How does ZT Browser automate key management?

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

1. What is Key Management? What needs to be managed? Why is this a problem?

Key management refers to the management of the private key used for email encryption, and the public key has been managed by ZoTrus Public Key Exchange System. So, how should the private key, the core of email encryption, be managed? Key management includes the generation, use, storage, and updating of keys, and as long as the encrypted email has the value of retention, the private key must be kept at all times so that it can be used to decrypt the encrypted email. Therefore, ensuring key security is one of the core tasks of email encryption, and it is also the most important work in email encryption.

When the user applies for an email certificate from the CA, the local computer generates the private key and CSR, submits the CSR to the CA to apply for the email certificate, and after obtaining the public key certificate issued by the CA, it is manually or automatically synthesized into a certificate file (.pfx/.p12) containing the private key and the public key, and a protection password must be set for the certificate PFX file. The user needs to keep the certificate file and the certificate protection password and must enter the protection password every time the certificate is imported and used in various email clients, if user forget the protection password, it is equivalent to the email certificate is invalid, and all emails encrypted with this certificate can no longer be decrypted. This is the importance of key management, because the content of some emails is very important, but you can't decrypt it when you need it, and you will regret encrypting it in the first place.

In other words, traditional email encryption requires users to keep the certificate private key and protection password by themselves, and they need to back up the certificate on multiple devices at the same time, because if a computer system is broken, the key will be completely gone. Encrypted emails can no longer be decrypted. This is the difficulty and pain point of key management, and it must be solved to let users use email encryption services with confidence.

2. Email encryption popularity can only be achieved by automating key management

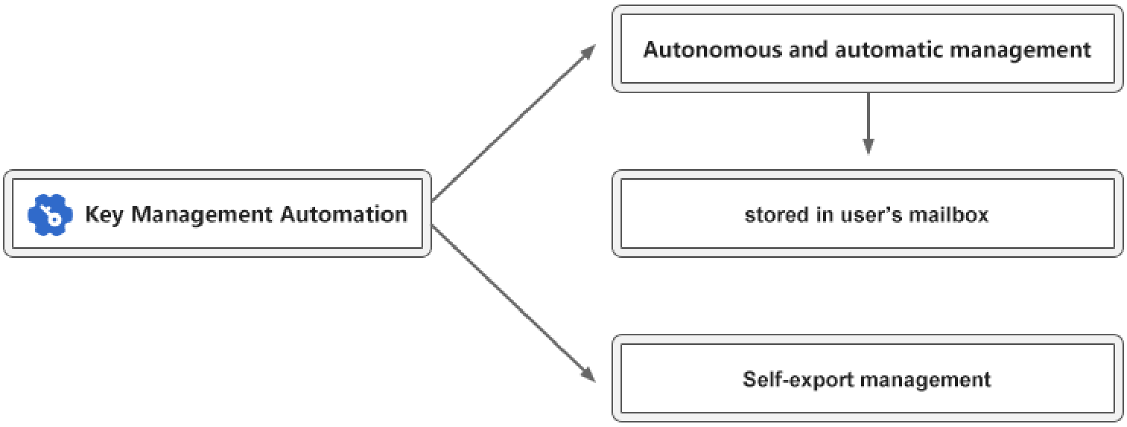
How to solve the key management problem? Users keep the key on their own computer, which is not only difficult to manage, but also in case the computer breaks, the key is gone. The only way out is to use cloud services, because we can assume that cloud services are always available. So, it is a good idea to keep keys in the cloud, and all well-known cloud service providers offer key management services for a fee.

However, ZT Browser does not intend to provide cloud key management service, because the product concept advocated by ZoTrus Technology is the concept of zero trust, and the custody of users' keys is not only a great responsibility, but also may encounter a trust crisis of users, and users may not trust our key management services and abandon our services, which is a thankless solution. However, what if you don't want to manage your keys by yourself and need a key management solution to solve the key management challenges?

ZT Browser has innovatively given a solution - the user's certificate file (.pfx) containing the private key and public key certificate will be automatically sent as an email attachment to the user's own mailbox for safekeeping, that is, the user can keep his own key, and it will be kept in the cloud and will not be lost, unless the email service provider goes bankrupt and goes out of business, which is a high probability of impossibility. The reason why it is plaintext email is, of course, that when the user reinstalls ZT Browser or installs ZT Browser on a new device, it must be able to obtain the email in plaintext and automatically obtain the private key of the certificate, and reinstall the certificate for decrypting encrypted emails and sending encrypted emails.

Of course, in order to protect the security of the key, the key file saved in this plaintext email must have encryption measures, which is an encryption implemented by a private algorithm, this certificate backup email is only used for ZT Browser, ZT Browser will automatically create a folder named

ZTBrowserOnly when backing up the PFX format certificate file to the user's mailbox, and save the key backup email in this folder, so that ZT Browser can quickly and automatically obtain the user key for use on the new device. If ZT Browser can't find this folder or can't find the key file email, it will think that the user does not have an email certificate, and it will automatically issue a new email certificate and back it up to this folder. If user previously had a email certificate and had encrypted messages, it will not be able to automatically be decrypt unless user have backed up the certificate file yourself and can import it manually. If the import is successful, ZT Browser will still automatically back up the key to the user's mailbox.


Key Management Automation
Autonomous and automatic management
stored in user's mailbox
Self-export management

In line with the concept of zero trust security, if users do not want to continue to use the email encryption automation service provided by ZT Browser, they can use the function of exporting all certificates (including private keys) with one click provided by ZT Browser at any time, and after exporting the certificate, they can manually import the email certificate to other email clients that support S/MIME standard, and then decrypt all emails encrypted by ZT Browser before, completely relieving the user's worry of being tied to ZT Browser. This is also an advantage that other closed-private protocols for email encryption cannot match.

ZT Browser's innovative key management solution not only realizes the automation of key management, but also solves the security concerns of the key managed by a third party, and it solves the problem that the key may be lost by the user's own management. Only by automating key management can we truly automate email encryption and popularize email encryption applications.

3. Email certificate automation, public key exchange automation, and key management automation are all indispensable.

The reason why S/MIME email encryption technology cannot be popularized is because this technology is difficult to apply, mainly in three aspects: certificate application, public key exchange and key management, and the only way to solve these three problems is automation. ZT Browser's email certificate automation, public key exchange automation and key management automation completely solve these three problems, this is an innovative solution of client-cloud integration, the three are indispensable, and it is natural together, which is the great contribution made by ZoTrus Technology in email security for global email security, and will definitely be welcomed by global email users, and we will work together to create a secure email world with zero fraud, so that the ancient decentralized email service will continue to better benefit mankind more.

Richard Wang

November 7, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 78 articles in English (more than 99K words)
and 189 articles in Chinese (more than 539K characters in total).