Document Security Needs to Be “Visible”

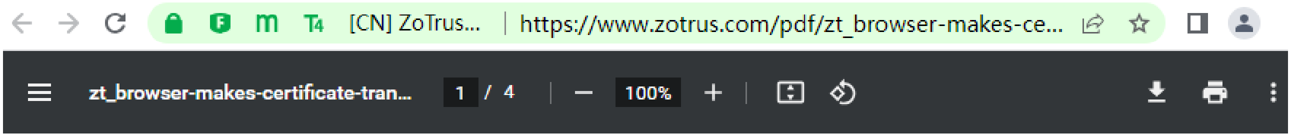
The author wrote an article "Website security needs to be "Visible" " about how ZT Browser displays 4 different icons on the browser address bar, so that users can understand at a glance whether the website they are visiting is secure and trustworthy. Readers who have not read this article can read it to have a comprehensive understanding of the user interface (UI) innovation of ZT Browser. Today's article is "Document security needs to be "Visible"" that it is a sibling of "Website security needs to be "Visible"". They are all about the UI innovation of ZT Browser, and this article is about ZT Browser’s latest UI innovations in the PDF Rader that it is of course also innovations in the application of cryptographic technology, because cryptography is invisible and intangible, so we must have an eye-catching UI to experience the cryptographic application and experience the contribution of cryptography in protecting document security.

Whether a document is secure or not is generally invisible. When you open a PDF file, you can only see the document content, but who published this document? Is the organization name displayed on the document header trusted? Is the red seal at the end of the document trustworthy? In the era of paper documents, official documents received through trusted channels can of course be identified based on the official seal on the front page and the back. This is a trusted way. However, in the digital age of the Internet, it is very easy to create a beautiful fake identity PDF document, and the cost of counterfeiting is zero. This has led to the proliferation of fake identity documents, not only fake government documents, but also fake bank statement, fake academic certificates, etc. How can we effectively helping users identify the authenticity of PDF documents is the responsibility and obligation placed in front of all PDF Readers.

Fortunately, when Adobe invented the PDF format document, it also used cryptography technology to ensure the trusted identity of the PDF document publisher. China ODF format document also has a similar solution, which also uses cryptography technology to implement document digital signature to ensure the trusted identity of the document publisher. The current status quo is that various readers that can open PDF documents (including browsers and readers that embedded in various APPs) do not support real-time recognition of digital signatures of PDF documents, and do not show the effect of the cryptography application to ensure the security of the document, letting the end user to see that the document has a digital signature to ensure the trusted identity of the document.

This is the problem that the upgraded version of ZT Browser aims to solve - to make documents security visible, so that end users can know at a glance whether the document is trustworthy when opening and reading the document. When a user uses ZT Browser to read a PDF document, the various icons displayed on the browser address bar are clearly explained by the author in "Website security needs to be "Visible"". This article talks about the innovative UI in the browser document reading bar (PDF bar) in detail, the PDF bar is under the address bar.

As shown in the figure below, when reading PDF documents, almost all browsers will add a document reading bar below the address bar to display document-related functions, such as displaying all pages of the document, document file name, page number, zoom in and out, window width, page rotation, document download, document printing, full-screen presentation and other functions related to various document operations.


[CN] ZoTrus...
https://www.zotrus.com/pdf/zt_browser-makes-ce...
zt_browser-makes-certificate-tran...
1 / 4
100%

ZT Browser believes that it is completely unnecessary to repeatedly display the document file name in the document reading bar, because the complete file name is already displayed on the address bar. ZT Browser innovatively turns the prime location into a document security display area. ZT Browser verify whether the document has a digital signature in real time when it is opened for reading. If so, verify whether it is trustworthy, and if yes, display the trusted identity of the document signer, as shown in Figure 1 below. If not, it will display "This document is not digitally signed; the identity of the publisher is unknown. Be careful!" This is the most important "visible" for document. It is a very eye-catching reminder for users to pay attention to avoid being deceived, as shown in Figure 2 below.

