Only by Automating End-to-End Encryption Can Truly ensure Email Security

There are many vendors in the global market that claim to provide end-to-end encryption for email security. The various claims make it difficult for end users to choose a truly effective end-to-end encryption solution. This article will explain what true end-to-end encryption is. What kind of end-to-end encryption should end users choose to truly protect the security of their confidential email information.

1. What is end-to-end encryption? Why does email need it?

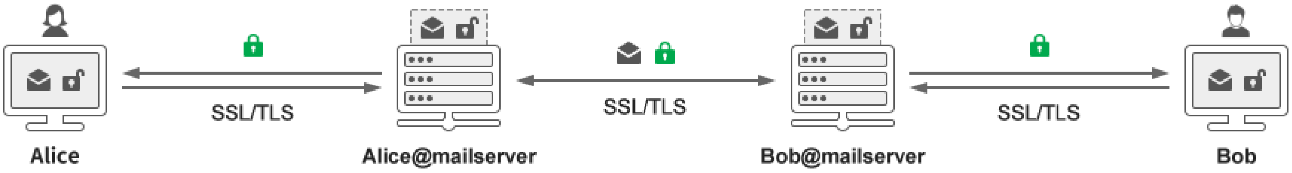
End-to-End Encryption (E2EE) means that information is encrypted from the sender to the receiver. For example, the commonly used website HTTPS transmission encryption, the information sent from the user's browser to the server is transmitted through the TLS encryption channel, which is end-to-end encryption. Only by implementing end-to-end encryption can we ensure that confidential data will not be illegally stolen or tampered with during transmission, and can we ensure that confidential information remains encrypted during transmission and ensure the security of confidential information transmission.

Email communication is a transmission process from the sender's computer to the recipient's computer. Unlike the HTTP protocol, emails are not sent directly from the sender to the recipient, but it is transferred through the mail servers of both parties. This feature means that end-to-end encryption cannot be achieved using the same technical solution as HTTPS encryption. It is precisely because emails are first saved and then forwarded by the mail server that emails need the end-to-end encryption, because a third party (mail server) takes over the transmission process, and emails will be stored in the mail server for a long time unless the user completely deletes them.

End-to-end encryption of email means that the email is encrypted before it is sent to the recipient in ciphertext. In this way, the mail server responsible for transit can only forward it in ciphertext and can only save it in ciphertext. Only in this way can it be guaranteed that the email is truly end-to-end encrypted throughout the entire process.

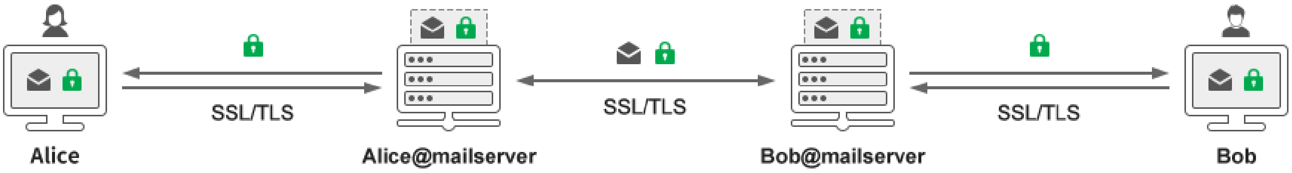
2. What are the technical solutions for implementing end-to-end encryption of emails? What technical solution is true end-to-end encryption of emails?

