Validating Digital Signatures in Adobe

Table of Contents

Validating Digital Signatures in Adobe	1
1. Certificates Recognized "Trusted by default" in Adobe	3
2. Add the Root Certificate on Adobe Trusted Identities	4
3. Validate the Signature using Windows Integration	9
4. Export/Import the FDF (Acrobat Forms Data Format)	
5. Validate Adobe Timestamps	
6. Other Validation Settings.	24

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 recipient must manually add the Root Certificate of the signing certificate on Adobe Trusted Identities because not all Root CA's are considered trusted by default by the Adobe certificate validation engine (See this article: <u>https://helpx.adobe.com/acrobat/kb/trust-services.html</u>).



Signature Properties	×
Signature validity is UNKNOWN.	
Summary Document Signer Date/Time Legal	
Signed by: Test Certificate < email@email.com> Show Certificate	
Reason:	
Signing Time: 2014/12/02 12:43:04 + 02'00'	
Validity Summary	
The Document has not been modified since this signature was applied.	
 The signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities. Signing time is from the clock on the signer's computer. 	
Signature was created using Adobe Acrobat. Signature was validated as of the current time: 2014/12/02 13:12:13 +02'00'	
Validate Signature Close	

The digital signature is not trusted

1. Certificates Recognized "Trusted by default" in Adobe

Adobe European Union Trust List (EUTL)

If the digital certificate is issued by an eIDAS accredited Certification Authority, the signature will appear as valid in Adobe by default.

An eIDAS certificate can be obtained from one of these Service Providers: https://webgate.ec.europa.eu/tl-browser/#/



Adobe Authorized Trust List (AATL)

The Adobe Approved Trust List (AATL) is the largest Trust Service for electronic documents in the world.

Service Providers: <u>https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html</u>

Adobe Certified Document Services (CDS)

Certified Document Services (CDS) is a Trust Service enabled by the Adobe Root Certificate Authority.

Service Providers: https://helpx.adobe.com/acrobat/kb/certified-document-services.html

2. 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).

🔁 File I	dit View Window Help	est document[sig
J	🔁 🗃 🖨 🖂 💿 💿 1 / 1 🗩 🗣 127% ▾ 🔚 🚱 🤛 🌠	
li	At least one signature has problems.	
	Signatures	
I)	Image: Walidate All Validate All Image: Walidate Structure validity is unknown: test/	1
-6-	Document has not been modified since this signature was applied Signer's identity is unknown because it has not been included in your li Signing time is from the clock on the signer's computer.	ficate
	 	×
	Signature validity is UNKNOWN. Summary Document Signer Date/Time Legal Image: Signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities.	
	Signed by: Test Certificate < email@email.com> Show Certificate Image: Click Show Certificate for more information about the signer's certificate and its validity details, or to change the trust settings for the certificate or an issuer certificate. Validity Details	
	 The signer's certificate has not been issued by a certificate authority that you have trusted. The path from the signer's certificate to an issuer's certificate was successfully built. Revocation checking was not performed. 	
	Signer's Contact Information: email@email.com	

Signature is not trusted

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.

Test CA Test Certificate < ema Select the Root CA	Summary Details Revocation Trust Policies Legal Notice This certificate is not trusted. Trust Settings Trust Settings X Sign documents or data X Certify documents X Certify documents X Execute dynamic content that is embedded in a certified document X Execute high privilege JavaScripts that are embedded in a certified document X X Perform privileged system operations (networking, printing, file access, etc.) Add to Trusted Identities
The selected certificate p	ath is valid.
The path validation chec	ks were done as of the signing time:
2014/12/02 12:43:04 +02'	00'
Validation Model: Shell	OK

Trust a CA certificate

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

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.
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.)
Help OK Cancel

Trust a CA certificate

After all dialog boxes are closed and the document is re-opened, the signature is considered Valid.

🛃 File	Edit View Window Heln			test document[signed].pdf - Adobe F
P	🔁 🗗 🖨 🥁 🛛 🕄 🗊 🖊 1		• 📑 🔛 🖻 🦻 🎾	
la	Signed and all signatures are valid.			
	Signatures		•	
D	8= -	Validate A	и	
49	 Rev. 1: Signed by Test Certificate <email@emails< li=""> Signature is valid: Document has not been modified since this Signed by the current user Signing time is from the clock on the signer Bignature Details </email@emails<>	il.com> signature was applied 's computer.	^{test} Signatur Test Cer	e valid tificate
	Last Checked: 2014.12.02 12:50:04 +02'00'		Signature Properti	es
	<u>Click to view this version</u>	Signature is N Summary Docum Signed by: Reason: Signing Time: Validity Summ Walidity Summ	VALID, signed by Test Certificate <email@ eent Signer Date/Time Legal Test Certificate <email@email.com> 2014/12/02 12:43:04 + 02'00' hary bocument has not been modified since this</email@email.com></email@ 	Demail.com>. Show Certificate Location: signature was applied.
		The do	ocument is signed by the current user. g time is from the clock on the signer's co	mputer.
77.10				