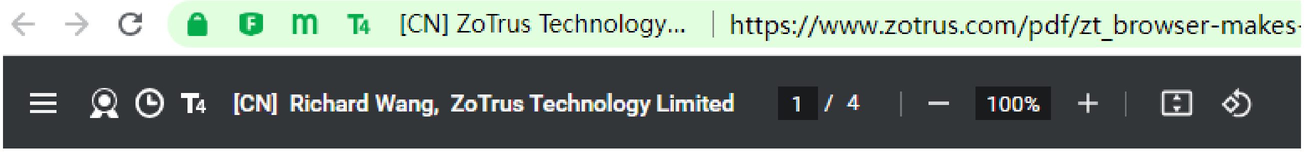
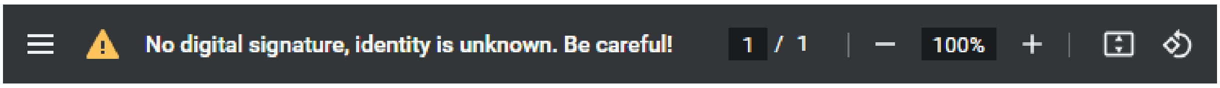

[CN] ZoTrus Technology...
https://www.zotrus.com/pdf/zt_browser-makes-
[CN] Richard Wang, ZoTrus Technology Limited
1 / 4
100%

Figure 1



No digital signature, identity is unknown. Be careful!

Figure 2

This is document security visible! So, what icons are visible for document security? As shown in the Figure 3 below, in addition to reminding users to pay attention to the security of documents without digital signatures, ZT Browser also innovatively adds 5 very distinctive "visible" document security, which can truly help users see whether the document they are reading is secure and trustworthy.

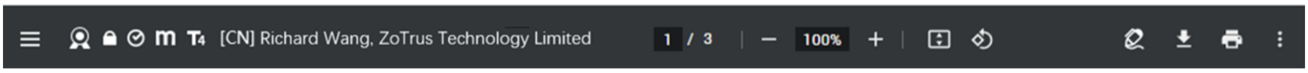
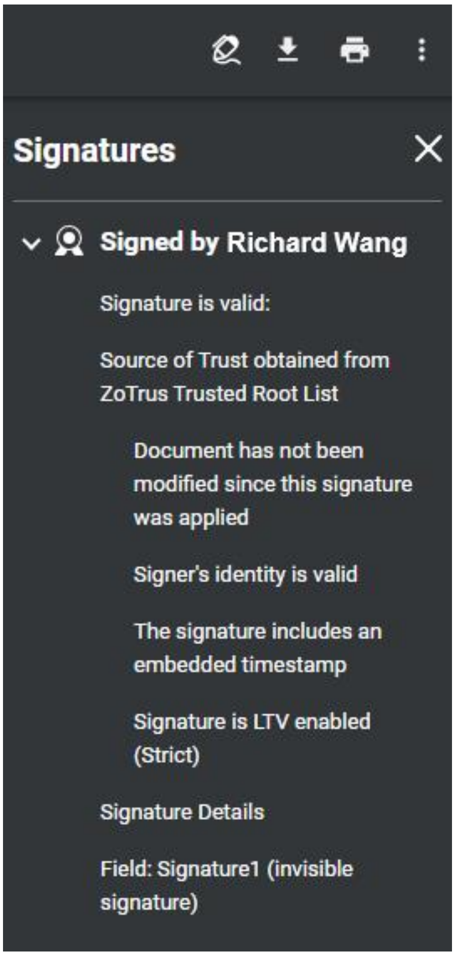


Figure 3

The first "visible" security is the document digitally signed icon

This icon clearly tells the users that the document being read has a trusted digital signature. The user can also click the "Signature Panel" icon on the far right of the PDF bar to view the detailed information of the document's digital signature, as shown in Figures 1 and 2 below. This information includes where the trust source comes from, whether the document has been modified, whether the document has a timestamp, whether it supports LTV (Long Term Validation), and details of the signing certificate, etc.