Let's first look at the popular TLS email encryption solution on the market. This technology is of course borrowed from HTTPS encryption, but as mentioned in the previous section, the email transmission process is different from the HTTP transmission process. As shown in the figure below, TLS email encryption technology is to deploy SSL certificates on the mail server to implement TLS IMAP and TLS SMTP encrypted transmission. The email is sent from Alice's mail client to Alice's mail server through the TLS encrypted channel, which can ensure transmission security. Alice's mail server saves this email in Alice's mailbox and then forwards this email to the recipient Bob's mail server. Whether this transmission process can achieve TLS transmission encryption depends on whether Bob's mail server supports the TLS SMTP protocol. If it does, TLS transmission encryption can be achieved. If it does not, it can only be transmitted in plain text, which is not end-to-end encryption. Fortunately, most email providers currently support the TLS SMTP protocol, so emails can still reach Bob's mail server in an encrypted manner, and Bob continues to use TLS transmission encryption to obtain the emails sent to him by Alice from the mail server.



Please note that the email content in the above solution is unencrypted plain text on the user side and the email server side. The email content is stored in plain text on the email server. The TLS email encryption technology solution only solves the encryption of the email transmission process, but it does not solve the problem of email content encryption.

Please see the figure below. The email was encrypted before it was sent from Alice's computer. Regardless of whether the mail server supports the TLS STMP protocol, it can ensure that the email is transmitted in ciphertext and stored in the mail server in ciphertext. This is end-to-end encryption. The mail server responsible for forwarding and storage in the middle cannot see the encrypted email content. The mail service provider cannot push content-related advertisements through machine-readable email content, which protects the security of confidential email information.



As for how to encrypt emails before sending, there are various technical solutions on the market, including converting email content into PDF files and adding a password, converting email content into so-called encrypted envelopes and saving them in cloud servers, and recipients will receive an online decryption link that must be connected to the cloud server to view, etc. These all use private protocols to achieve encryption and decryption, which are not feasible solutions and are only applicable to a closed system. They are not applicable to the basic requirements of email, an open system that reaches the world.

At present, the mature technical solution on the market is to use cryptographic technology to achieve email encryption, mainly including S/MIME encryption, PGP encryption and IBC encryption. The latter two encryption methods only focus on encryption with digital certificate, and use self-signed certificates without trusted identity information, without focusing on the sender's trusted identity validation. Emails are not face-to-face communications, which not only need to be encrypted, but also need to prove the sender's trusted identity. Only a trusted identity validated by a trusted third-party CA can prevent email identity fraud. Both identity trust and encryption are very important, and only S/MIME technology can do this. S/MIME is not only what the author love, but also the technical route adopted by most email encryption solutions in the industry, and it is also the solution adopted by commonly used email clients. The International Standards Organization - CA/Browser Forum has established an S/MIME Certificate Working Group and formulated the S/MIME Certificate Baseline Requirement, requiring global trusted CAs to follow this international standard from September 1, 2023. This is the greatest recognition of S/MIME technology in the global industry, making it the first time that CAs issue S/MIME certificates in a regulated manner.

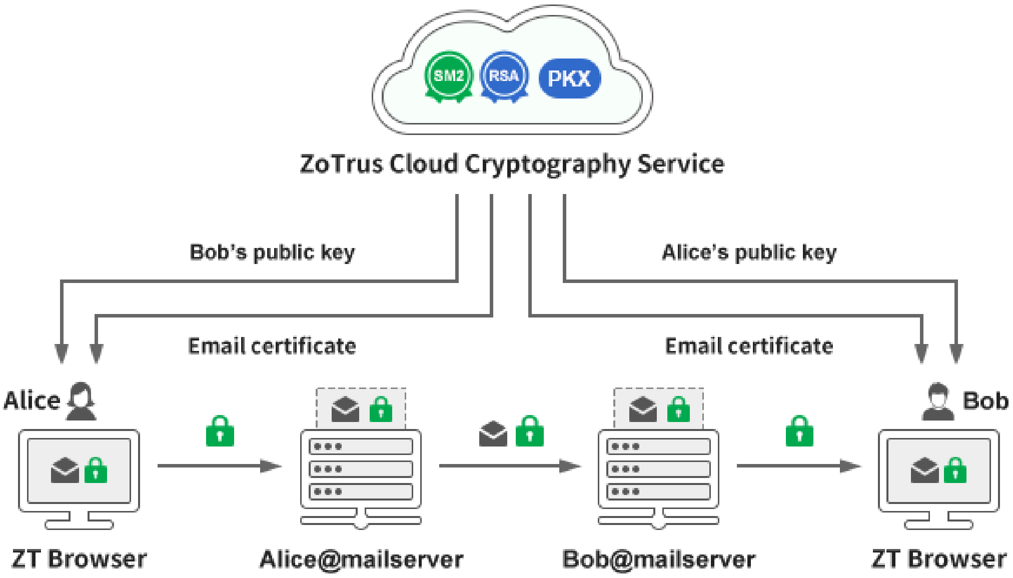
The core of S/MIME technology is that a third-party CA issues an email certificate after verifying the user's identity in strict accordance with international standards. End users need to configure the email certificate in the email client to use it to achieve email encryption and digital signature, so that the email is encrypted with the certificate before it is sent. This is truly reliable end-to-end encryption. Common email clients such as Microsoft Outlook, Mozilla Thunderbird, Apple Mail, Huawei Mail, etc. all support S/MIME technology to achieve end-to-end encryption of emails.

