How does ZT Browser implement the trusted email timestamping service?

As we all know, ordinary post office letters have postmarks, although these letters are rare nowadays. A postmark is a stamp on the letter by the post office to prove that the letter was sent from this post office and when it was sent. This postmark is the authoritative proof of the time when the letter was sent.

For email, the email time displayed by the email client when you receive the email is the time when the email is sent from the sender's email client, this time is the sender's computer time, which is a time that can be modified at will, so it is not a trusted time, and it cannot accurately prove the real sending time of the email, which is a time for reference only.

The email encryption service provided by ZoTrus Technology innovatively refers to the technical solution that both code signing and document signing require the timestamp, to provide an email timestamping service for each email sent. This article will talk about how this innovative service is implemented. Users can be sure that this time is indeed a trusted time after understanding the implementation method. This completely free innovative service will likely bring about various Internet applications based on trusted email timestamp, because there are many application scenarios in real life that require time proof.

1. What is an email timestamp? Why do emails need a timestamping service?

An email timestamping service is a cryptography timestamp signature attached to an email digital signature; it is not the electronic form of a traditional postmark. In the PKI application system, code signing has a timestamp service to prove that the code signing time is within the validity period of the code signing certificate, this timestamping service ensures that the digital signature of the signed code is valid even if the code signing certificate has expired. Document signing also has a timestamping service to prove that the signing time of the document is trusted.

There is no timestamp standard for emails. In fact, the sending time of emails needs to be proved by timestamp like traditional mail with postmark. This is why email timestamping service is needed to prove that the sending time of emails is trusted, non-repudiation and tamper-proof. Email timestamping service is also a cryptographic timestamp signature service, which follow the RFC3161 standard to provide timestamping services for emails.
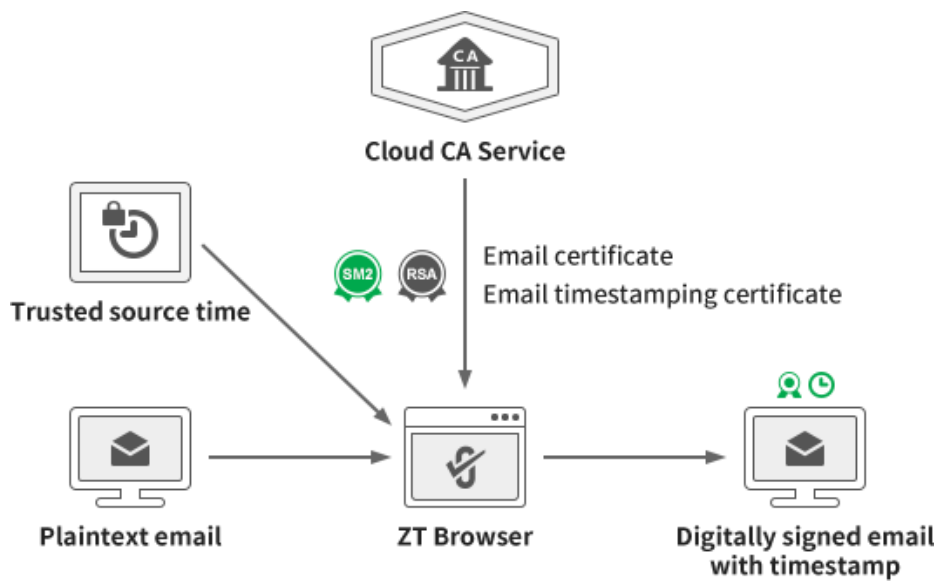
2. How does ZT Browser implement email timestamping service?

Traditional timestamping services are provided by CAs, which provide code signing timestamping service and document signing timestamping service for free to users of their code signing certificates and document signing certificates. If users need to use timestamping service for email digital signature, user can continue to use the timestamping service provided by CA by following the practice of code signing certificates, because the CA also issue email certificates. This is one of the options for implementing email timestamping service.

However, considering the huge volume of emails sent, according to statistics released by relevant websites, more than 360 billion emails are sent every day worldwide, 250 million emails per minute. With such a large volume of emails sent, no timestamping service provider can provide timestamp signature services for every email. What can we do? Traditional centralized timestamping services cannot meet the timestamp signature requirements of emails.

The innovative solution of ZoTrus Technology is that users use ZT Browser to provide email

timestamping service for each email they send, without relying on third-party timestamping service. When users enable ZoTrus email encryption automation service, ZT Browser will automatically apply for and configure email certificates and email timestamping certificates for users. Email certificates are used for digital signatures of emails, while email timestamping certificates are used to attach timestamp signatures after completing digital signatures of emails. The trusted time required for timestamp signatures comes from multiple trusted network time sources (NTP service), such as: the China Time Service Center, Microsoft Windows time server, and US NIST network time service.


