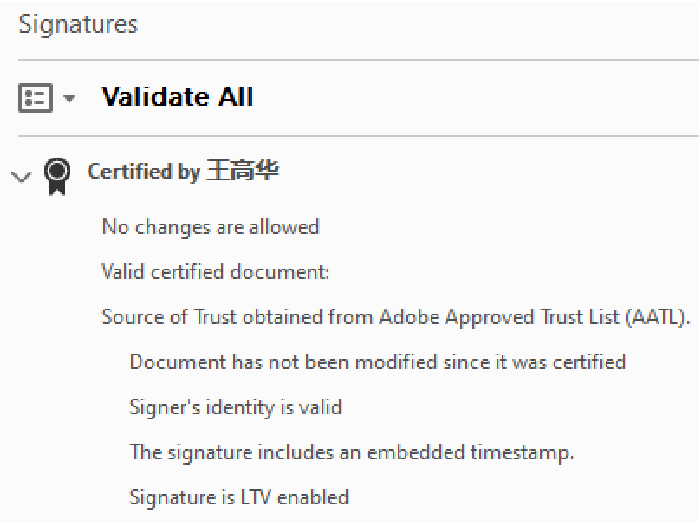
What is LTV? How to make document digital signature valid for a long time?

If readers use Google to search "What is LTV" or "LTV", the results have many explanations, so I would like to inform readers that the "LTV" we are talking about today is a technical term for document digital signature, it is the abbreviation of "Long Term Validation" that it means the digital signature of this document is valid for a long time.

When you use Adobe Reader to open the PDF file of the CEO blog article and click on the "Signature Panel", the following signature information will be displayed. There is a line showing "Signature is LTV enabled", as shown in Figure 1 below. When viewed in ZT Browser, "Signature has strict LTV enabled (long-term validity)" will be displayed, as shown in Figure 2 below. This article talks about why we made such changes.



Signatures

Validate All

Certified by 王高华

No changes are allowed

Valid certified document:

Source of Trust obtained from Adobe Approved Trust List (AATL).

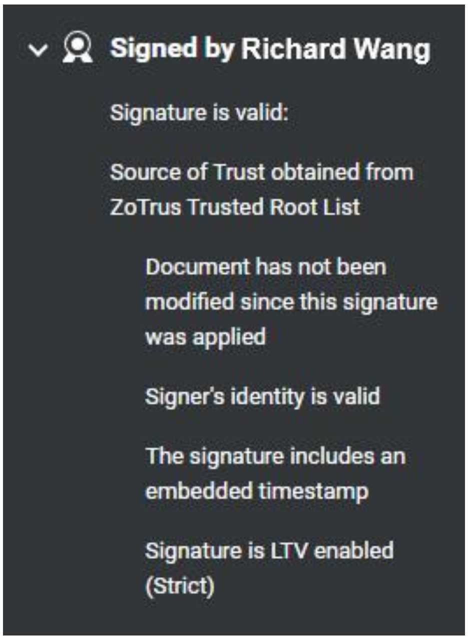
Document has not been modified since it was certified

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

Figure 1



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)

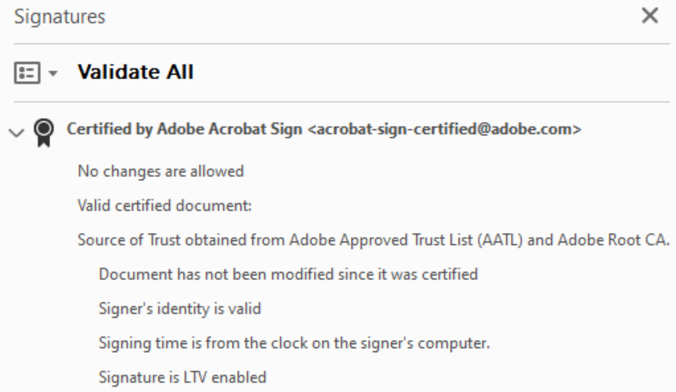
Figure 2

As we all know, all digital certificates have a validity period. Document signing certificates are valid for up to 3 years. However, a document may need to be saved for many years, more than 3 years, or even permanently. So, what if the document signing certificate expires? Even if the signing certificate has expired, can we still ensure that the signed document can be displayed as a valid signature? Are digital signatures still valid?

To meet this application demand, Adobe invented LTV. When signing a document, the LTV parameters are directly added to the signed document to prove that the document signing certificate used to digitally sign the document is valid. This "time" requires a time basis to determine and confirm whether the document signing certificate has expired at the time of signing, and whether the signing certificate has been revoked, and write the signing certificate status information at this time point into the signed document for archiving, which it can be used to determine whether the digital signature is valid later.