Signatures

Signed by Richard Wang

Signature is valid:

Source of Trust obtained from ZoTrus Trusted Root List

Document has not been modified since this signature was applied

Signer's identity is valid

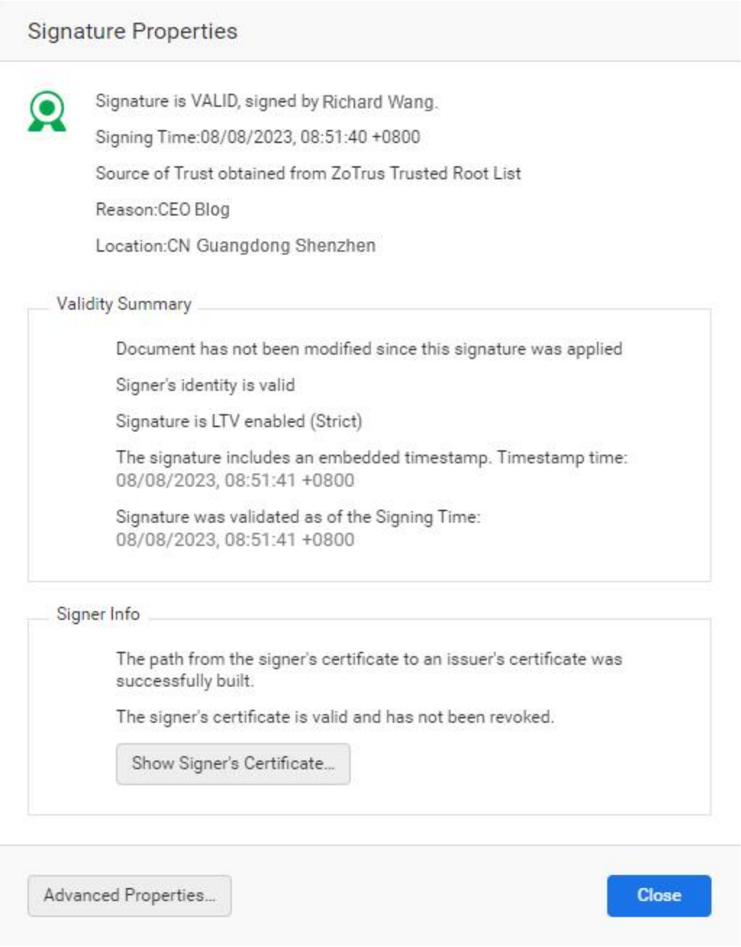
The signature includes an embedded timestamp

Signature is LTV enabled (Strict)

Signature Details

Field: Signature1 (invisible signature)

Figure 4



Signature Properties

Signature is VALID, signed by Richard Wang.

Signing Time:08/08/2023, 08:51:40 +0800

Source of Trust obtained from ZoTrus Trusted Root List

Reason:CEO Blog

Location:CN Guangdong Shenzhen

Validity Summary

Document has not been modified since this signature was applied

Signer's identity is valid

Signature is LTV enabled (Strict)

The signature includes an embedded timestamp. Timestamp time: 08/08/2023, 08:51:41 +0800

Signature was validated as of the Signing Time: 08/08/2023, 08:51:41 +0800

Signer Info

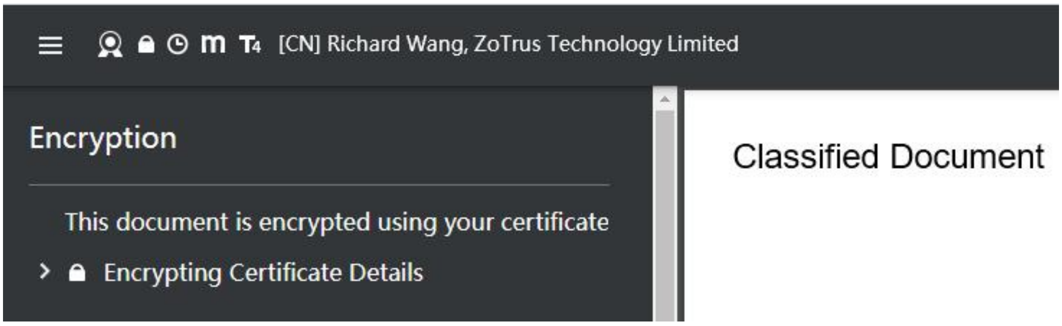
The path from the signer's certificate to an issuer's certificate was successfully built.

The signer's certificate is valid and has not been revoked.

Figure 5

The second "visible" security is the document encrypted icon 🔒

This icon clearly tells the users that the document being read is an encrypted document. If the user has the right to read this document, the document will be automatically decrypted and read seamlessly, as shown in Figure 3 below. If ZT Browser cannot find the digital certificate used for decryption, it will remind the user that it cannot be decrypted, as shown in Figure 4 below. This is the only reliable technical means to ensure the security of classified documents, because as long as the documents are not encrypted, there is no guarantee that the documents will not be illegally leaked. However, if the document is encrypted with the encrypting certificate of the authorized person, even if the confidential document is leaked, it cannot be decrypted because the private key of the authorized person's certificate cannot be obtained, thus effectively ensuring the security of the classified document.



