Understanding S/MIME Email Encryption (Part II)

This article continues the previous part "Understanding S/MIME Email Encryption (Part I)" and continues to explain S/MIME email encryption. In the previous part, the article focuses on the technical principles of S/MIME and two core products - S/MIME certificates and S/MIME clients. After reading the detailed introduction in the previous part, you may ask the following question: Why has such a good email encryption technology based on international standards not been widely used 27 years since the international standards were formed? This is a good question. This part will explain this problem, explain the difficulties encountered in implementing S/MIME email encryption, and briefly explain how ZoTrus Technology solves these problems.

1. Why has S/MIME technology not been widely used?

To successfully use S/MIME technology to implement email encryption, users must purchase and apply for an S/MIME certificate from a CA. This is not just a matter of cost, there is also a certificate application process. Users must manually apply for a certificate according to the CA's process and complete email validation after receiving the email verification code. For email certificates that need to be bound to personal or corporate identities, users also need to submit relevant identity validation proof documents and wait for the CA to complete identity validation. Once the CA issues an email certificate, users need to configure the email certificate to an email client that supports S/MIME technology. The configuration methods of each email client are different, and the configuration process is very cumbersome. This is the first difficulty – S/MIME certificate application and configuration.

The second difficulty is exchanging the public key. Once you have an email certificate, you must first exchange the public key with the recipient. The classic approach is to send a digitally signed plain text email to the recipient, who saves the sender's public key and replies with a digitally signed email to the sender, who saves the recipient's public key. This completes the exchange of public keys between the sender and the recipient. If there are 100 recipients, you need to do this 100 times, which is very cumbersome.

The third difficulty is key management. After users apply for email certificates from CA, they must manage the private and public keys of the certificates themselves and import these certificates into all email clients for use. If the certificate expires, a new certificate must be re-applied for. However, in order to decrypt previously encrypted emails, the expired certificate with private key must be kept available at any time for decrypting previously encrypted emails. These certificate management tasks are also very cumbersome, especially the private key protection password set when backing up the certificate must be remembered. Once forgotten, the certificate cannot be imported to decrypt encrypted emails.

These three difficulties are often stumped at the first step, where it is impossible to configure the email certificate to be used in the email client. The second difficulty is that exchanging public keys is not just a one-time exchange. When the certificate expires, the public key must be exchanged again. The third difficulty is not just managing one certificate. Multiple mailboxes require multiple certificates, and all email certificates over the years must be managed. This management process is more complicated than managing SSL certificates. Once an SSL certificate expires, it is useless and does not need to be managed anymore. These three difficulties are huge obstacles to the popularization of S/MIME email encryption, making it impossible for S/MIME technology to be popularized.

2. How does ZoTrus Technology solve the application difficulties of S/MIME encryption?

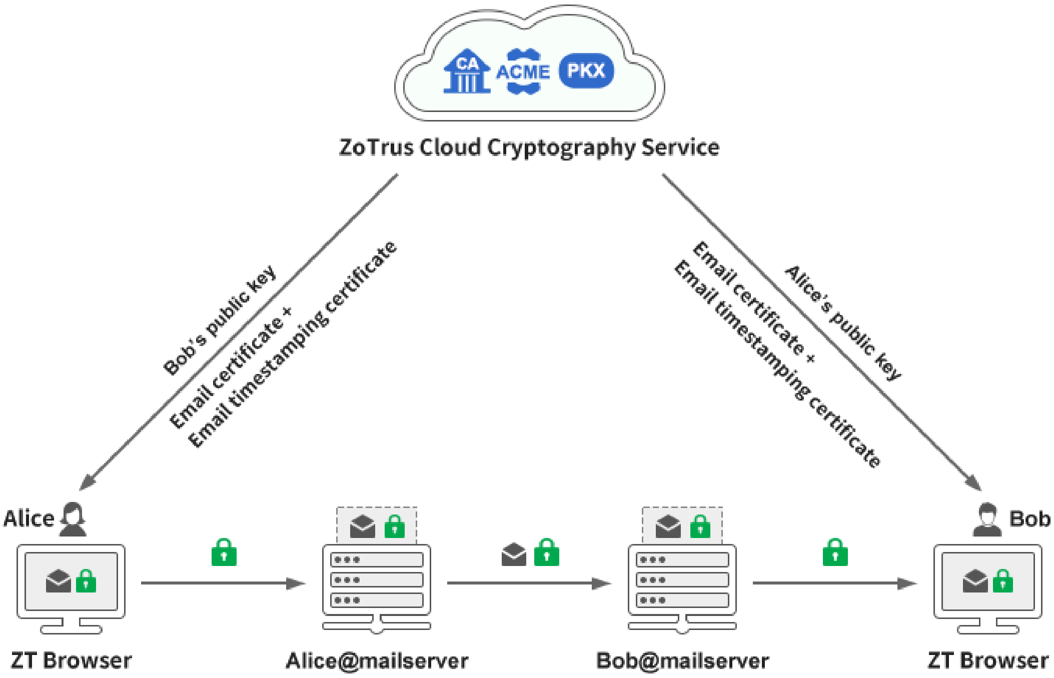
To solve the three difficulties faced by S/MIME email encryption, we must learn from the popularization of HTTPS encryption and implement automatic certificate management like SSL certificate, including automatic email certificate application, automatic mailbox control validation, automatic certificate configuration for use, automatic public key exchange, and automatic private key management. These automations are more difficult than automatic SSL/TLS certificate management, because they involve automatic certificate management for every email user, while SSL certificates only need to be implemented on each website, not on every website visitor.

