How does ZT Browser realize the automatic email certificate management?

There are many ways to encrypt emails in the global market. The commonly used email encryption technology is S/MIME, and the commonly used email clients all support S/MIME email certificate encryption, but users need to apply for email certificates from CA and configure them in email clients for use. This process is as painful as applying for SSL certificates and configuring it in the Web server. To popularize email encryption technology, we must learn from the successful experience of SSL certificate automation management and solve the email certificate automation management problem. This article will talk about how ZT Browser can realize automatic email certificate management to archive email encryption automation.

1. Automatic email certificate management is the only way forward

As we can see, HTTPS encryption has basically been widely used in the global market, the credit for the popularization of HTTPS encryption should certainly be attributed to the SSL certificate automation management service pioneered by Let's Encrypt globally and the RFC8555 ACME standard. As a result, more than 90% of the world's SSL certificates have been automatically issued and deployed, thus quickly realizing the popularization of HTTPS encryption.

To achieve the goal of popularizing S/MIME email encryption, the only one way is to realize automatic email certificate management, because the traditional way of applying for email certificates from CA and configuring email certificates in email clients is very difficult, which makes it impossible to popularize S/MIME email encryption. Just like the path of HTTPS encryption automation, S/MIME encryption automation can only be achieved by email client developers. But now, the author has not seen any plans by the world's three leading email client providers, Apple Mail, Google Gmail, and Microsoft Outlook, to provide email certificate automation services. Although these email clients all support S/MIME email encryption, but they all require users to apply for email certificate from CA and configure them manually.

2. Is there any precedent for automatic email certificate management in the global market?

You can search for "email encryption automation". You probably won't find a definite answer except for a few related articles written by the author. However, the author found that Microsoft Office 365 already provides email encryption services, which can also be understood as automated. Although the author has not had the opportunity to test it, the information on the official website is certain that this is a solution like PGP/IBC encryption. Users can read encrypted emails seamlessly using Outlook. If it is not Outlook, they will receive a link to read encrypted emails online. This is obviously a cloud-based encryption and decryption solution, and its premise is that the email is already on the Microsoft cloud. This is not a true end-to-end encryption solution.

If other email encryption solutions support S/MIME, they must require users to apply for email certificate from CA and configure it for use manually, or other various encryption solutions. The author has not seen an automatic email certificate management solution based on international standards ACME, but a British company has submitted an RFC proposal for automatic management of email certificates based on ACME standard RFC8555 in April 2021, it is RFC8823. The status of this proposal is Informational, which belongs to the non-standard tracking category. This type of proposal refers to some information about the Internet community on specific topics, and it does not represent community consensus and suggestions, it is only for the next consideration and verification of whether it will become an experimental standard. The author carefully studied this proposal and found that the problem is that it requires the email client to reply to a specific email to the CA specified email address to complete the email validation. This is very unreasonable and does not conform to the current process of users applying for email certificates from CA. After receiving the verification code, the user copies and pastes the verification code to the certificate application page, or directly clicks the verification link to complete the email validation. In this way, CA does not need to build a system to automatically receive, and process emails replied by users. Not only that, but the author also found one minor errors and submitted an RFC Errata, which status is reported.

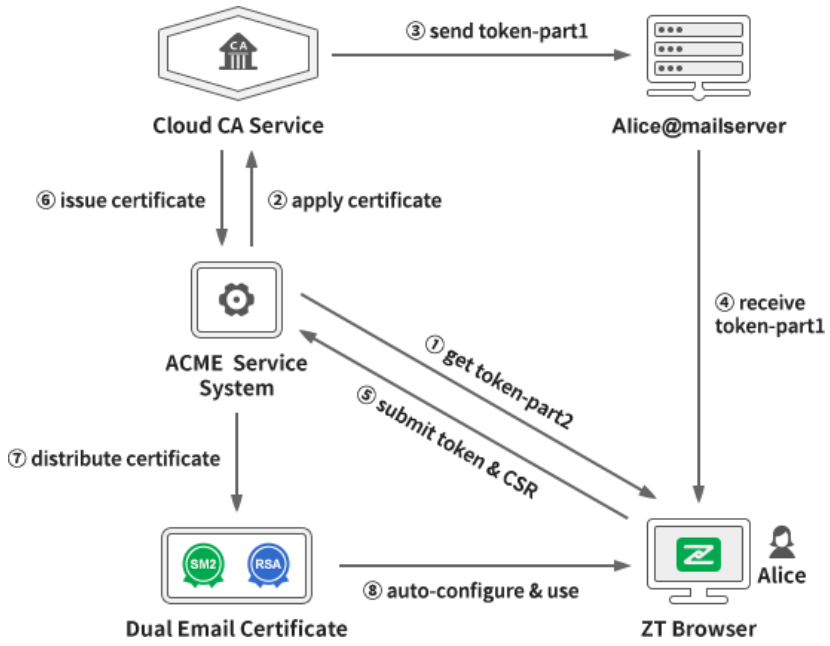
In other words, there is currently no precedent in the global market for truly end-to-end email encryption automation based on the S/MIME standard. ZoTrus Technology will set this precedent, being the first in the world to implement it, and it is the automatic management of dual-algorithm (RSA

and SM2) email certificates.

