RFC 8823: Bringing HTTPS-Style Certificate Automation to S/MIME

Why the ACME-email-aware Mail User Agent is the missing half of automated S/MIME certificates

September 22, 2026

HTTPS became operationally simple not because certificates stopped being complicated, but because TLS/SSL certificate management was increasingly moved into software. ACME turned certificate requests, validation, issuance, retrieval, and renewal into an automated workflow.

S/MIME has long provided the cryptography needed for secure email, yet certificate enrollment and lifecycle management have often remained separate from the email client. Why hasn't email achieved the same level of certificate automation?

1. HTTPS Made Certificate Management Automatic. Email Can Follow.

The success of HTTPS is often described as a story about encryption, but from an operational perspective, an equally important development was that certificate management gradually moved into software. ACME, standardized for certificate management in RFC 8555, allowed software to communicate with a certificate service, prove control of a resource, obtain a certificate, and repeat the process when renewal was required, moving users away from manually handling certificate files and administrative portals.

S/MIME has long provided the cryptography required for secure email, yet the operational work surrounding that cryptography has often remained outside the email application itself. An S/MIME certificate binds a public key to an email identity and enables signing, validation, encryption, and decryption, while the user-facing challenge lies in requesting the certificate, proving control of the mailbox, obtaining the issued certificate, configuring it in the email client, and keeping it current.

If those activities continue to exist as a separate administrative process, S/MIME remains a security capability that users must learn to manage; if they become part of the email client, however, the certificate can begin to behave more like HTTPS infrastructure than an administrative project. That raises a basic question: Why hasn't email achieved the same level of certificate automation?

2. RFC 8823 Defines the Missing ACME Layer for S/MIME

RFC 8823, published by the IETF in April 2021, extends ACME for end-user S/MIME certificates by introducing an “email” identifier type and the email-reply-00 challenge for demonstrating control over an email address. What makes the specification particularly significant is that it does not treat the email client as a passive consumer of certificates; instead, it explicitly describes a Mail User Agent (MUA) with a built-in ACME client that understands the ACME extensions as an “ACME-email-aware” MUA, including a user interface through which certificate issuance can be automated.

The architectural implication is important because a certificate authority can provide the ACME service for S/MIME certificate, the server-side machinery for automated issuance, but an email certificate ultimately must be used inside an email application. When that application understands the ACME workflow, it can initiate the request, recognize the expected challenge message, participate in mailbox validation, retrieve the certificate, and make it available for S/MIME operations without forcing the user to move between unrelated tools.

RFC 8823 therefore describes more than another certificate-validation mechanism: it provides a path for certificate automation to move closer to the application in which the certificate is used, making the email client an active participant in the lifecycle rather than simply the destination for a certificate **issued somewhere else.**

3. How RFC 8823 Connects the Mailbox to ACME

The RFC 8823 workflow illustrates why the email client matters. The process begins when a user requests an S/MIME certificate for an email address, after which the ACME client creates an order using the new “email” identifier and the ACME server creates an email challenge. For an ACME-email-aware MUA, the client can retrieve and parse that challenge automatically rather than requiring the user to interpret and transfer the relevant information manually.

RFC 8823 defines a two-part token model in which one token component is delivered through the challenge email while another is obtained through HTTPS; the ACME client combines those components to calculate the required key authorization and prepares the response. The MUA then sends the response email in the format defined by the RFC, while the ACME client notifies the ACME server and checks the authorization status. Once the challenge has been validated, the certificate

request can be finalized and the issued S/MIME certificate retrieved.

The significance is not that every implementation must expose these protocol steps to the user; it is almost the opposite. The specification creates a path by which software can handle the underlying exchange as part of the application workflow, allowing certificate issuance to become an implementation detail rather than another task that users must understand before they can use secure email.

4. The CA Is Only Half of the Equation

This leads to an important distinction between protocol support and product support. An ACME-capable certificate service can provide the server-side machinery required for automated issuance, but that capability alone does not create an integrated email experience, because the other half of the workflow is the client in which the certificate will be used.