[CN] Richard Wang, ZoTrus Technology Limited

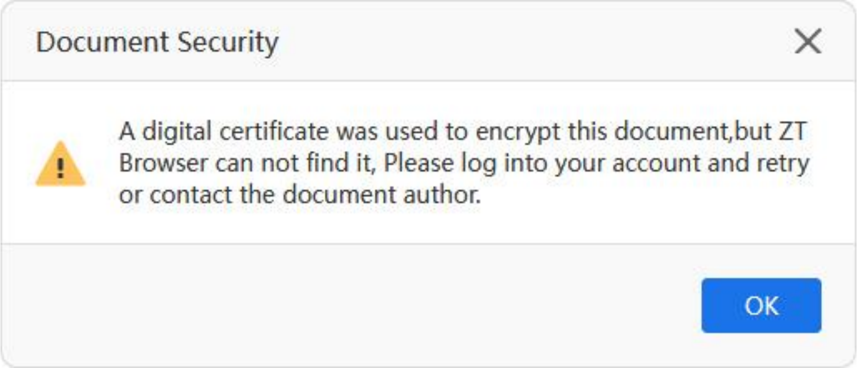
Encryption

This document is encrypted using your certificate

> Encrypting Certificate Details

Classified Document

Figure 6



Document Security

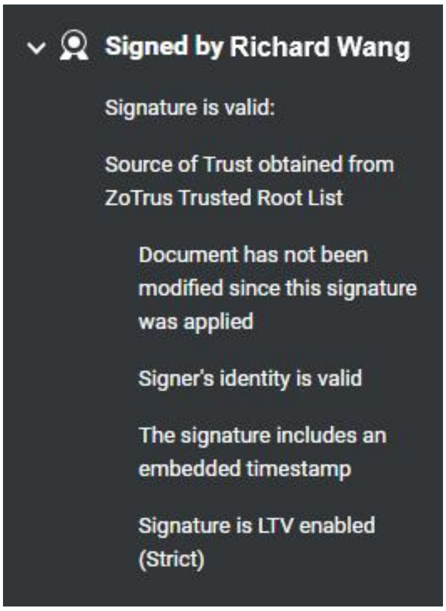
A digital certificate was used to encrypt this document,but ZT Browser can not find it, Please log into your account and retry or contact the document author.

Figure 7

The third "visible" security is the document timestamped icon ✓

This icon clearly tells the user that the document being read is signed by a timestamp service, and the document signature time is trusted. As shown in Figure 8 below, this document not only has a digital signature, but also a timestamp signature trusted by ZT Browser - "The signature includes an embedded timestamp". If the document is signed without using a timestamp service, it will display "Signing time is from the clock on the signer's computer." See Figure 9. Everyone knows that computer time can be modified at will, and this is an untrusted time. Therefore, when it is necessary to prove the time when signer signed the document, timestamp is the only solution, which can ensure that the signature time is trusted, non-repudiation, and cannot be tampered with. There are many applications that require timestamps, such as e-contract signing, official document release, submission documents, bidding documents, etc., all of which have trusted signature time requirements. ZT Browser has been included and trusted the timestamp signing certificates of some timestamp service providers, and only timestamp signatures trusted by ZT Browser are displayed.

Please also pay attention to another related "visible" - LTV (Long Term Validation), which is a technical parameter related to the timestamp. If the signing time comes from the signer's computer clock, this is the default LTV state set by Adobe Reader, the premise is that the signer's computer time is trusted. The "Strict LTV" status will only be displayed when the document signature has an embedded timestamp, indicating that the signer's computer time is not trusted because it can be modified at will.