So, why does the Adobe Reader display "Signature is LTV enabled" and ZT Browser PDF Reader changes it to " Signature is LTV enabled (Strict)"? Why should ZT Browser add the word "Strict"? This brings us back to the topic in the previous paragraph. Since it is to judge whether it is valid for a long time, the key is the signature time point. Whether this time point is trusted is very critical.

Let’s look at Figure 3 below. This is the signature information displayed in Adobe Reader for a document signed by Adobe Sign. Please note that the bottom one also displays “Signature is LTV enabled”, and the above line is "Signing time is from the clock on the signer's computer" that it tells the user that the time of the signer's computer was used to determine whether the signing certificate had expired, and to query the certificate revocation list at that time. However, please note that the signer's computer time is not trustworthy, and the signer can modify this time at will. In other words, using an untrustworthy time to judge whether the signature of a signed document is trustworthy is itself untrustworthy judgment logic, because the signer can modify the computer time at the time of signing, even if the signing certificate has expired or been revoked, the digital signature can be completed, and the LTV enabled. So why does Adobe Reader trust this data and show that LTV is enabled? The author checked a lot of information before discovering the mystery. As shown in Figure 4 below, there is a "Control how and when signatures are verified" setting in the Adobe Reader Preferences setting. By default, “Time at which the signature was created" is used to verify signature, which is the signer's computer time. In other words, Adobe Reader trusts the signer's computer time by default, so that the LTV enabled can be displayed normally. This may be a compromise adopted by Adobe so that documents without timestamps can also support LTV. It may also be to take care of its own Adobe Sign business, because the Adobe Sign electronic signature service does not use timestamp service.



Signatures

Validate All

Certified by Adobe Acrobat Sign <acrobat-sign-certified@adobe.com>

No changes are allowed

Valid certified document:

Source of Trust obtained from Adobe Approved Trust List (AATL) and Adobe Root CA.

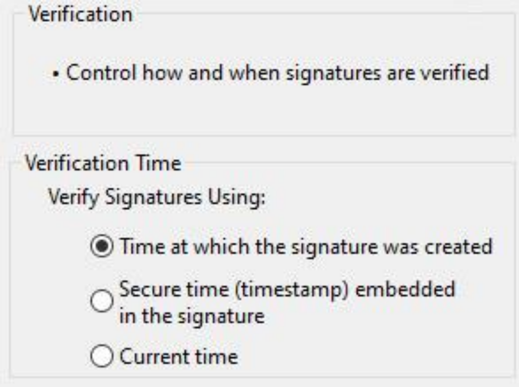
Document has not been modified since it was certified

Signer's identity is valid

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

Signature is LTV enabled

Figure 3



Verification

- Control how and when signatures are verified

Verification Time

Verify Signatures Using:

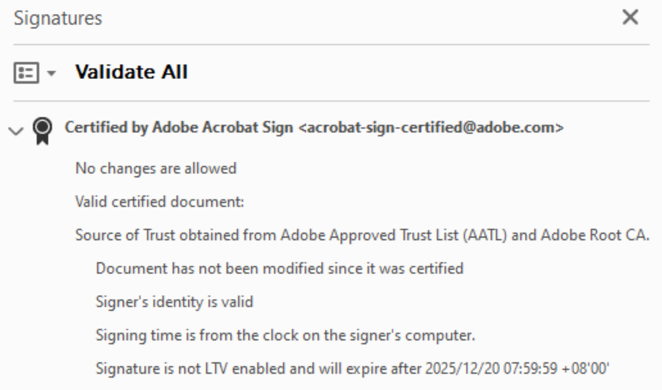
● Time at which the signature was created

○ Secure time (timestamp) embedded in the signature

○ Current time

Figure 4

If you set the default verification time to "Secure time (timestamp) embedded in the signature" in Adobe Reader, documents that originally displayed “LTV enabled” normally will be displayed as "Signature is not LTV enabled", and the signed document valid will expire after the signing certificate expires. As shown in Figure 5 below. For signed documents whose signing certificate has expired, Adobe Reader display "Signer’s identity is invalid because it has expired", as shown in Figure 6 below. If you change the default verification time setting to " Time at which the signature was created", then the document in Figure 6 will display “LTV enabled” again.



Signatures

Validate All

Certified by Adobe Acrobat Sign <acrobat-sign-certified@adobe.com>

No changes are allowed

Valid certified document:

Source of Trust obtained from Adobe Approved Trust List (AATL) and Adobe Root CA.