3. **ZT Browser is the first in the world to launch Automatic Email Certificate Management**

The Automatic Email Certificate Management (AECM) implemented by ZoTrus Technology adds automatic management of email certificates based on the automatic management of dual-algorithm SSL certificates implemented by ZoTrus Technology base on the Chinese Cryptography Standard draft – “Automatic Certificate Management Specifications” led by ZoTrus Technology. This solution also refers to RFC8823, but it improves its automatic verification code submission process. The email client automatically reads the email content containing the verification code and submits it to the ACME service system directly, no need to reply to the verification code by sending email, to automatically complete the email control validation. This improved process has been added to the draft Chinese standard of "Automatic Certificate Management Specifications".

The specific workflow is shown in the figure below. After the user sets up the email account in ZT Browser, ZT Browser automatically connects to the ZoTrus ACME Service System to obtain the second part of the verification code, token-part2. The ZoTrus Cloud CA Service sends the first part of the verification code, token-part1, to the email address where the user applies for the email certificate. The built-in email client of ZT Browser combines the two parts of the verification code obtained through the two channels into a complete Token and submits it with CSR to the ACME Service System to complete the email control validation and certificate application. In this way, the CA system can issue the dual-algorithm email certificate. After the certificates are issued, ZT Browser is responsible for connecting to the ACME Service System to retrieve the certificate and configure it for use. This entire process is the Automatic Email Certificate Management (AECM), which realizes the automatic application, automatic verification, automatic issuance, and automatic configuration of email certificates.



ZoTrus Automatic Email Certificate Management (AECM) is a system designed specifically for automatic management of email certificates based on the mature SSL Certificate Automation Management standard -ACME. It can not only automatically issue RSA/ECC algorithm email certificates, but also automatically issue SM2 algorithm email certificates. It can automatically configure dual-algorithm email certificates for users free of charge to realize email digital signature and encryption with adaptive algorithm. ZT Browser uses SM2 algorithm to implement email encryption and digital signature by default, and users can select the default cryptography algorithm.

In order to ensure the credibility of email sending time, ZoTrus Technology innovatively introduces the concept of Email Timestamp. While automatically configuring email certificates for users, it also automatically configures dual-algorithm timestamp signing certificates - Email Timestamping Certificate, and automatically configures them for use in ZT Browser. It digitally signs every email sent by users that refers to related standard to attach timestamp signature, to prove that the sending time of each email sent is trusted.

ZT Browser automatically configures 6 certificates for each mailbox for free, 3 certificates each for the RSA algorithm, and 3 certificates for the SM2 algorithm (optional), including one MV email signing certificate, one MV email encrypting certificate, and one MV email timestamping certificate. The RSA algorithm email certificate issued by CA is a single certificate that contains both signature

and encryption key usages. ZoTrus Technology adopts a dual usage separation mode, both the RSA algorithm and the SM2 algorithm use a single key usage certificate. This is to ensure that users can share the same encrypting certificate to decrypt previously encrypted emails when using ZoTrus Email Encryption Service on a second device. However, each new device will automatically configure a new signing certificate to distinguish and identify the new device. In other words, each email address has only one encrypting certificate, but multiple signing certificates. This is the main reason why a single key usage certificate with separated key usage is used. For paid users, ZT Browser will also automatically configure the IV/OV/SV email signing certificate of the corresponding validation level for the user, which is a dual-algorithm dual-certificate by default, and the user can set which email signing certificate as the default signing certificate.

ZoTrus Technology is the first in the world to realize the automatic management of email certificates based on the ACME standard and the RFC8823 proposal. Only in this way can the first major obstacle to the popularization of email encryption be removed, and the core components for implementing email encryption using S/MIME technology is the S/MIME certificate. More importantly, the S/MIME certificates configured by ZoTrus Email Encryption Automation Service are completely free. Only in this way can the popularization of email certificates for email encryption be realized, effectively ensuring the in-transit and in-cloud security of global email.

Richard Wang

October 30, 2024
In Shenzhen, China

2024.10.30
16:23:46
+08'00'

Follow ZT Browser at X (Twitter) for more info.
The author has published 76 articles in English (more than 96K words) and 187 articles in Chinese (more than 535K characters in total).