Signed by Richard Wang

Signature is valid:

Source of Trust obtained from ZoTrus Trusted Root List

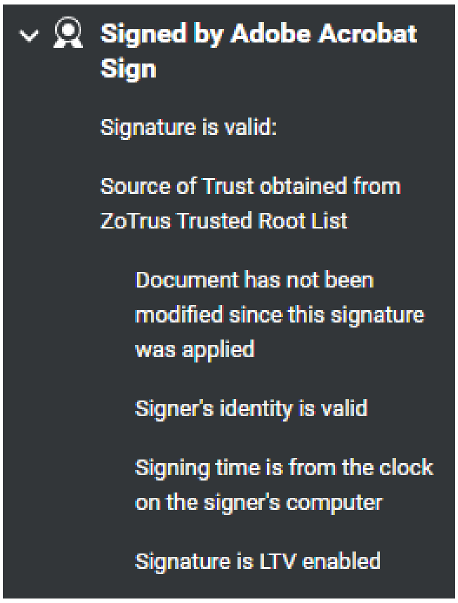
Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp

Signature is LTV enabled (Strict)

Figure 8



Signed by Adobe Acrobat Sign

Signature is valid:

Source of Trust obtained from ZoTrus Trusted Root List

Document has not been modified since this signature was applied

Signer's identity is valid

Signing time is from the clock on the signer's computer

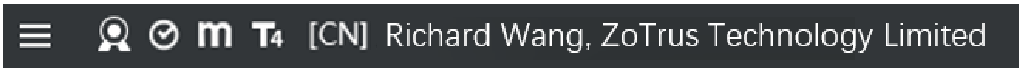
Signature is LTV enabled

Figure 9

The fourth "visible" security is the document signed by SM2 signing certificate for cryptography compliance m

This icon clearly tells the user that the document being read is signed with a SM2 signing certificate or encrypted by SM2 encrypting certificate. According to China "Electronic Signature Law" and "Cryptography Law", reliable digital signatures should be implemented using the SM2 algorithm. However, given that the commonly used Adobe Reader does not support the SM2 algorithm, this limits the use of the SM2 algorithm to achieve document signing application scenarios. ZT Browser PDF Reader supports the verification of PDF documents and OFD documents digitally signed by SM2 signing certificate, and displays the cryptography compliance icon, laying an application foundation for the popularization of electronic documents digitally signed by the SM2 algorithm.

ZT Browser PDF Reader supports real-time verification of dual-algorithm dual digital signatures and gives priority to displaying the SM2 algorithm digital signature in the document. The ZoTrus document digital signing service planned to be provided also use dual-algorithm document signing certificates by default to achieve dual signatures and dual timestamps. RSA signatures are only for compatibility with Adobe Reader, while SM2 signatures are for cryptography compliance. For document encryption, it is more secure and reliable to use the SM2 algorithm to achieve encryption. Therefore, ZT Browser PDF Reader uses the same cryptography compliance icon (**m**) as the SM2 HTTPS encryption to display the SM2 algorithm digital signature and document encryption.

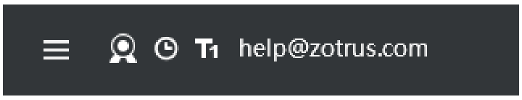


m T4 [CN] Richard Wang, ZoTrus Technology Limited

Figure 10

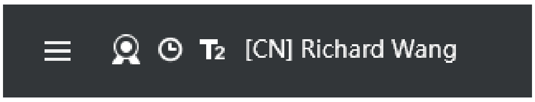
The fifth "visible" security is the icons for identity trusted level of the document signer and the trusted identity information of the signer T4

This icon clearly tells the user the identity trusted level of the signer of the document being read, which is divided into four levels: T1/T2/T3/T4. After the trusted level icon, the CN field and O field (if any) information in the signing certificate is displayed, as per [Country abbreviation] + CN field format display. The T1 level only displays the signer's email address because the signer has only validated the email address, as shown in Figure 7 below; the T2 level displays the signer's full name because the signer has validated his/her personal identity, as shown in Figure 8 below; the T3 level displays the signer's organization name because the signer has validated the organization identity, as shown in Figure 9 below; the T4 level displays the signer's full name and organization name because the signer not only validated the personal identity but also the organization identity, and the signer is an employee of this organization, as shown in Figure 10 below.



