

## Webmail vs Email client

There are many articles on this topic online, and everyone agrees that each has its own advantages and is used in different email application scenarios. Both are indispensable, and both webmail and email client need to be used. In this article, the author discusses this issue from another perspective, because this issue is also the technical direction that needs to be determined when ZoTrus Technology sets up the project to develop email encryption automation service. Since ZoTrus Technology already has a browser - ZT Browser, should it provide email encryption automation services based on ZT Browser or develop an independent ZoTrus Email Client? Is there a perfect solution that has both the advantages of webmail and email client and overcoming their respective shortcomings?

### 1. What is an Email client? What is Webmail? What are the pros and cons of each?

Why do we talk about email clients first? Because email clients came first in the history of email. When email was first invented, email clients were used to send and receive emails. Because email is a special protocol, special software is needed to manage email sending and receiving. Email was the first application of the Internet, and there was no Web service at that time.

Email clients use the POP3/IMAP protocol to receive emails from the email server and the SMTP protocol to send emails. They also provide services such as email management and address book management, allowing users to view and write emails offline and save emails on their local computers. The first email client software was written by Larry Roberts in 1972, this software had the functions of displaying emails in a list, selecting, forwarding, and replying to emails. The first email client software to provide a graphical user interface was Eudora, written by Steve Dorner in 1988. Commonly used email clients now are Microsoft Outlook, Apple Mail, Mozilla Thunderbird, Tencent Foxmail, etc.

Email client software is a must-have for sending and receiving emails before Hotmail appeared in 1996, the world's first Web mail service. Users can send and receive emails directly using the browser used

for Internet access without using email client software, and each registered user is given a @hotmail.com email address for free. Hotmail not only allows users to have an email address for free, but also allows users to send and receive emails using a browser if they can access the Internet. It quickly became popular around the world, with 10 million users in just one year. In 1998, it was acquired by Microsoft for \$400 million and later renamed to Outlook.com. The climax of Webmail was Google's launch of Gmail on April 1, 2004, the world's first free web mail service with up to 1GB of free storage space. Gmail is still the world's number one free web mail service now.

Webmail is easy to use, because any computer or mobile phone has a browser, people can log into the web mailbox to send and receive emails. However, there are still many inconveniences, such as the inability to view and send emails offline and the need to login every time. Therefore, all Webmail service providers provide users with email client software. According to the latest third-party statistics, the world's top four email clients are Apple Mail, Google Gmail, Microsoft Outlook, and Yahoo Mail, with market shares of 53.67%, 30.70%, 4.38%, and 2.64%, respectively, totaling 91.39%, and the total of all other email client software market share is 8.61%. The ranking of global Webmail service providers is Google Gmail, Microsoft Outlook, Yahoo Mail, and Apple iCloud Mail, with market shares of 43%, 19%, 10%, and 8%, respectively, totaling 80%, and the total of all other Webmail service providers market share is 20%.

Whether it is email client or Webmail service, the top four companies are both email client developers and Webmail service providers, but the ranking is slightly different. Google Gmail has the second largest email client market share due to its first-place free Webmail service. This also fully demonstrates that Webmail and email client are constantly merging and complementing each other, but the mainstream still uses email clients. Apple Mail ranks first among email client software, which has a lot to do with the popularity of mobile Internet, because users using mobile phones to send and receive emails has become the first rigid demand, which has turned Webmail from being very popular to being just a supplementary means when email clients cannot be used.

## **2. What is the core security of email? Are there any unsolved issues?**

Although Webmail and Email client seem to be two different ways of using email, Webmail also uses

a client software - the browser to process email. The difference lies in: (1) whether to use a general client or a dedicated client; (2) whether to process emails in the cloud or on the user's end. Therefore, users may ask: Which is more secure, Webmail or Email client? This is not a good question. Email security has nothing to do with the type of email client used.

