Cryptography automation + Innovative UI, new solutions to deal with new threats

People can no longer live without the Internet, whether for work or life. However, while the Internet brings convenience to people, it also brings many security threats. This article summarizes the three most recent security threats and provides solutions to eliminate them, which is the innovative client-to-cloud integrated cryptographic application. And how can people clearly understand that the cryptographic application is protecting people's online security? That is the UI innovation of ZT Browser, which makes the cryptographic application visual.

1. Three major cybersecurity threats to Internet life

The first thing in Internet life is browsing information, online shopping, online banking, online securities, online office and other online activities. Whether it is through browser or APP, the biggest security threat is fake websites and data theft, which is to impersonate various high-value websites to deceive users and defraud money; data theft is to illegally steal user confidential data and illegally tamper with important data submitted by users through illegal means on the data transmission channel of plaintext HTTP websites. According to Cybersecurity Ventures, by 2024, global cybercrime losses (including fake websites, phishing and related fraud) are expected to exceed US$ 10 trillion, with fake e-commerce websites selling counterfeit goods and fake bank websites obtaining user login account information and transferring account funds. Global estimates show that if the direct financial blow and secondary costs such as legal fees and recovery efforts are considered, fake websites alone may cause losses of hundreds of billions of dollars. Recently, many fake websites and apps of well-known AI service have appeared, and many AI applications are deployed in HTTP plaintext, which is very insecure and cannot ensure the security of AI applications.

The second thing in Internet life is sending and receiving emails, which is something that everyone must do every day. However, since emails have been sent and received in plain text since their invention, the content of emails is very easy to be illegally stolen and tampered with during transmission and storage, which is very unsecure. According to the "2023 Internet Crime Report"

released by the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI), Business Email Compromise (BEC) caused US$2.9 billion in losses to US companies in 2023, becoming the second most destructive Internet crime. Between October 2013 and December 2023, BEC attacks caused nearly US$55.5 billion in losses to US and global organizations.

The third thing in Internet life is the management of PDF documents, including reading, publishing, archiving, etc. Since PDF files are also in plain text without a trusted identity, they are very easy to be counterfeited and tampered with, resulting in the proliferation of various fake government documents, fake bank bills, fake contract documents and other fake identity documents. This is the third largest Internet crime, which is estimated to cause hundreds of billions of dollars in global economic losses each year.

The above are the three major cybersecurity threats facing in Internet life. The root cause is that when the Internet was invented, no encryption technology was used. All protocols were in plain text. Because it was only used internally at the time, it was not expected to be so popular today. Of course, industry is constantly making up for this design flaw, so there are various cryptographic technologies used to ensure the security of all Internet applications.

2. Only by deeply integrating cryptographic applications can the three cybersecurity threats be eliminated

It is precisely because the Internet application is so important, therefore, with the deepening of Internet application, there are also various cryptographic technology applications to ensure the security of Internet data transmission, email security and e-document security.

The first cryptographic application is HTTPS encryption, which is the only reliable technology to solve the plaintext HTTP transmission protocol and has been widely used worldwide, including all AI applications. The number of valid publicly trusted SSL certificates has exceeded 1.1 billion now. These SSL certificates are constantly ensuring the data transmission security of the global Internet of Everything, thus eliminating the illegal theft and illegal tampering of data during the transmission process. Of course, such a large-scale cryptographic application is inseparable from automation. Only by realizing the automatic application and deployment of SSL certificates can this cryptographic

technology be widely used to ensure the security of global data circulation.

However, the currently popular HTTPS technology has not solved the problem of fake websites. Instead, it has made it more difficult for people to identify fake websites, because fake websites also have a padlock icon. This icon, which was previously taught to indicate that the website is secure, has become a protective umbrella for fake website crimes. This may be one of the considerations for Google Chrome to no longer display the padlock icon, but it has not solved the problem and has not helped users correctly identify the trusted identity of the website. This is a difficult problem that has not been solved in website security. The SSL certificate widely used by websites around the world is a DV SSL certificate that does not contain website identity information. The DV SSL certificate only has an encryption function, and its function of proving the identity of the website has been castrated, so it cannot be used to solve the problem of fake websites. Its advantage is that it can be automatically issued, which lowers the threshold for the popularization of SSL certificates, thereby promoting the popularization and application of HTTPS encryption. The latest global SSL certificate issuance data shows that OV SSL certificates that can prove the trusted identity of a website have also begun to be automatically issued and deployed. The default SM2 SSL certificate configured for ZoTrus HTTPS Automation Gateway is the OV SSL certificate, and the default dual-algorithm (RSA/SM2) intranet SSL certificate configured for ZoTrus Intranet HTTPS Automation Gateway is also the OV SSL certificate.