ZoTrus Technology proposes corresponding automatic solutions to the three difficulties of S/MIME email encryption. This solution must be the integration of the email client and the CA system, and it must completely solve the current situation where the email client only uses certificates and the CA system only issues certificates. In fact, this integration capability is the advantage of ZoTrus Technology. The author (the company founder) has been engaged in CA business for 18 years and email client development for 4 years and knows the integration of the two.

In order to solve the first certificate application and configuration difficulty, ZoTrus Technology draws on the international standard for automatic management of SSL certificate (ACME) and the RFC standard proposal for automatic management of email certificates to achieve automatic issuance and configuration of dual-algorithm S/MIME email certificates. Users only need to set up their mailboxes to send and receive emails normally. ZT Browser will automatically connect to ZoTrus Cloud CA System to automatically apply for dual-algorithm email certificates and configure the issued email certificates for email encryption and digital signature. Users do not need to purchase and apply for email certificates from CA, do not need to manually complete email control validation, and do not need to tediously configure email certificates. Everything is done automatically.

In order to solve the second difficulty of public key exchange, ZoTrus Technology has built a public key exchange system. When a user writes an email to a recipient, ZT Browser will automatically connect to ZoTrus Public Key Exchange System to obtain the recipient's public key certificate. After the user finishes writing the email, they click Send to send an encrypted email without having to exchange public keys with the recipient in advance. This solves the problem of public key exchange and allows users to send encrypted emails without feeling anything.

In order to solve the third difficulty of key management, ZoTrus Technology's innovative solution is to use the user's own mailbox to back up and save the user's private key and certificate. As long as the user's mailbox is there, the private key is there, and ZT Browser can automatically obtain the private key to decrypt all encrypted emails, regardless of whether they are encrypted with an expired certificate or an unexpired certificate, and regardless of which device they are on. It can automatically obtain the key that the user has used to automatically decrypt all encrypted emails, and users don't have to worry about key management issues at all.



ZoTrus Technology uses an innovative client-to-cloud solution to achieve email certificate automation, public key exchange automation, and key management automation. These three automations ensure that users can realize email encryption and decryption, email digital signature and signature verification without feeling, and realize S/MIME encryption and digital signature automatically. And this automation service is completely free, including free configuration of email certificates, free implementation of email encryption and digital signature.

3. What other improvements and enhancements have been made to ZoTrus email encryption automation service?

ZoTrus Technology not only realizes the email certificate automation, public key exchange automation and key management automation, but also adds email timestamping service to email digital signature services based on existing digital signature technology and timestamp technology. Just like traditional paper letters have postmarks, each digitally signed email sent is automatically affixed with a timestamp signature, ensuring the trust of the email sending time.

Email digital signature ensures that the identity of the email sender is trusted and non-repudiable, email encryption ensures the integrity and confidentiality of the email content, and the email timestamping ensures that the email sending time is trusted and non-repudiable. It is particularly suitable for Internet applications that need to prove the email sending time. This is a global exclusive innovative application. In terms of key management, the traditional solution is to use a cloud key management system, which can indeed solve the problem of users managing their own keys, but it cannot solve the privacy protection issues that users are worried about. How to do a good job of cloud key management and permission management is the key. Users may not be confident that a third party will keep the keys used for encryption and decryption. ZoTrus Technology has improved the key management solution, which not only ensures the reliability and availability of keys stored in the cloud, but it also ensures that users manage their own keys and save their own keys in their own mailboxes. This is a perfect solution that can have the best of both worlds. This innovative key management solution realizes autonomous cloud storage of encryption keys.

Another improvement is the implementation of S/MIME encryption. The traditional way is to develop an independent email client software, which is also a common implementation method. However, considering the actual application scenario that users are accustomed to using a certain email client and do not want to install other email clients, ZoTrus Technology directly integrates the email client in the ZT Browser, so that users do not need to install independent email client software. For users who have not installed the ZT Browser, most users would like to install multiple browsers on their computers, if they need to install an extra browser to realize email encryption automation, it is acceptable. After all, ZT Browser is not only a free SM2 browser that supports the SM2 algorithm, but also a PDF reader and an encrypted email client, it does’t matter to install one. What’s more, after installing ZT Browser, Windows will be automatically patched to support the SM2 algorithm, and the automatically configured free email certificate can also be used for Outlook to decrypt all encrypted emails, killing two birds with one stone.

4. S/MIME technology can only be widely used if it is automated

Through the detailed explanation in the first half of this article, you can understand the history of S/MIME technology, the implementation principles of S/MIME encryption and digital signatures and understand S/MIME certificates and S/MIME clients. The second half of this article explains in detail why S/MIME technology is difficult to implement and how ZoTrus Technology innovatively solves this difficulty.

Just as the popularization of HTTPS encryption that everyone is familiar with benefits from the automatic management of SSL certificates, the only way to popularize S/MIME encryption is to use the automatic management of S/MIME certificates. Only by realizing the automatic management of S/MIME certificates can we truly take the first step in the implementation of S/MIME technology. ZoTrus Technology has not only taken this step, but also realized the automation of public key exchange in the second step, the automation of key management in the third step, and innovatively added the automation of email timestamping. The four automations perfectly realize the implementation of S/MIME standard technology, removing all technical barriers for the popularization of S/MIME technology to ensure global email security, allowing the ancient email to serve all mankind more securely.

Richard Wang

Feb. 24, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 86 articles in English (more than 113K words)
and 203 articles in Chinese (more than 593K characters in total).