All emails sent by ZT Browser is encrypted, digitally signed and timestamped. After implementing the digital signature of the email, ZT Browser will automatically call the built-in email timestamping service to attach the timestamp signature data to complete the digital signature and timestamp of the email. After receiving the digitally signed email sent by ZT Browser, ZT Browser will synchronously parse the timestamp signature data and complete the timestamp signature validation at the same time as the email digital signature validation.

After the verification is completed, the trusted email sending time will be displayed in the place where the email time is displayed, instead of the email sending time contained in the email header, and the timestamp icon 🕒 is added in the email encryption icon area near the digital signature icon to prove that the displayed email time is a trusted time, as shown in the following figure, the real time of email sending is 23:51.
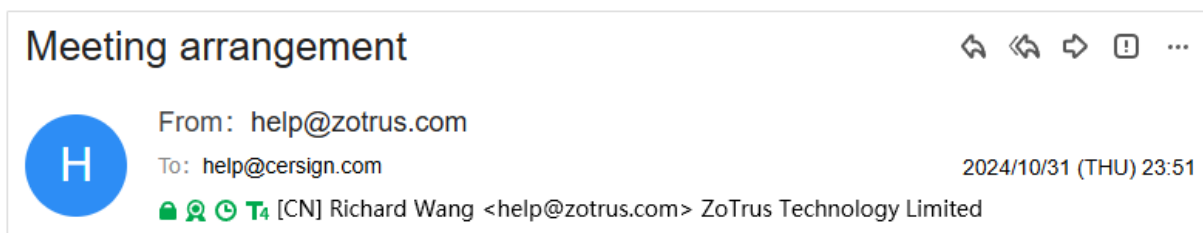
If using Outlook to view the same email above, as shown in the figure below, the time displayed in Outlook is 23:34, which is the time of the sender's computer, and the computer time of the email sender is 17 minutes slower than the standard time.
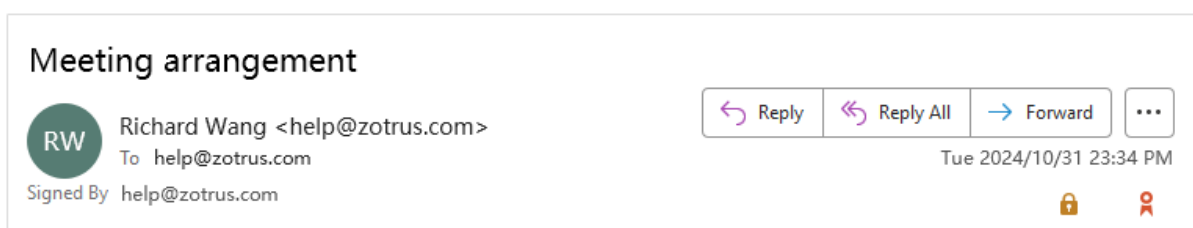
3. What are the special advantages of ZoTrus Email Timestamping Service? What scenarios can it be used for?

ZoTrus Email Timestamping Service is a free innovative supporting service for ZoTrus Email Encryption Automation Service. For the first time in the world, every email has a trusted sending time. This timestamp signature does not rely on a third-party timestamping service, but it is provided by a third-party software - ZT Browser on the user's own computer. It is more reliable than traditional timestamping service, better protects user privacy, and is also a trusted timestamping service.

ZoTrus email timestamping service can be used for various Internet applications that require proof of email sending time, such as the need to prove that a certain file must be submitted before a certain time. The deadline requirements for various email submissions and email declaration can all use this email timestamping service. Users only need to submit emails through ZT Browser. All business completion notification emails, express delivery notification emails, bill emails, etc. can all use the email timestamping service to prove the email sending time and related service delivery time. The author firmly believes that with the popularization and application of ZoTrus email encryption automation service, its email timestamping service will definitely have more value-added service innovations, so that emails can also have trusted postmarks like traditional mails, enhancing the service capabilities

and service scope of emails.

Email timestamping automation provides email timestamping service by the email timestamping certificate issued by the email certificate automation, and the email certificate automation, public key exchange automation and key management automation work together to perfectly realize the email encryption automation service, the first three automation is necessary for the email encryption automation, and the last automation is the icing on the cake, making the ZoTrus email encryption automation solution better, and more perfect to provide email encryption automation service for global users.

Richard Wang

November 11, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 79 articles in English (more than 101K words)
and 190 articles in Chinese (more than 542K characters in total).