricing, policies, validation procedures, and customer relationships.

© 2026 **ZoTrus Technology Limited**

ZoTrus provides a common automation and integration capability that allows different CA services to be accessed through a consistent application experience. This approach can help reduce fragmentation and make automated S/MIME services available to a much wider market.

5.1 Supporting the Evolution of S/MIME Standards

ZoTrus also intends to apply for participation in the CA/Browser Forum S/MIME Certificate Working Group. We believe that practical implementation experience from certificate automation platforms and email applications can contribute valuable perspectives to the continued development of S/MIME standards.

Our goal is to support an ecosystem in which standards, CA services, automation platforms, and email applications evolve together.

5.2 Beyond a Business Opportunity: A Better Future for Email Security

The significance of S/MIME automation extends beyond the commercial interests of CAs and technology providers. Email remains one of the world's most important communication channels. Yet message-level identity assurance and content protection are still not consistently available to ordinary users.

TLS protects communication in transit between systems, but transport encryption alone does not provide the same end-to-end message protection as S/MIME. S/MIME addresses this gap through digital signatures and message encryption:

(1) Digital signatures help recipients verify the sender's identity and detect changes to signed content.
(2) Message encryption helps protect email content from unauthorized access.
(3) Certificate-based identities provide a foundation for trusted digital communication.

Technology already exists. The standards are established. What has been missing is an accessible way to make these capabilities work in everyday email. By reducing the complexity of certificate management and integrating S/MIME into normal email workflows, ZTmail aims to help make trustworthy, encrypted email much more widely accessible.

This is not only a new business opportunity for CAs. It is also an opportunity to improve the security of global email communications.

6. Make S/MIME Automatic. Expand the Market Together.

The traditional SSL/TLS certificate market has changed. For commercial CAs, finding new growth opportunities is no longer optional. S/MIME offers a substantial opportunity, but its growth depends on making certificates easy to obtain, configure, renew, and use.

© 2026 **ZoTrus Technology Limited**

The standards are in place. Technology is mature. The market needs practical implementation.

CAs do not need to wait for a complete in-house ACME implementation. By integrating existing APIs with ZoTrus automation services, they can enter the automated S/MIME market with minimal additional investment.

Beyond API Integration: Broader Partnership Opportunities

While API integration provides the fastest and most practical way for CAs to enter the S/MIME certificate automation market, cooperation with ZoTrus is not limited to this model. Depending on each CA's business strategy and market reach, partnership opportunities may also include reselling CA-issued certificates through ZTmail, as well as offering OEM-branded versions of ZTmail App and ZTmail Gateway.

ZoTrus welcomes discussions with CAs worldwide to explore flexible cooperation models that expand market reach, create new revenue opportunities, accelerate the adoption of S/MIME security, and bring trustworthy, encrypted email to more people and organizations around the world.

ZoTrus, Cryptography for Trust, Automation for Security, AI for Productivity.

Richard Wang

November 16, 2026
In Shenzhen, China

Follow ZTmail at X (Twitter) for more info.
The author has published 143 articles in English (more than 209K words) and 302 articles in Chinese (more than 918K characters in total).

© 2026 **ZoTrus Technology Limited**