A standalone ACME tool can communicate with an ACME service, yet an ordinary user may still have to move between the ACME tool, the mailbox, and the email client, after which the issued certificate may need to be imported or configured separately. RFC 8823 recognizes this distinction by explicitly describing both models: an MUA can contain an ACME client, or certificate enrollment can be handled by a separate client.

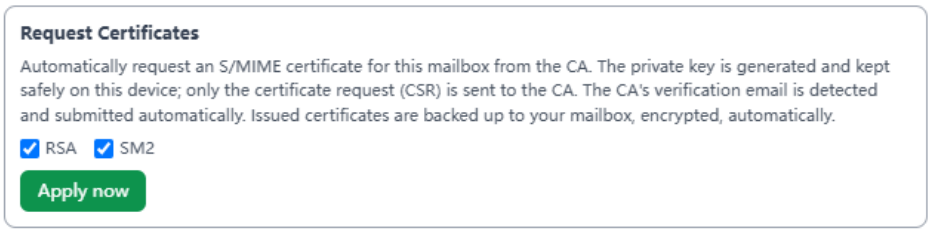
The ACME-email-aware model is the more application-integrated approach because the email client already has access to the mailbox and already knows that the resulting certificate is intended for email. It can therefore turn certificate enrollment into a native part of the email workflow, which is the point at which S/MIME begins to approach the operational model that made automated HTTPS certificates so effective.

5. ZTmail App Turns RFC 8823 into a Working Workflow

ZTmail App is built around the ACME-email-aware MUA model described by RFC 8823, integrating certificate enrollment into the application rather than requiring the user to obtain an S/MIME certificate elsewhere and then import it into the email client. The workflow follows a straightforward sequence: Request → Validation → Issuance → Automatic Configuration → Renewal, but the important point is that these stages are connected within the same application rather than presented as separate

administrative tasks.

The user initiates a certificate request from the App, after which the certificate automation service processes the request; when the verification email arrives, the App can detect the expected message as part of the certificate workflow, and once mailbox verification succeeds and the CA issues the certificate, the App can retrieve and configure it for S/MIME use. The same workflow can continue into lifecycle management rather than stopping at first issuance, allowing renewal to remain part of the application's ongoing operation.



This is the practical meaning of the ACME-email-aware MUA concept: the certificate is no longer a separate object that users must learn how to manage before they can use secure email, because certificate management becomes part of the application that already handles the user's email.

6. From Internal Implementation to Public Product

ZTmail implemented this certificate automation capability in internal testing during August 2026 and subsequently released the ZTmail App Global Public Beta on September 11, 2026. The public release brought automated S/MIME certificate enrollment into the email client and supports both RSA and SM2 algorithm certificate workflows.

The timeline matters because it separates the standards discussion from the product implementation. RFC 8823 has described the ACME-email-aware MUA model since 2021, while the CA/Browser Forum subsequently adopted ACME for S/MIME automation through Ballot SMC012 in 2025, adding ACME-based mailbox-control validation to the S/MIME Baseline Requirements. ZTmail's implementation puts the application side of that model into an actual email client in August 2026.

The result is therefore not simply an ACME endpoint or a certificate-ordering website, but an email application in which certificate enrollment, mailbox validation, certificate installation, and renewal are connected as one operational workflow, bringing the protocol model described by RFC 8823 into the place where users actually send and receive email.

7. One Application, Two Cryptographic Environments

The implementation also demonstrates that certificate automation does not have to be tied to a single cryptographic environment. For international interoperability, RSA remains a central S/MIME certificate model, while in China commercial cryptography environment, SM2-based certificates provide another important certificate ecosystem; ZTmail App can automate both RSA and SM2 S/MIME certificate enrollment within the same application workflow, this is thanks to ZoTrus Technology leading the creation of the China commercial cryptography industry standard 'Automatic Certificate Management Protocol', which references RFC8555 and RFC8823.

That means users do not need to learn two separate certificate-management procedures simply because the underlying algorithms and trust infrastructures differ. Instead, the application layer provides consistent experience while the certificate automation service and CA infrastructure handle the appropriate certificate process, allowing the operational workflow to remain stable even when the underlying cryptographic environment changes.