The core security of email is how to ensure the security of email content during transmission and storage in cloud mail servers, which is referred to as email in-transit security and in-cloud security. The email in-transit security has implemented TLS encryption transmission, which can effectively ensure the security of email transmission regardless of whether users use Webmail and email client to send and receive emails. If an email service does not support TLS encryption transmission (TLS IMAP and TLS SMTP), it is an unqualified email service and users should not choose such email services, whether free or paid.

How to ensure the email in-cloud security is a problem that has not been solved in the world at present, or it is a problem that everyone repeats. All email service providers may say that they have taken many technical measures to ensure the security of emails in the cloud. The in-cloud security here refers to whether the emails are stored in the mail server as encrypted emails. Only in this way can the email in-cloud security be truly guaranteed. Other claims to ensure the security of emails in the mail server are just verbal promises. If it's plaintext email, no measure can guarantee the email in-cloud security.

Although there are many email encryption solutions on the market, and commonly used email clients already support S/MIME email encryption, but they are difficult to use and cannot be widely used. As a result, current emails are stored in plain text in cloud email servers, so that all Webmail service providers can rely on machine-readable email content and display related advertisements as a profit model, a bunch of annoying ads appear when viewing emails on the Webmail, this is also one of the reasons why many users are reluctant to use free Webmail services.

The email security issue that needs to be addressed is to popularize the end-to-end email encryption. Only by achieving end-to-end encryption can the email in-transit security and in-cloud security be truly guaranteed, and email fraud and BEC attacks can be effectively prevented. The reliable technology for achieving end-to-end encryption of emails is S/MIME technology. This technology, like HTTPS

technology, requires users to purchase and apply for email certificates from CAs, manually configure it in email clients that support S/MIME, and exchange public keys with recipients to achieve end-to-end email encryption. This solution is very cumbersome, time-consuming, labor-intensive, and costly, and cannot be widely used.

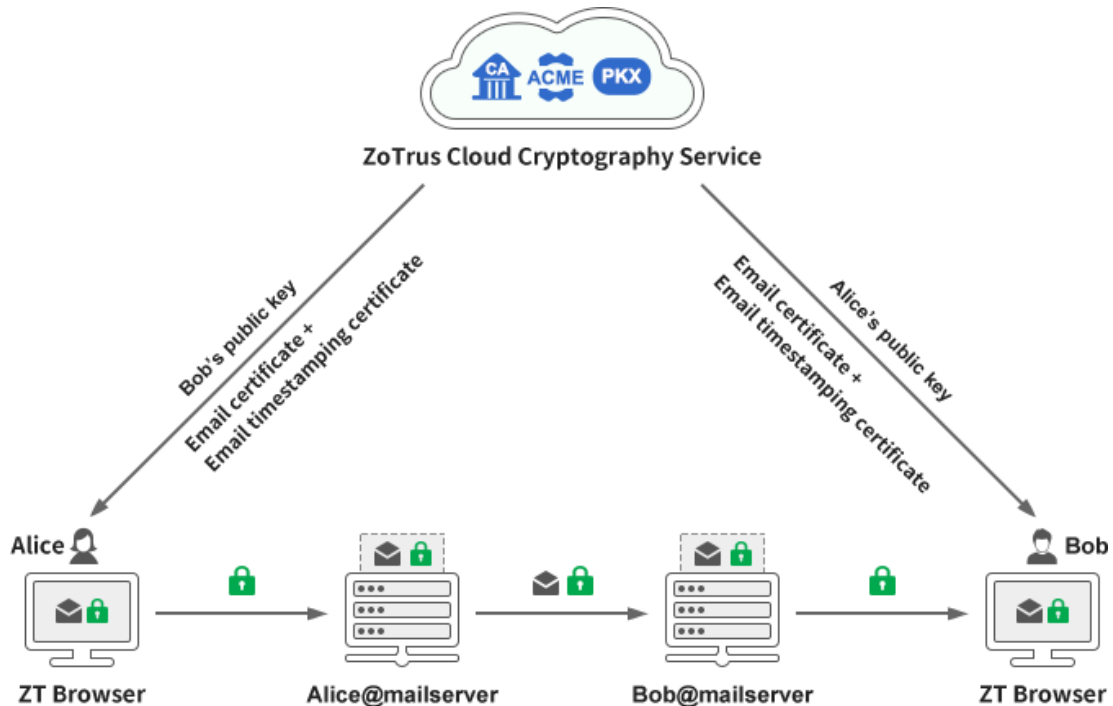
### **3. ZoTrus innovation solution - ZT Browser with email client, two-in-one.**

