

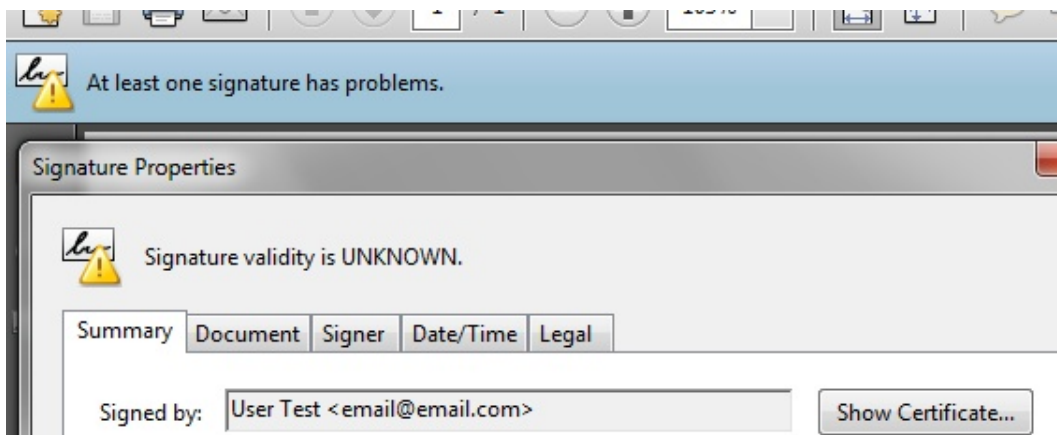
Validating Digital Signatures in Adobe

Every digital certificate is issued by a Root CA (Certification Authority). Some of the Root CA's are included by default in Windows Certificate Store (Trusted Root Certification Authorities) and only a few are included in Adobe Certificate Store. Microsoft and Adobe use different Certificate Stores different certificate validation procedures.

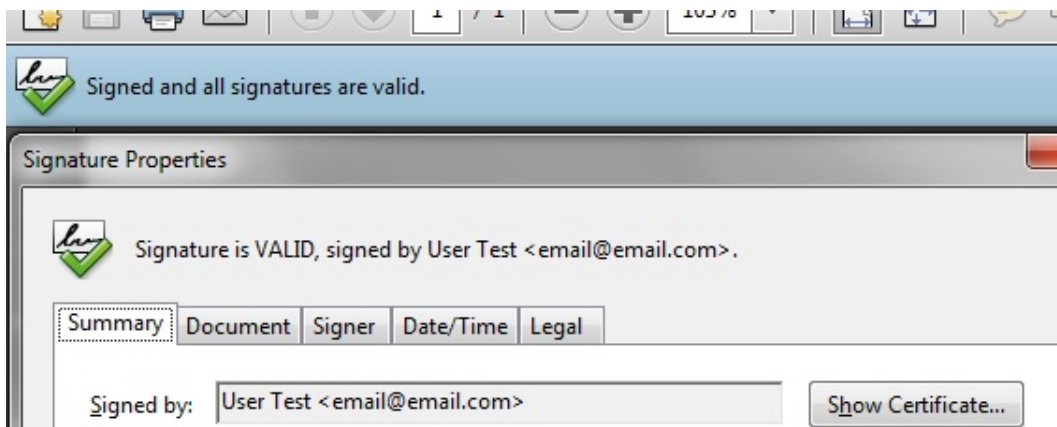
If the signing certificate (or the Root CA that issued the signing certificate) is not included in Adobe Store, the digital signature is considered "not trusted" when a user open a document with Adobe Reader (see example).

This behavior has nothing to do with the signing engine but with the Adobe certification validation procedure.

