HTTPS Encryption Automation and Email Encryption Automation

ZoTrus Technology has completed the research and development of all products related to HTTPS encryption automation and has started small-scale production and deployment of applications. This article will tell readers about the next upcoming hot solution - email encryption automation and talk about the relationship between these two automations.

1. What is HTTPS encryption automation? What has ZoTrus done?

HTTPS encryption automation is derived from the RFC standard ACME (Automatic Certificate Management Environment), which realizes the automation of applying for and deploying SSL certificates for website domain names, completely freeing website administrators from manually applying for and deploying SSL certificates, greatly accelerating the popularization and application of HTTPS encryption.

However, the purpose of automatic certificate management is to automate HTTPS encryption. Since the HTTPS encryption solution based on the RSA cryptographic system has been very mature after more than 30 years of rapid development, the only thing that has not been realized at that time is the automatic application and deployment of SSL certificates. Therefore, ACME came out. However, for some older systems, it is impossible to install ACME client software. Some systems are too important, and the administrators are unwilling to change these servers to install ACME client software. Perhaps there is also a consideration of not trusting this third-party software.

Although cloud service providers such as Cloudflare and Amazon have extended automatic certificate management to the cloud services based on this standard, they still rely on the very mature RSA cryptographic application system - they only need to apply for and deploy SSL certificates. This solution cannot be used in the immature SM2 cryptographic application system because the goal of users is to automate HTTPS encryption, and HTTPS encryption is not just an SSL certificate product, but an ecological application.

ZoTrus Technology has also realized the limitations of international standards and the ultimate need of users to realize HTTPS encryption automation. Therefore, after developing the SM2 ACME client software with reference to the international standard, it decided to abandon this solution, because many Web server software in China are not Nginx, and the ACME client software cannot be installed, and even third-party client software cannot be installed. This is why ZoTrus produce the HTTPS Automation Gateway and Cloud Service that you see now. This is a solution with zero reconstruction of the original Web server, a solution where users do not need to care about what SSL certificates are, because SSL certificates are the intermediate products for the ultimate realization of HTTPS encryption. What users need is to realize HTTPS encryption automation, including the SM2 HTTPS encryption automation.

To realize HTTPS encryption automation, a Gateway alone is not enough. A PKI/CA cloud service is also needed - ZoTrus Cloud SSL Service System, which provides SSL certificate automation service for the Gateway to apply and deploy dual-algorithm SSL certificates. And ZoTrus provide SM2 certificate transparency log service for issuing SM2 SSL certificates, this is also the service currently provided exclusively by ZoTrus. And a browser that supports the SM2 algorithm is also required to implement SM2 HTTPS encryption, this is the ZT Browser, a completely free, clean, ad-free browser that supports SM2 algorithms, supports SM2 certificate transparency, strictly verifies the validity of SM2 SSL certificates.

These are two SM2 algorithm cryptographic application ecosystems that ZoTrus Technology has created to achieve HTTPS encryption automation - the SM2 Certificate Transparency Ecosystem and the SM2 Automatic Certificate Management Ecosystem. The two ecological products ensure that they can reliably provide HTTPS encryption automation services with RSA/ECC/SM2 algorithm support, meet users' globally trusted and cryptography compliance website security application needs, and provide one-stop HTTPS encryption automation and WAF protection automation services.

2. What is email encryption automation and why is it important?

HTTPS encryption automation has reached its peak application, more than 90% websites achieved HTTPS encryption automation. The next hot spot for certificate automation is email encryption

automation. Because email is the first and earliest Internet application, many years earlier than HTTP application, and this oldest Internet application with a history of more than 50 years still works in plain text, which is indeed an unacceptable fact. The author believes that this situation will be rewritten! ZoTrus Technology decided to do this big thing that changes the world!

The email encryption protocol S/MIME is only two years later than the HTTP encryption protocol HTTPS, but the fundamental reason why HTTPS encryption has been widely used is automation, which points the right way for email encryption. Only by automating email encryption can email encryption be widely used. However, this automation cannot be certificate automation only like HTTPS encryption automation, it also requires support from email clients.

Just as the promoters of HTTPS encryption automation are browsers – SSL certificate clients, the promoters of email encryption automation can only be the email clients, because CA can only issue email certificate and have no ability or no idea to develop email client to achieve email certificate automation management. As early as 2017, the author decided to do this email encryption automation and decided to develop an email client to achieve email certificate automation and email encryption automation, but unfortunately it was impossible to continue, and the project was stopped.

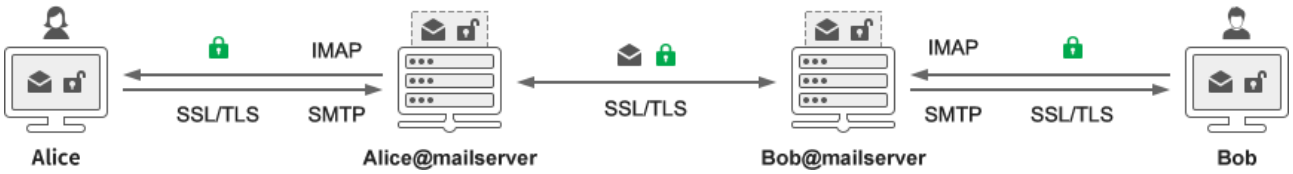
In June 2021, the author re-started his business and determined to continue to develop email encryption automation solution, and in the past three years, the construction of cloud cryptography infrastructure has been completed, and the research and development and production of HTTPS encryption automation related products have been completed. The research and development of email encryption automation solution is also nearing completion, an innovative solution to the century problem of email encryption is about to come out.