3. ZoTrus Technology automates end-to-end encryption of emails, effectively protecting the security of the entire email life cycle.

Although everyone agrees that using S/MIME technology to achieve end-to-end encryption is the only reliable technology to protect email security, there are still very few Internet users who actually use S/MIME technology to encrypt daily email communications, because the threshold for using this technology is too high. Not only do users need to apply for email certificates from CA, but they also need to manually configure certificates to be used in common email clients. The recipient also needs to have an email certificate, and both parties must exchange public key certificates in advance. And they also need to manage encryption keys themselves (never to lose them) and update email certificates regularly. These are all technical obstacles to the popularization of S/MIME technology to achieve email encryption. Without solving these usability issues, it is impossible to popularize this technology to popularize email encryption.

The reason why HTTPS encryption has been widely used around the world is that the secret lies in automation, which is to automatically apply and configure SSL certificates to achieve HTTPS encryption. Like the HTTPS encryption solution, ZoTrus email encryption solution also takes the automatic route, automating the application and configuration of email certificates for users, automating the exchange of public key, and automating the management of encryption keys. Only automation can achieve the grand goal of popularizing email encryption.

To achieve automation, of course, it must be a client-cloud integration solution. The client is ZT Browser, a high-performance browser based on the Google Chromium with a built-in email client. After the user logs into the mailbox using the ZT Browser, ZT Browser will automatically connect to the ZoTrus Cloud Cryptographic Service System to automatically complete the email certificate application, email control validation, email certificate issuance and configuration for the user. And when using ZT Browser to send encrypted emails, it will automatically connect to the Public Key Exchange (PKX) Service provided by ZoTrus Cloud Cryptography Service System, automatically obtain the recipient's public key certificate, and send encrypted emails without exchanging public keys with the recipient in advance. The client-cloud integration completely solves the various technical problems encountered in email encryption, allowing users to send encrypted emails as easily as sending plain text emails, achieving end-to-end email encryption. The email content is also stored in ciphertext on the mail server, perfectly realizing the security of the entire life cycle of emails.



ZoTrus Technology also uses S/MIME technology to achieve email encryption and realizes the compatibility and interoperability of email encryption between ZT Browser and all other email clients around the world that support S/MIME standards. The difference is that ZoTrus solution is automatic, which perfectly solves the various inconveniences and high barriers to use of S/MIME technology, so that end users can enjoy the email security brought by advanced S/MIME technology to users without feeling, and only by realizing email encryption automatically can email encryption be popularized, and truly ensure the in-transit security and cloud security of emails, that is, to ensure the security of the entire life cycle.

Richard Wang

October 11, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 71 articles in English (more than 88K words)
and 182 articles in Chinese (more than 521K characters in total).