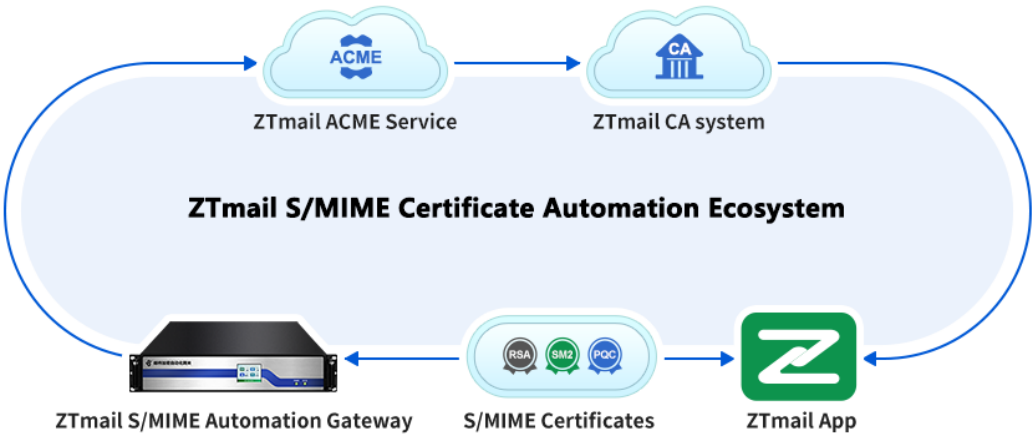
This is one of the practical advantages of treating certificate lifecycle management as application infrastructure: the complexity can remain below the application boundary, while the user-facing workflow stays consistent across different certificate and trust environments.

8. ZTmail Trust: Completing the Current Automation Loop

The current ZTmail implementation extends beyond the client itself. ZTmail App, ZTmail S/MIME

Automation Gateway, ZTmail ACME Service, ZTmail CA system, and ZTmail Trust MV certificates form an integrated trust and automation loop, providing not only ACME-aware client experience but also the corresponding certificate infrastructure needed to operate that workflow within the ZTmail Trust domain.

For the user, the practical result is that requesting, validating, issuing, deploying, and renewing a certificate can occur without turning certificate management into a separate administrative workflow. This is where the architecture described by RFC 8823 becomes a product rather than merely a protocol concept: the RFC provides the application model, while ZTmail implements that model in the email client and connects it to its own certificate automation and trust infrastructure.



The broader ecosystem question comes later. The immediate technical task is to make the core workflow operate end to end, so that certificate automation is not simply available as a protocol capability but is integrated into the application where the certificate is consumed.

9. RFC 8823 Defines the Path. ZTmail Makes the Path Usable.

RFC 8823 does not replace S/MIME, nor does it attempt to redesign the certificate authority ecosystem. Its contribution is more focused: it provides an ACME extension for end-user S/MIME certificates and explicitly recognizes that an email client can participate directly in certificate automation, a distinction that is easy to overlook when certificate management is treated as an activity that happens before or beside the email client.

For many years, the certificate lifecycle could be handled as a separate administrative process, with the resulting certificate eventually delivered to the application that needed it. RFC 8823 describes a different path, in which the email client itself becomes part of the automation system and can

participate in enrollment, mailbox validation, certificate retrieval, and the transition into actual S/MIME use.

ZTmail applies that model to a working product: the application can initiate certificate enrollment, participate in mailbox validation, obtain the issued certificate, use it for S/MIME, and continue managing its lifecycle, while ZTmail Trust provides the current integrated certificate and trust environment in which that workflow operates. The broader lesson is like HTTPS: automation creates its greatest value when protocol complexity disappears into software, allowing users to use encrypted and signed email without first becoming certificate administrators.

Standards define the path. ZTmail makes the path usable.

Richard Wang

September 22, 2026
In Shenzhen, China

Follow ZTmail at X (Twitter) for more info.
The author has published 134 articles in English (more than 188K words) and 292 articles in Chinese (more than 872K characters in total).