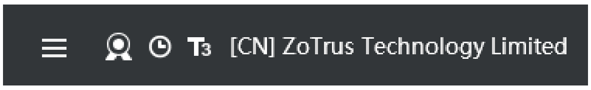
T1 help@zotrus.com

Figure 11



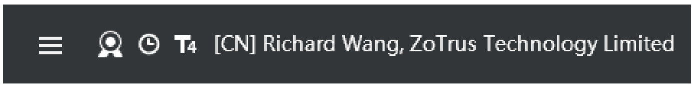
T2 [CN] Richard Wang

Figure 12



T3 [CN] ZoTrus Technology Limited

Figure 13



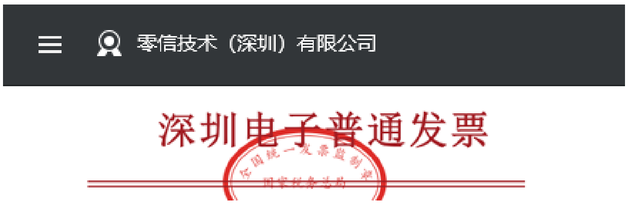
T4 [CN] Richard Wang, ZoTrus Technology Limited

Figure 14

Some readers may have questions, why is the trusted level of employee signatures of an organization T4 higher than the trusted level of organization signatures T3? These are the first three types of identity validation levels that follow the SSL certificate identity validation. T3 level is similar to the validation level of the OV SSL certificate and validated the identity of the organization. The T4 icon in the SSL certificate is used for the EV SSL certificate, while ZT Browser continues to use the T4 icon for digital signature of organization employee, which means T3+1 validation, which not only validates the identity of the organization, but also validates the employee's personal identity, it is reasonable to use the T4 icon.

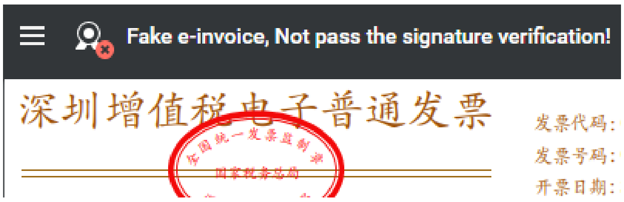
ZT Browser believes that it is very important to distinguish the trusted level of document digital signatures, because it is not enough to just show that the document has a digital signature. In Europe, many company names are the same as personal names, so it is very important to directly and clearly tell the user whether the signer is an individual, an organization or an employee of the organization, so that the user can make correct processing decisions based on the identity of the signer.

It is worth mentioning that ZT Browser not only displays the trusted identity of the digital signer of the document but is also optimized for the verification the e-invoices in China. Although e-invoices are also PDF documents, e-invoice is a special purposes PDF document, therefore, after verifying the digital signature of the e-invoice, ZT Browser directly displays the authenticity of the e-invoice, which greatly facilitates users to identify the authenticity of the e-invoice. Adobe Reader displays "At least one signature has problems" because the digital signing certificate used in the e-invoice is not trusted by Adobe.



零信技术（深圳）有限公司

深圳电子普通发票



Fake e-invoice, Not pass the signature verification!

深圳增值税电子普通发票

发票代码:
发票号码:
开票日期:

ZT Browser currently only included and trusted some digital signing certificates for e-invoices. CAs with unrecognized document signing certificate for e-invoice are welcome to contact us to include and trust their special root CA certificates for e-invoice, so that cryptography can ensure the security and trustworthiness of e-invoices. It will be smoother and provide users with a better e-invoice experience, thereby further promoting the healthy development of e-invoice cryptographic applications.

The author believes that readers will be able to fully understand whether a document is secure and trustworthy through the above five "visible" document security innovation. The five secure "Visible" plus one "unsecure" "Visible", a total of 6 "Visible" can effectively help users know at a glance whether the document they are reading is secure and trustworthy. These innovations are exclusively provided by ZT Browser globally and can truly protect users' online security.

The author firmly believes that document security is the second most important focus of the security industry after website security (HTTPS encryption), because documents are everywhere, and this is because of their ubiquity. The security issue has become an urgent problem, and the only solution to solve the document security problem is to use cryptography to protect document security, to use digital signature, encryption, and timestamp to ensure that the identity of the document is trusted, non-tamperable, encryption protected, and document publish time is trusted.

The first important thing to do to ensure document security is to make document security visible, so that users can easily know whether the document they are reading is secure. ZT Browser is the first to do so in the world. Welcome to download and use ZT Browser for free, to experience document security and visibility, and protect your online security.

Richard Wang

October 11, 2023
In Shenzhen, China