Email encryption automation is not just the email certificate automation, but also an ecological application system. It must not only be able to issue email certificates, but also require email clients to support automatic application and use of email certificates to implement email encryption and digital signatures. ZoTrus Technology has already completed cloud cryptographic infrastructure that can automatically issue email certificates. It only needs an email client to automatically connect to the cloud email certificate automatic issuance system, automatically configure email certificates for each

mailbox, and automatically implement email encryption and decryption and digital signatures. It is also planned to automatically configure timestamp signing certificates for each user and automatically stamp each outgoing email with an electronic postmark to ensure that the sending time of each email is trusted, filling the gap in international standards in this area.

3. What is the relationship between HTTPS encryption automation and email encryption automation?

The realization of HTTPS encryption automation can be used to realize the automation of email transmission channel encryption, because the email sending protocol SMTP and the email receiving protocol IMAP already support SSL/TLS certificates to realize TLS SMTP encrypted email sending channel and TLS IMAP encrypted receiving channel. The encryption of these two channels also requires SSL certificates, that is, the automation of SSL certificate management is also required. In other words, the automation of SSL certificate management used to realize HTTPS encryption automation can also be used in email encryption automation of email transmission encryption automation.



This is the TLS transmission encryption solution commonly used in the global email security market now. It can solve the problem of channel encryption of emails from the sender to the receiver. However, this depends on the email servers of both the sender and the receiver supporting TLS transmission encryption. If one party does not support it, the encryption transmission channel cannot be achieved. Fortunately, more than 90% of email services have been migrated to the cloud, and the email services provided by these cloud service providers all support TLS transmission encryption. The SSL certificate used for TLS transmission encryption can use the current ACME technology to realize the automatic application and deployment of SSL certificates.

However, the drawback of this solution is that emails are sent in plain text from the time they are sent to the recipient, and it are also stored in plain text in the cloud mail server. This only implements end-

to-end email transmission encryption, which can effectively prevent email content from being illegally tampered with and stolen in the transmission, but it cannot prevent the security of email content stored on the mail server because it is stored in plain text. Currently, many email service providers, especially free service providers, may not be able to find a profit model and can only make profits by reading user email content and pushing related advertisements to users. This may be one of the main reasons why industry giants have no motivation to promote encrypted email.

To ensure the security of emails, the ultimate solution must be an end-to-end encryption solution, that is, the email itself is encrypted before being sent. This not only ensures the security of emails during transmission, but also ensures the security of emails in the cloud, because the ciphertext is stored in the mail server. This end-to-end email encryption solution must use email certificates to implement encryption and digital signatures, and combined with TLS transmission encryption, it can truly ensure the security of the entire life cycle of emails. Only encrypted emails cannot protect the email content from being illegally tampered with during transmission and cause encryption failure, resulting in the recipient being unable to receive the encrypted email normally, and even if they can receive it, they cannot decrypt it normally. This is the close relationship between HTTPS encryption automation and email encryption automation. With the help of SSL certificate automation to ensure the encryption security of email transmission, coupled with email end-to-end encryption and decryption automation, the great mission of email encryption automation can be perfectly accomplished.

4. Email encryption automation is the next hot spot, and the global Internet will usher in the second peak of cryptographic application

Email is the first Internet application, the second largest Internet traffic, although there are many waste traffic caused by SPAM, but if the problem of email encryption automation is solved, that is, it automatically solves the problem of SPAM and malicious attack email flooding, because email encryption automation will realize that each email has a trusted identity of digital signature and encryption, as long as the mail server refuses to receive email without digital signature and encryption, it will also eliminate SPAM. And if the commercial model of WeChat official account article publishing is applied to mature mailing list subscription, then there is a feasible email marketing solution, which is a new undisturbed encrypted way of publishing and obtaining information that has the potential to

subvert the current WeChat solution.

Email encryption automation must be the next cryptography application hotspot, and it will also be very popular with global users, because email is not only a communication tool, but also a notification tool for all Internet services, and a centralized storage place for all Internet data in personal life and work. Even today, with the increasing popularity of social media, Internet users around the world have not only not reduced their use of email, but it has become more and more frequent in the use of email, and its information storage and aggregation functions have become more and more important.

However, Internet users deeply feel that plaintext email is seriously insufficient to protect personal privacy and business confidential information, and the industry has been exploring various email encryption solutions. The only right direction is automation, which uses email certificates to encrypt emails and ensure the security of the entire email lifecycle. ZoTrus Technology will come up with different innovative solutions to provide global users with different email encryption automation services, so stay tuned.

Richard Wang

September 29, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.