To trust a signature the user must add the signing certificate on the Adobe Certificate Store because only a few Root CA's are considered trusted by default by Adobe certificate validation engine (See this article: http://www.adobe.com/security/partners_cds.html)



Signature validity is UNKNOWN



Validated digital signature

Validating the time stamping response on Adobe

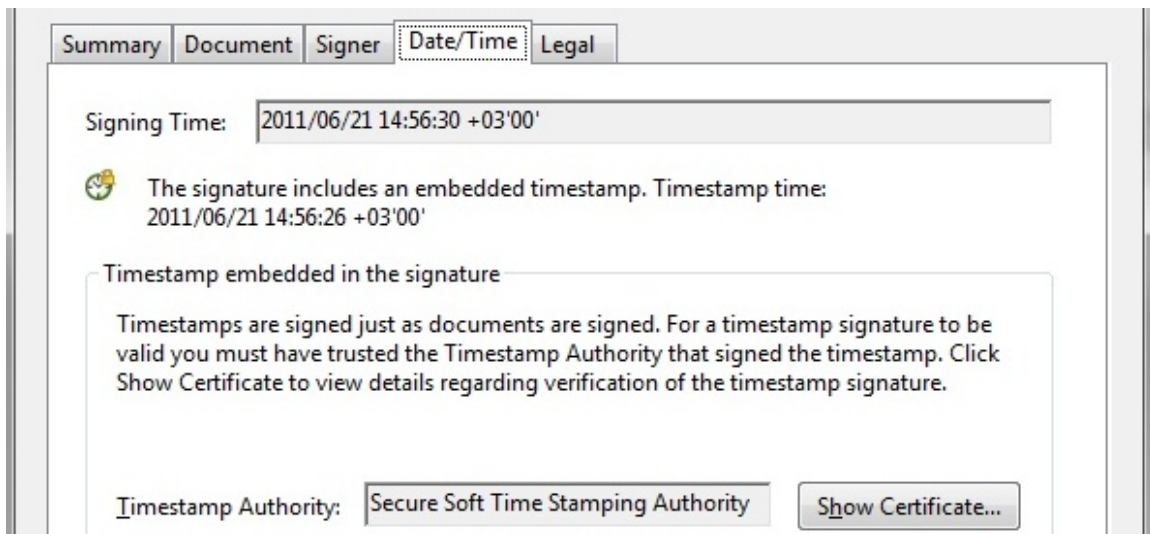
As digital signatures certificates, the time stamping responses are signed by a certificate issued by a Certification Authority.

If the time stamping certificate (or the Root CA that issued the time stamping certificate) is not included in Adobe Store, the time stamping response could not be verified when a user open a document with Adobe Reader (see example).

This behavior has nothing to do with the signing engine but with the Adobe certification validation procedure.



Not verified time stamping response



Trusted time stamping response

To validate the signing certificate (or embedded time stamp) in Adobe use the methods below.

Export the certificate using Acrobat FDF (recommended)

This method is the best solution in case you want to propagate validation to all users that will manage documents signed by your digital certificate.

On the first step you should export the FDF file:

- Open a signed document with a certificate issued by your root certificate.
- Click on the signature rectangle (or go to the *Signatures* tab)
- Click on the *Signature Properties* button
- Go to the *Signer* tab (or *Date/time* tab for time stamping)
- Click on the *Show Certificate* button
- Select the Root certificate (or the signing certificate)
- Go to *Summary* tab
- Click on *Export* button
- Select *Acrobat FDF Data Exchange*
- Click *Next*
- Click *Next* (do not sign the FDF)
- Save the FDF File

After the FDF file is created you can distribute the FDF file to the users. They must follow these steps:

- Open the saved FDF file
- Click on the *Set Contact Trust*
- Check all checkboxes
- Click on *OK* button

After you follow this procedure, all the documents signed by this certificate are recognized as trusted.

Note: The FDF file for the Secure Soft Private CA Root certificate is available at this link: <http://www.signfiles.com/certs/AdobePolicy.fdf>.

To validate the PDF documents signed with a certificate issued by Secure Soft, you must install the FDF file and the signature will be considered validated.

Add the certificate manually to the Adobe Trusted Identities

- Open the signed document
- Click on the signature rectangle (or go to the *Signatures* tab)
- Click on the *Signature Properties* button
- Go to the *Signer* tab (or *Date/time* tab for time stamping)
- Click on the *Show Certificate* button

- Select the Root certificate (or the signing certificate)
- Go to the *Trust* tab
- Click on the *Add to Trusted Identities*
- Check all the checkboxes

After you follow this procedure, all the documents signed by this certificate are recognized as trusted.

Windows Integration

If your certificate Root Key is imported on Microsoft Store (Start-Run-certmgr.msc - Trusted Root CA), start Adobe - Edit - Preferences - Security - Advanced Preferences - Windows Integration - check all checkboxes and all your documents will be considered validated.