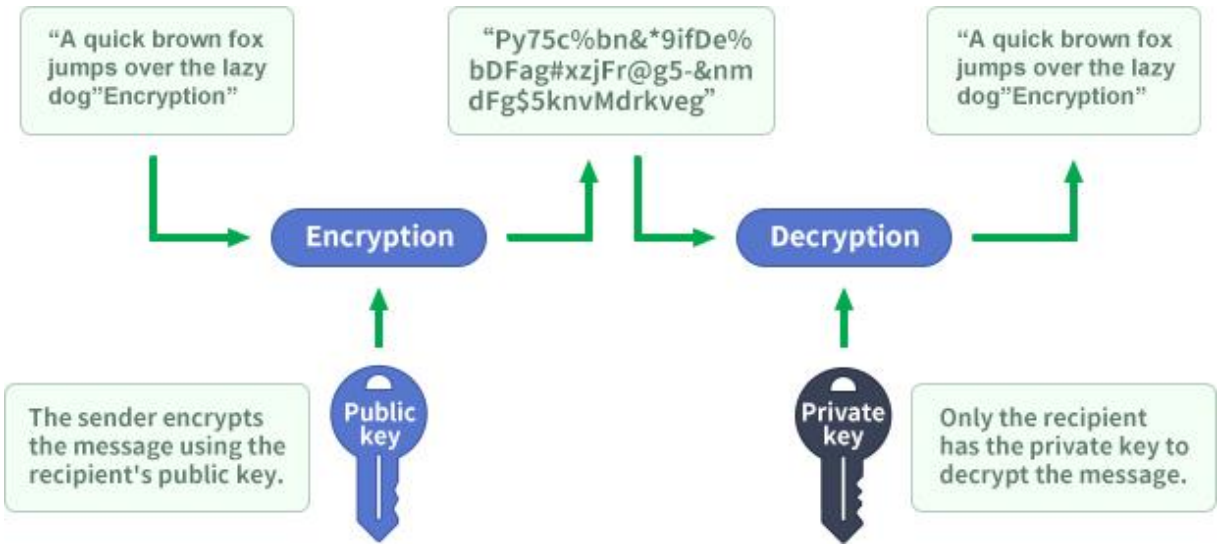
How does ZT Browser automate public key exchange?

There are three major challenges in email encryption: certificate application, public key exchange and key management. This article explains how ZT Browser solves the problem of public key exchange and how to automate public key exchange.

1. What is public key exchange? Why is it a problem?

The magic of PKI technology is the design of public key and private key, which is commonly known as "two keys to open one lock", because "one key to open one lock" cannot solve the problem of how to give the key to the other party. This clever design of the two keys is that the public key can be obtained publicly through various channels, and the private key is only owned by oneself. The combination of public and private key can achieve encryption and decryption, without having to give the entire key to the other party like a door key. As shown in the figure below, let's first talk about the technical principle of email encryption. The sender uses the recipient's public key to encrypt the information, turning the plaintext information into ciphertext, and can then be safely sent to the recipient, regardless of whether the mail servers of both parties use TLS transmission encryption. After receiving the ciphertext, the recipient can use his own private key to decrypt the encrypted message. This is asymmetric encryption, unlike symmetric encryption where both parties share a key.



The question is, how should the sender get the recipient's public key? This requires both parties to exchange public keys. Only after exchanging public keys can both parties achieve mutual email encryption. The traditional exchange of public keys is achieved by sending a digitally signed email to the recipient, and the other party also replies with a digitally signed email to complete the public key exchange. This process looks very scientific and simply. In fact, it is not easy to implement. Imagine that you have 100 contacts, and you have to exchange public keys with these 100 contacts, provided that these 100 people also have email certificates. If the recipient does not have an email certificate, public keys cannot be exchanged, and email encryption cannot be achieved.