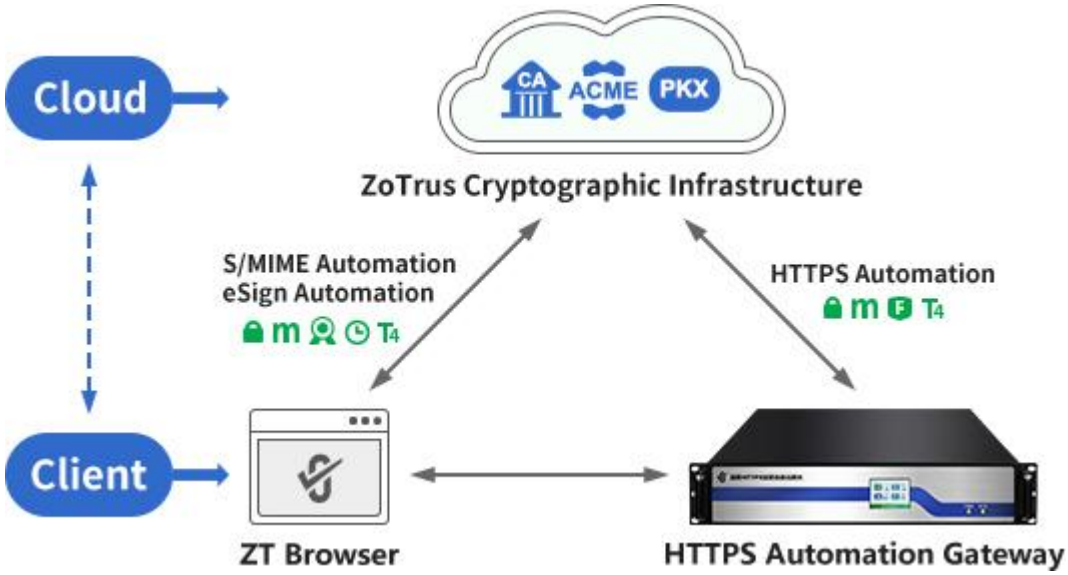
The second cryptographic application is S/MIME encryption and digital signature, which is the only reliable technology to solve the security of plain text emails. Email digital signature technology can effectively solve the problem of email identity fraud, and email encryption technology can effectively solve the problem of email leakage, and solve the security issues of email transmission in transit and in cloud storage. Although S/MIME email encryption technology was released at the same time as HTTPS encryption technology, it is too difficult to use and has not been widely used so far, let alone popularized. To implement S/MIME email encryption, it is necessary to learn from the popularization experience of HTTPS encryption, that is, to realize the automated management of S/MIME email certificates. Only in this way can S/MIME technology be popularized to ensure global email security. ZoTrus Technology uses client-to-cloud integration to achieve automatic S/MIME encryption and digital signatures for emails, completely solving the technical problems that have puzzled email users

around the world for more than half a century. Users only need to enable the automatic email encryption service, then the free S/MIME email certificates are automatically configured, then use ZT Browser to automatically encrypt each outgoing email, automatically decrypt each received encrypted email, and automatically implement the digital signature and timestamp of each outgoing email, reliably proving the trusted identity of each sender and the trusted email sending time.

The third cryptographic application is document digital signature (eSign) and encryption, which is the only reliable technology to solve the problem of plain text PDF documents without trusted identity information. It has been widely used in electronic contract signing. However, it has not been widely used in daily document management, including office documents. And, if we want to solve the problem of confidential document leakage, the only reliable solution is to encrypt the document with a certificate. Only those who have the key can decrypt and read this encrypted document, then there is no need to have a variety of management methods to prevent the leakage of confidential documents. Users only need to keep the document encrypting certificate used for decryption. Document digital signature can effectively solve the problem of document identity trust, and document encryption can completely solve the problem of confidential document leakage. If we want to popularize these two cryptographic applications, the only feasible solution is to automate certificate management and application. ZoTrus Technology will continue to use client-to-cloud integration to automatically configure document signing certificates and document encrypting certificates, automatically implement digital signatures and encryption of electronic documents, effectively prove the trusted identity of each electronic document and ensure the security of each confidential document.

ZoTrus Technology innovation solution is a client-cloud integrated solution, which has invested in the construction of cloud cryptography infrastructure to realize the computing power required for certificate automation services in the "cloud", and can provide dual-algorithm (RSA/SM2) SSL certificates, email certificates and document certificate automatic issuance services for HTTPS automation, S/MIME automation, and eSign automation, completely solving the computing power and automation service capabilities that cannot be realized by only the "client". ZT Browser and ZoTrus HTTPS Automation Gateway are two important "clients", the former is to ensure that the user's key data is on the "client" to completely solve the privacy protection problem of "cloud only"; The

latter is to realize the user's key application on the "client" to completely solve the problem that the web server needs to install the ACME client in order to realize the SSL certificate automation.



3. Only innovative UI can make users aware of cryptographic applications and use the Internet with confidence

The three cybersecurity threats in Internet life can only be eliminated by deeply integrating cryptographic applications. However, if cryptographic applications are invisible and intangible, users will not be able to perceive that cryptographic technology has been used to ensure Internet security. This is why browsers have had a padlock icon since the invention of HTTPS encryption, so that users know that HTTPS encryption has been implemented as soon as they see this icon, and can safely exchange data and online transactions in websites.