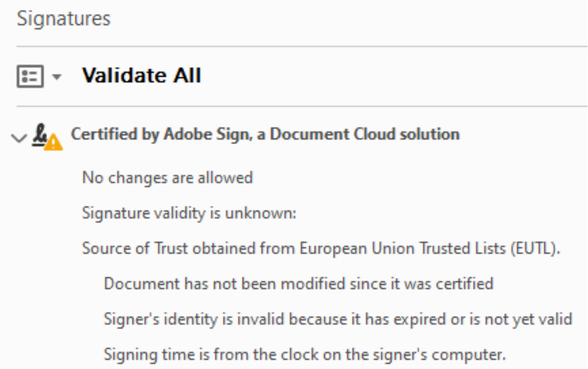
Document has not been modified since it was certified

Signer's identity is valid

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

Signature is not LTV enabled and will expire after 2025/12/20 07:59:59 +08'00'

Figure 5



Signatures

Validate All

Certified by Adobe Sign, a Document Cloud solution

No changes are allowed

Signature validity is unknown:

Source of Trust obtained from European Union Trusted Lists (EUTL).

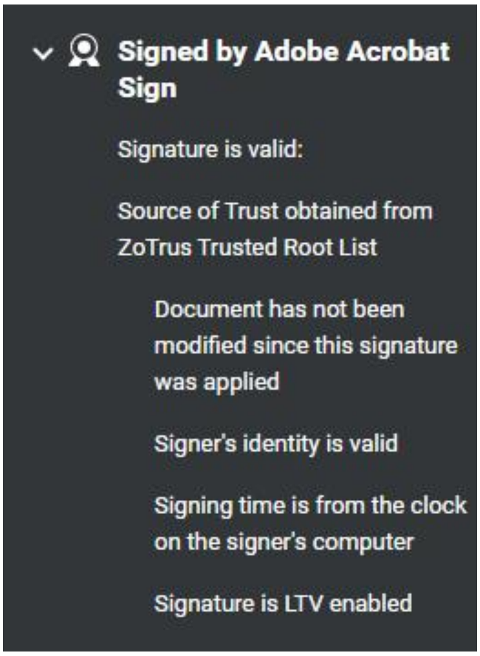
Document has not been modified since it was certified

Signer's identity is invalid because it has expired or is not yet valid

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

Figure 6

The above describes how Adobe Reader displays the LTV attribute. For signed documents that do not have a timestamp signature but have LTV data, ZT Browser PDF Reader also adopts the same policy as Adobe by default and will also show that it is LTV enabled, as shown in Figure 7 below. However, for signed documents with timestamps and LTV data, as shown in Figure 8 below, ZT Browser displays "Signature is LTV enabled (Strict)", which is the first "Strict LTV" concept proposed in the industry, because the time of this LTV signature time point comes from a trusted timestamp signature, which is a trusted time. This is a more strict LTV verification. Therefore, ZT Browser gives a different status identifier - Strict LTV, similar to HSTS (HTTP Strict Transport Security), this is the truly trusted LTV enabled, because the time point that LTV relies on is a trusted timestamp, not the user's computer time. In this way, no matter how the Verification Time is set in Adobe Reader, it must display "LTV Enabled".



Signed by Adobe Acrobat Sign

Signature is valid:

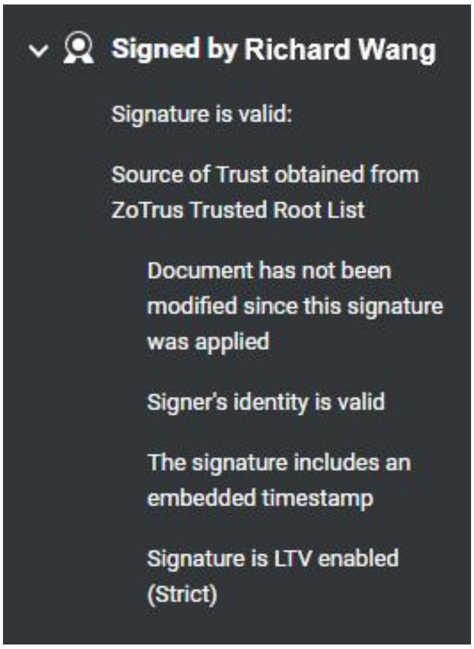
Source of Trust obtained from ZoTrus Trusted Root List

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



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 7

Figure 8

The author believes that readers have understood the importance of adding a timestamp when signing document. With the timestamp, the “LTV enabled” information can be displayed normally no matter how the user's Adobe reader is set. If not, it depends on the user's specific settings. This is the fundamental reason why ZT Browser distinguishes between these two LTV statuses. One is a document without timestamp, which displays the same LTV status as the default settings of Adobe Reader. The other is a strict LTV status for signed document with timestamp, which supports LTV no matter how the user sets it.

To summarize, in order to ensure the long term validity of signed documents, digitally signed PDF documents must support LTV feature. In order for the PDF Reader to ensure that the LTV is valid for a long time no matter how the user sets it, a timestamp signature must be attached to the document signature. This is the “Strict LTV” and ensure that the document signature is truly strict and valid for a long time.

Richard Wang

October 16, 2023
In Shenzhen, China