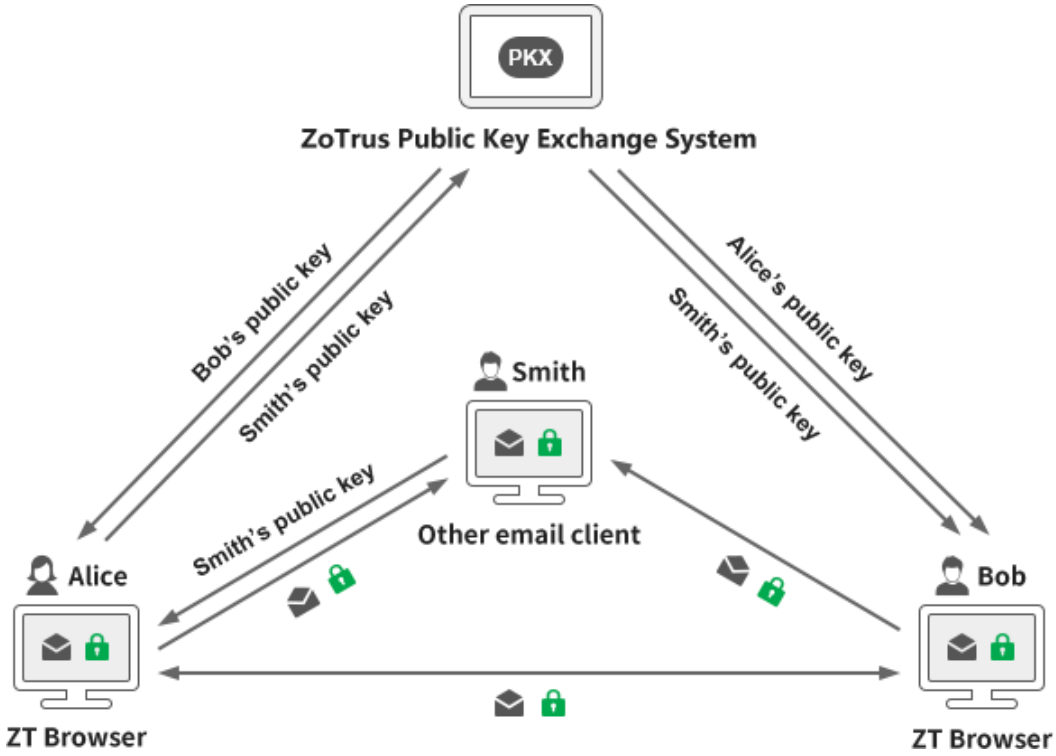
Even if the two parties have exchanged public keys, for private key security, the email certificate can only be valid for two years at most, which means that the public keys need to be exchanged with these 100 contacts every two years. After the public keys are exchanged, they need to be configured in the recipient's address book according to the requirements of the email client so that the email client can retrieve the public key to send encrypted emails.

2. Only by automating the exchange of public keys can we achieve widespread email encryption

The above manual exchange of public keys is the least efficient way to exchange public keys. If Alice has 100 contacts and needs to exchange 100 times, 100 million email users will have to exchange 10 billion times. However, if there is a third-party public key database that provides public key management services, everyone only needs to submit their public key to the public key database once, and when someone's public key is needed, the email client can directly obtain it from the public key database, which saves the operation of exchanging public keys in advance. This is the solution to improve the efficiency of public key exchange. ZoTrus Technology has built a public key exchange system to provide free public key exchange automation services to all ZT Browser users.

In the blog post " How does ZT Browser realize the automatic email certificate management? ", the author explained how ZT Browser automatically configures email certificates for users. All email certificate public keys issued for users are automatically written into the public key exchange database, so ZT Browser users do not need to exchange public keys in advance to send encrypted emails. As shown in the figure below, Alice can directly obtain Bob's public key from the public key exchange

system and send encrypted emails to Bob directly without exchanging the public key with Bob in advance. Boo obtained Alice's public key from the public key exchange system and sent encrypted emails directly to Alice.