ZoTrus Technology planned to provide automatic email encryption services three years ago, which required first determining the technical solution. The original plan was to develop an email client software to automate the configuration of email certificates, automate public key exchange, and automate end-to-end email encryption. However, Webmail must be considered that users like to use Webmail. If users can automatically encrypt and send emails and decrypt encrypted emails after logging into the Webmail service using ZT Browser, would this be a very good solution?

It is very difficult to implement S/MIME email encryption in traditional Webmail, even though Microsoft has released an S/MIME email encryption plug-in, and there are many such browser plug-ins on the market. The main obstacle is that it cannot be automated, and it is still the traditional email client implements S/MIME encryption without any technical breakthroughs.

The innovative solution of ZoTrus Technology is to integrate the email client into ZT Browser. Users can continue to enjoy the convenience of Webmail and can also send encrypted emails as easily as sending plaintext emails, and they can decrypt and read the encrypted emails using browser. This is a client-cloud integration automatic email certificate management solution, which automates the application and configuration of S/MIME email certificates. This is also a client-cloud integration automatic public key exchange management solution, exchange of public keys automatically, to let users to directly send encrypted emails without having to exchange public keys with recipients in advance. This is also a client-cloud integration automatic private key management solution, which allows users to not worry about private key management, and automatically stores the private keys in user mailbox, rather than using a third-party cloud key management system, to ensure the security of user private keys. This is also client-cloud integration automatic email timestamping management solution, which allows every email sent by users to have a trusted sending time, rather than the

untrusted user computer time.



ZT Browser automatic email encryption service is a solution that uses S/MIME certificates to achieve end-to-end email encryption. ZT Browser can be used for both Webmail and email client, solving the problem that Webmail cannot send encrypted emails while having all the advantages of an email client. It is a perfect solution that combines the advantages of both client methods without their disadvantages. It uses automatic email certificate management to perfectly solve the problem of protecting the full life cycle security of email content that has not yet been solved by current email security solutions, and automatically ensures the in-transit and in-cloud security of emails.

It is worth mentioning that the innovative UI of ZT Browser email client, which inherits the UI characteristics of ZT Browser in terms of HTTPS encryption and document reader, adopts 5 different icons, respectively shows whether each email has been encrypted, what algorithm is used, whether there is a digital signature, whether there is a trusted email timestamping, whether there is a trusted identity and displays the sender's trusted identity information.






## Meeting arrangement



From: help@zotrus.com

To: help@cersign.com

Fri 2024/11/1 00:14

     [CN] Richard Wang <help@zotrus.com> ZoTrus Technology Limited

If it really needed to classify it, ZT Browser can be classified as an email client, an encrypted email client, an email client with integrated automatic email certificate management, it automatically implements email encryption, digital signature and timestamp, supports all email services provided by all email service providers, can be used for all email addresses that support IMAP and SMTP services, automatically configures dual-algorithm (RSA & SM2) S/MIME email certificates for free, and automatically implements end-to-end email encryption, making it easier to popularize email encryption and ensuring global email security. Welcome to the email encryption automation service provided by ZT Browser, completely free of charge.

*Richard Wang*

**December 23, 2024  
In Shenzhen, China**

---

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

The author has published 84 articles in English (more than 109K words) and 197 articles in Chinese (more than 565K characters in total).

