Validating Digital Signatures in Adobe

Table of Contents
Validating Digital Signatures in Adobe.............................................................................................................1
  1. Add the Root Certificate on Adobe Trusted Identities.................................................................3
  2. Validate the Signature using Windows Integration.....................................................................8
  3. Export/Import the FDF (Acrobat Forms Data Format).................................................................12
  4. Validate Adobe Timestamps........................................................................................................18
  5. Other Validation Settings.................................................................................................................23

Usually, the digital certificates are issued by a Root CA (Certification Authority).

If the Root CA that issued the signing certificate is not included in Adobe Trusted Identities, the digital
signature is considered "not trusted" (but NOT invalid) when the document is opened in Adobe Reader
(see example below).

This behavior has nothing to do with the signing engine (e.g. PDF Signer, Adobe Reader) but with
the Adobe certificate validation procedure.

The user can validate the signature if the Root CA is already installed on Microsoft Certificate Store
(see the section Validate the Signature using Windows Integration).

As an alternative, the recipient must manually add the Root Certificate of the signing certificate on
Adobe Trusted Identities because only a few Root CA's are considered trusted by default by the Adobe
certificate validation engine (See this article: http://www.adobe.com/security/partners_cds.html).

The digital signature in not trusted
The digital signature is not trusted.
1. Add the Root Certificate on Adobe Trusted Identities

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 Trusted Identities.

Because the Root CA of the signing certificate is not included on Adobe Trusted Identities, the signature is considered “not trusted” (but NOT invalid).
To manually add the Root Certificate on the Adobe Trusted Identities, open the signature properties and click Show Certificate and select Trust tab.

Be sure that you have selected the topmost Root Certificate.

*Trust a CA certificate*
Press *Add to Trusted Identities tab* and be sure you have checked all checkboxes, as below.

![Certificate Details]

**Certificate Details**

**Subject:** Test CA  
**Issuer:** Test CA  
**Usage:** Sign certificate (CA), Sign CRL

**Expiration:** 12/2/2019 10:39:52 AM

**Trust**

A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.

- [x] Use this certificate as a trusted root

If signature validation succeeds, trust this certificate for:

- [x] Signed documents or data
- [x] Certified documents
  - [x] Dynamic content
  - [x] Embedded high privilege JavaScript
- [ ] Privileged system operations (networking, printing, file access, etc.)

*Trust a CA certificate*
After all dialog boxes are closed and the document is re-opened, the signature is considered Valid.

Valid digital signature
The Root Certificate is now Trusted and all signatures generated with this Root Certificate will be also Trusted.

Trusted Root Certificate
2. Validate the Signature using Windows Integration

You can use this method if your digital certificate is issued by a Root CA already installed on Microsoft Certificate Store. Microsoft and Adobe use different Certificate Stores and different certificate validation procedures.

To see if your Root CA is installed on Microsoft Certificate Store, go to Start – Run – certmgr.msc
You can also import your Root Certificate here.
After you check that your Root Certificate is installed, in Adobe Reader go to Edit menu – Preferences option – Security tab – click on Advanced Preferences button – Windows Integration tab and check all checkboxes.
When the document is re-opened, the digital signature is considered valid.
3. Export/Import the FDF (Acrobat Forms Data Format)

In order to avoid to manually add the Root Certificate on every client machine, the Root Certificate can be exported as Adobe FDF file. Once the file is exported, it can be installed on every machine where the digital signatures must be verified.

The FDF file can be exported from the Digital signature properties – Certificate section. Be sure the Root Certificate is selected and not the signing certificate.
On the next window select Acrobat FDF data Exchange, as below:
Save the FDF file.
The signature before importing the FDF file is considered “not trusted”, like below:

To install the FDF file on the computer where the signature must be validated, open the FDF file, press *Set Contact Trust button* and check all checkboxes, as below:
Import the FDF file.
After the FDF file is imported, the signature is considered Trusted.
4. Validate Adobe Timestamps

An Adobe Timestamp is in fact a subsequent signature added to the PDF signature so to validate an Adobe Timestamp simply follow the instructions from the section above.

Signature Properties

- Signed by: Test Certificate <email@email.com>
- Signing Time: 2014/12/02 12:51:18 +02'00'

Validity Summary
- The Document has not been modified since this signature was applied.
- The document is signed by the current user.
- The signature includes an embedded timestamp but it could not be verified.

Signature was created using Adobe Acrobat.
Signature was validated as of the signing time:
2014/12/02 12:51:18 +02'00'

Timestamp is not trusted
Go to Date/Time Tab and display the Timestamp Authority certificate.

Timestamp embedded in the signature

Timestamps are signed just as documents are signed. For a timestamp signature to be valid you must have trusted the Timestamp Authority that signed the timestamp. Click Show Certificate to view details regarding verification of the timestamp signature.

Timestamp Authority: Secure Soft TSA

Timestamps are created with specific policies that are defined by the Timestamp Authority. Amongst other things, a policy can indicate how reliable the time source is. There is no policy identified for this timestamp, or the policy could not be determined because the timestamp was not processed. To understand timestamp policies, you must contact the Timestamp Authority.
Press Add to Trusted Identities button

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

- Show all certification paths found

This certificate is not trusted.

- Sign documents or data
- Certify documents
- Execute dynamic content that is embedded in a certified document
- Execute high privilege JavaScripts that are embedded in a certified document
- Perform privileged system operations (networking, printing, file access, etc.)

Add to Trusted Identities...

The selected certificate path is valid.

The path validation checks were done as of the current time:
2014/12/02 12:51:22 +02'00'
Be sure you have checked all checkboxes, as below.

A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.

- Use this certificate as a trusted root

If signature validation succeeds, trust this certificate for:

- Signed documents or data
- Certified documents
  - Dynamic content
  - Embedded high privilege JavaScript
  - Privileged system operations (networking, printing, file access, etc.)
After all dialog boxes are closed and the document is re-opened, the timestamp is considered Valid.
5. Other Validation Settings

In some cases, the digital signature cannot be correctly validated because of some reasons like:
- Internet Connection is not available
- Proxy Settings cannot be set on Adobe
- CRL/OCSP revocation information cannot be downloaded or are not available.

On this case, even if the digital signature is trusted and valid, Adobe will consider this signature “not trusted” because the revocation information cannot be obtained.

This section can be applied when you will get one of the following messages:

*OCSP revocation server is not available*
CRL revocation list is not available.
The digital signature is considered not trusted even if the signature is not altered.
To avoid this behavior, Adobe must be configured to bypass this additional revocation checking.

Go to *Edit menu – Preferences option – Security tab – click on Advanced Preferences button – Verification tab* and set the interface as below:
After this settings was saved, the document is considered valid by Adobe.