However, with the popularity of HTTPS encryption, fraudulent websites also display the padlock icon, which led to the come out of the green address bar of EV SSL certificates, and the improvement of displaying the website owner name directly in the address bar. Unfortunately, Google Chrome was the first to abandon this good solution, allowing fraudulent websites to make a comeback and menacing. ZT Browser makes up for this regret. It is currently the only browser in the world that continues to support EV SSL certificate deployment websites to display green address bar and organization name. It also displays a light green bar and organization name for websites that have deployed OV SSL certificates, and it uses a special icon to identify websites that have deployed SM2 SSL certificates.

There are also more innovative UIs that allow users to quickly perceive cryptographic applications that resolve three security threats - HTTPS encryption, S/MIME email encryption and digital signatures, and document digital signatures and encryption.

ZT Browser is not only a must-have browser for surfing the Internet, but also an email client that can send and receive encrypted emails. It is also a PDF document reader that can verify the digital signature of a document in real time and display the trusted identity of the signer. Its rich UI display allows users to see at a glance whether the website is secure, whether the email is secure, and whether the document is secure.

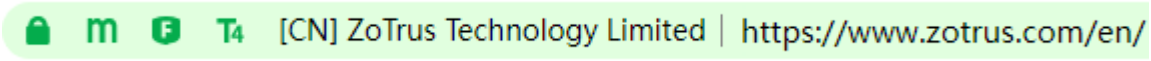
To let users to directly perceive the HTTPS encryption, ZT Browser innovates the UI to achieve:

(1) **Padlock icon**: directly inform users that this website has implemented HTTPS encryption in the first position of the address bar.

(2) **SM2 algorithm icon**: displayed next to the padlock to inform users that this website has implemented SM2 algorithm HTTPS encryption.

(3) **WAF protection icon**: directly tell users in the address bar that this website has adopted web application firewall protection.

(4) **Trust level icon**: display the website's trusted identity information that has been validated by an authoritative third party in front of the https:// URL.



To let users to directly perceive the S/MIME encryption, ZT Browser innovates the UI to achieve:

(1) **Padlock icon**: Indicates that this email is encrypted

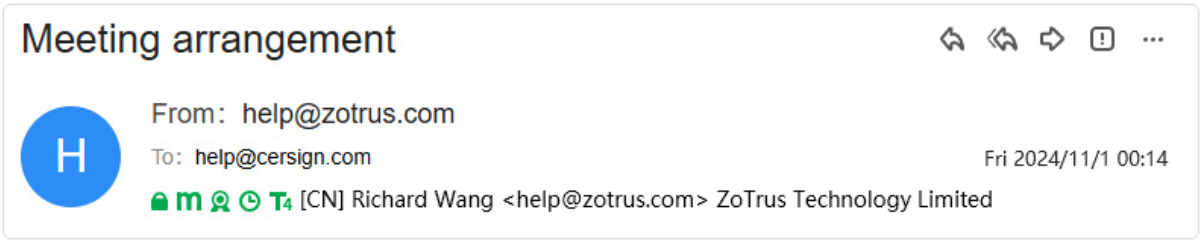
(2) **SM2 algorithm icon**: displayed next to the padlock, indicating that this email has been encrypted with the SM2 algorithm.

(3) **Digital signature icon**: This indicates that the email has been digitally signed, the email content has not been tampered with, and the sender identity is trusted.

(4) **Timestamp icon**: This indicates that the email has an email timestamp, and the email sending time is trusted and non-repudiation.

(5) **Trust level icon**: displays the sender's trusted identity information that has been validated by

an authoritative third party.



To let users to directly perceive the eSign service, ZT Browser innovates the UI to achieve:

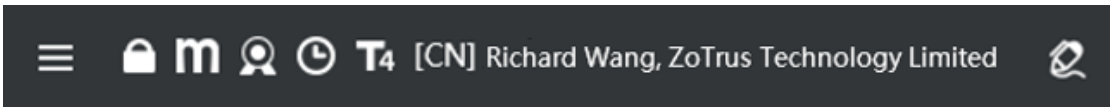
(1) **Padlock icon**: Indicates that this document is encrypted.

(2) **SM2 algorithm icon**: displayed next to the padlock, indicating that this document has been encrypted with the SM2 algorithm.

(3) **Digital signature icon**: Indicates that the document has been digitally signed, the document content has not been tampered with, and the identity of the document publisher is trusted.

(4) **Timestamp icon**: This indicates that the document has a timestamp, and the release time of the document is trusted and non-repudiation.

(5) **Trust level icon**: displays the trusted identity information of the document publisher that has been validated by an authoritative third party.



The innovative client-to-cloud integration of ZoTrus Technology not only realizes HTTPS encryption automation, email encryption automation and document signing automation, but also integrates the PDF reader and email client into the ZT Browser. The world's exclusive innovative UI displays various cryptographic application effects, making the invisible cryptographic applications clear at a glance, letting users to truly feel the charm of cryptographic applications, letting users to use the Internet with confidence, enhancing users' online trust, and facilitating more online transactions.

Richard Wang

April 14, 2025

In Shenzhen, China

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

The author has published 90 articles in English (more than 119K words)

and 208 articles in Chinese (more than 611K characters in total).