All e-Documents Require Zero Trust

Electronic documents (e-documents) generally refer to text and picture formed by people in social activities and carried by chemical and magnetic physical materials such as computer hard drives, magnetic disks, and optical disks, and rely on computer network systems for storage and transmission. The e-documents referred to in this article refer to various electronic files, such as text files, Word files, PPT files, Excel files, PDF files, OFD files, etc.

Compared with traditional printed documents, e-documents have five main characteristics: Easy to modify, Easy to delete, Easy to copy, Easy to damage and Easy to spread. And "Easy to modify" makes e-documents not trustworthy at all, because everyone can easily modify it in any time; "Easy to delete" results in unreliable e-documents because they are easily deleted and disappears; "Easy to copy" results in the leakage of e-documents; "Easy to damage" results in e-documents being unusable, which is the security of storage media, the problem is beyond the scope of this article; "Easy to spread" is the unique advantage of e-documents. It completely solves the problem of paper documents requiring express delivery to achieve exchange. This feature also makes it very easy to leak.

How to solve these security problems in e-documents, especially today with the comprehensive digital transformation of government services and enterprise services, people are inseparable from e-documents whether in daily life or work. Adobe is the first company to provide solutions, it invented PDF format files and PDF file digital signatures. Digital signatures are used to prove the trustworthy identity and ownership (copyright) of the document, and it can prove that the document has not been modified or damaged. Using digital certificates to encrypt documents can effectively solve the problem of document leakage, because only those with the right to read can use their private keys to decrypt the encrypted documents. If technical measures such as watermarks are added to digital signatures and encryption, the problem of e-document leakage can be completely solved. And in order to prove the trusted time of the digital signature, a third-party timestamp signature is also required when the document is digitally signed.

As shown in Figure 1 below, the digital signature information displayed when Adobe Reader views the PDF file of the CEO's blog post, it displayed <Certified by "Wang Gaohua, ZoTrus Technology Limited"> in the signature bar. As shown in Figure 2 below, the digital signature information of this blog post is displayed in ZT Browser version 23. It not only displays the signer information like Adobe Reader, but also adds an icon to prove that this document includes a trusted timestamp signature.

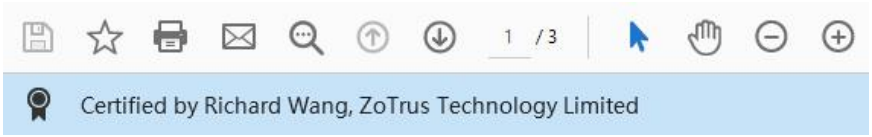

Figure 1

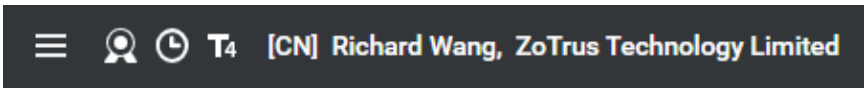

Figure 2

If a PDF document does not have a digital signature, Adobe Reader currently does not give any prompts. Based on the zero trust principles, ZT Browser displays "No digital signature, identity is unknown. Be careful!" This is zero trust to documents without digital signatures, and it is a very eye-catching reminder to users to avoid being deceived.

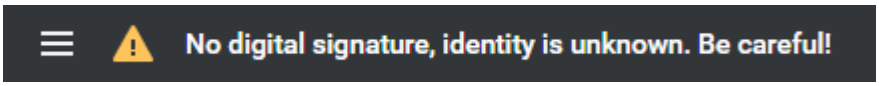

Figure 3

As for classified documents, do not believe that the so-called intranet viewing is secure. You must zero trust to unencrypted classified documents. Only by encrypting classified documents with the digital certificate of the authorized reader can the security of classified documents be truly guaranteed. Non-authorized readers cannot decrypt and read the classified documents even if they obtain them illegally, thus effectively ensuring the security of classified documents.

As shown in Figure 4 below, if the user has the right to read this encrypted document, ZT Browser will automatically use the user's certificate to decrypt the document for non-sensitive decryption and smoothly reading. This is the only reliable technical means to ensure the security of classified documents, because as long as the document is not encrypted, there is no guarantee that the document will not be illegally leaked. As shown in Figure 5 below, if ZT Browser cannot find the digital

certificate used for decryption, it will remind the user that the document cannot be decrypted.

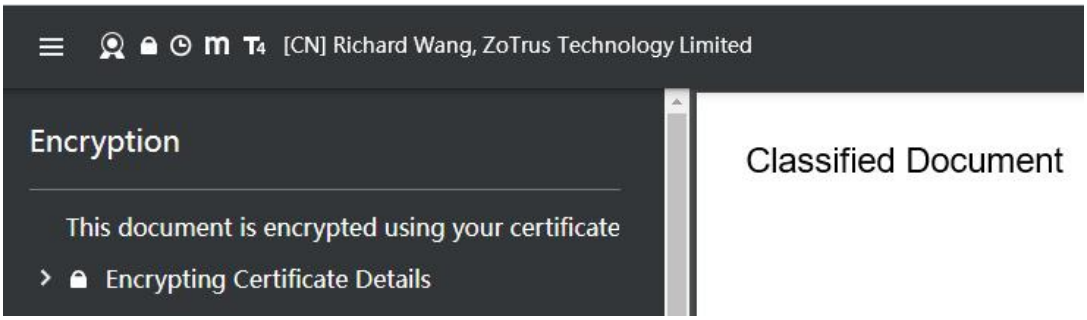

Figure 4

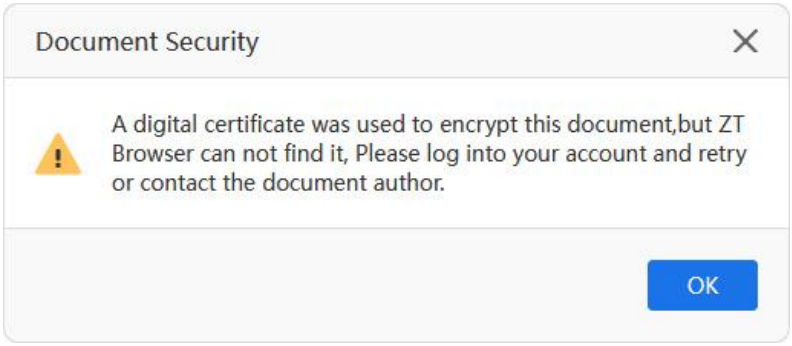

Figure 5

In summary, all e-documents without digital signatures are not trustworthy, because everyone can easily create a PDF file claiming to be issued by someone or a certain organization. All e-documents security requires zero trust, and the e-document digital signature and encryption are the best zero trust document security solutions to ensure document security and trustworthiness.

Richard Wang

October 11, 2023
In Shenzhen, China