But this is not enough. What if Alice, a user of ZT Browser, needs to send an encrypted email to Smith, a user of another email client that supports S/MIME? Of course, Alice and Smith need to exchange public keys by sending a digitally signed email manually in the traditional way. In this way, Alice can send encrypted emails to Smith. At the same time, ZT Browser will automatically submit Smith's public key to ZoTrus Public Key Exchange Database. In this way, all ZT Browser users, such as Bob, no longer need to exchange public keys with Smith. Bob can automatically obtain Smith's public key from the Public Key Exchange System and automatically send encrypted emails to Smith without exchanging public keys with Smith in advance. This greatly improves the exchange efficiency of the traditional manual exchange of public keys.

As the number of ZT Browser users continues to increase, the probability that users need to manually exchange public keys with other non-ZT Browser users is getting smaller and smaller. However, given that there are still only a few users with email certificates, what if a ZT Browser user needs to send an encrypted email to a user who does not have an email certificate? In other words, what if a ZT Browser user does not know whether the recipient has an email certificate and does not want to manually send

a digitally signed email to the recipient to exchange public keys? ZT Browser has a default mechanism that does not require manual exchange of public keys. Users do not need to care whether the recipient has an email certificate, nor do they need to ask the recipient whether the recipient has an email certificate, nor do they need to manually exchange public keys. They can directly send encrypted emails to anyone. Once ZT Browser cannot obtain the recipient's public key from the Public Key Exchange System, it will automatically generate a key pair (private key and public key) for the recipient temporarily, encrypt the email with this temporary public key, and let the user send the encrypted email to the recipient automatically. At the same time, ZT Browser automatically sends a plaintext email to the recipient in the name of the sender, telling the recipient how to decrypt the encrypted email sent to him/her by the sender. The recipient only needs to download and install ZT Browser, enable the email encryption automation service, and then use ZT Browser to log into his or her mailbox to view the encrypted emails that have been automatically decrypted.

This is the public key exchange automation service provided by ZT Browser. Users do not need to worry about whether the recipient has an email certificate, nor do they need to exchange public keys with the recipient in advance. They can directly use ZT Browser to send encrypted emails to all email users. The recipient will be able to decrypt and read the encrypted emails, and the recipient will use the email certificate that ZT Browser automatically configures for free to decrypt the emails locally, rather than decrypting and reading them using the cloud service.

With the support of ZoTrus Public Key Exchange System, ZT Browser can add all the recipient's public keys to the recipient's key list when sending encrypted emails, including the email certificate automatically configured by the ZT Browser and email certificates issued by other CAs. This ensures that the recipient can decrypt the encrypted email using any email client on any device, achieving maximum compatibility support for encrypted emails.

3. The email certificate automation and public key exchange automation provided by ZT Browser remove technical barriers to popularizing email encryption

Users only need to download ZT Browser and use the free email encryption automation service provided by ZT Browser to automatically apply for and configure 4 email certificates and 2 email

timestamping certificates for free. These certificates can be used for email encryption services. In order to realize email encryption, you also need the recipient's public key. This is the second free automation service provided by ZT Browser - the Public Key Exchange Automation Service. With these two automation services, users can send encrypted emails to all email users just like sending the normal plain text emails. Users do not need to worry about how to apply for certificates from CA, nor do they need to worry about exchanging public keys with all recipients. They can send and receive encrypted emails without feeling. All emails are end-to-end encrypted and stored in the cloud email server in ciphertext, effectively ensuring the security of emails in transit and in the cloud.

The email certificate automation and public key certificate automation provided free of charge by ZoTrus Technology allow users around the world to send encrypted emails to any email user without any awareness and at zero cost, removing the technical barriers to the popularization of email encryption. The remaining work is for everyone to use it to effectively protect the security of confidential information in personal emails and the security of commercial secrets in corporate emails.

Richard Wang

November 4, 2024
In Shenzhen, China

2024.11.04
15:57:54
+08'00'

Follow ZT Browser at X (Twitter) for more info.
The author has published 77 articles in English (more than 98K words) and 188 articles in Chinese (more than 537K characters in total).