Valid digital signature

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

Add to Trusted Identities

Trusted Root Certificate

3. 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



🚡 certmgr - [Certificates - Cu	rrent User\Trusted Root Certific	ation Authorities 🗕 🗖 ⋗	<
<u>File Action View H</u> elp			
🗢 🔿 🖄 🖬 🖌 🖬	1 📑 👔 🖬		
Certificates - Current User Personal	Issued To	Issued By	^
Trusted Root Certification Au	StartCom Certification Authority	Starfield Services Root Certificate StartCom Certification Authority	
Enterprise Trust	StartCom Certification Authorit	StartCom Certification Authority G2	
Intermediate Certification Au	Test CA	Test CA Test Root Certificate	
Active Directory User Object Trusted Publishers	Thawte Premium Server CA	Thawte Premium Server CA	
Untrusted Certificates	Thawte Premium Server CA	Thawte Premium Server CA	
Third-Party Root Certification Trusted People	Thawte Timestamping CA	Thawte Timestamping CA	
Client Authentication Issuers	UTN - DATACorp SGC	UTN - DATACorp SGC	
Other People MSIEHistory/ournal	UTN-USERFirst-Hardware	UTN-USERFirst-Hardware	
Certificate Enrollment Reques	VeriSign Class 3 Public Primary	VeriSign Class 3 Public Primary Ce	
Smart Card Trusted Roots	VeriSign Trust Network	VeriSign Trust Network	
	VeriSign Trust Network	VeriSign Trust Network	~
Trusted Root Certification Authorities	store contains 67 certificates.	>	-

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.

	Preferences	
Categories:	Digital Signatures	
Commenting Documents Full Screen	 Verify signatures when the document is opened View documents in preview document mode when signing 	Advanced Preferences
General Page Display	Digital Sign	natures Advanced Preferences
3D & Multimedia Accessibility Forms Identity International Internet JavaScript Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing Search Security	Verification Creation Windows Integration Image: Creative of the searching the Windows Certificate Store for certificates Trust ALL root certificates in the Windows Certificate Store for the operations: Image: Creative of Validating Signatures Image: Validating Certified Documents Image: Creative of the searching the Windows may be treated as trusted content enabling this feature.	s other than yours e following npanies that have certificates 2. Care should be taken in

When the document is re-opened, the digital signature is considered valid.



Valid Signature

4. 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.

	Certifi	icate Viewer					×
This dialog allows you to view t the selected entry.	he details of a certific	cate and its ent	tire issua	ince chai	n. The details	correspond to	•
Show all certification paths fo	und						
E Test CA Test Certificate <ema< th=""><th>Summary Details</th><th>Revocation T</th><th>rust P</th><th>Policies</th><th>Legal Notice</th><th></th><th></th></ema<>	Summary Details	Revocation T	rust P	Policies	Legal Notice		
	ē	Test CA Organization					
	Issued by:	Test CA					
		Organization					
	Valid from:	2014/12/02 12	2:39:52 +0	02'00'			
	Valid to:	2019/12/02 12	2:39:52 +0	02'00'			
	Intended usage:	Sign CRL, Sig	n certific	ate (CA)			
< >			E <u>x</u> port)		
The selected certificate participation of the path validation check 2014/12/02 14:17:55 + 02'0 Validation Model: Shell	ath is valid. <s as="" done="" of="" the<br="" were="">10'</s>	current time:					
						ОК	

The FDF file can be exported from the D*igital 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:

	Data Exchange File - Exporting Certificate
 Steps Choose Export Options Identity Sign Data Exchange File Choose a Path to Save File Review and Complete 	You have chosen to export the following data: Selected address book entries To open the exported data, you need Adobe Acc Reader 6.0, or later versions. Destination © Email the exported data © Save the exported data to a file © Acrobat FDF Data Exchange © Certificate Message Syntax - PKCS#7 © Certificate File

Save the FDF file.

	Data Exchange File - Exporting Certificate
Steps Choose Export Options Identity Sign Data Exchange File Choose a Path to Save File Review and Complete	Please review the options you have specified below. Once reviewed, click Finish to export the data. You have chosen to export the following data: o=Organization, cn=Test CA
	You have chosen these options for export: The name and email included in the exported data are: You have chosen to save the exported data to this path: d:\RootFDF.fdf To open the exported data, you need Adobe Acrobat 6.0 Professional or Standard, Adobe Reader 6.0, or later versions.
	Cancel < <u>B</u> ack <u>Einish</u>

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:

Data Exchange File - Import Contact	
You have opened an Acrobat FDF Data Exchange File containing the following data: Contact Information	
Sender Name: Test CA Email Address:	
Add Certificate to List of Trusted Identities This file contains Contact information for the sender. Click Set Contact Trust to set options on how to include this Contact in your list of trusted identities. Contact information includes certificates that, once trusted, can be used to validate signatures from and encrypt documents for the associated Contact. Set Contact <u>T</u> rust	
<u>C</u> lose]

Import the FDF file.

Import Contact Settings	×
Certificate Details	
Subject: Test CA	
Issuer: Test CA	
Usage: Sign certificate (CA), Sign CRL	
Expiration: 12/2/2019 10:39:52 AM	
Trust Policy Restrictions	
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.	
✓ Signed documents or data	
Cer <u>t</u> ified documents	
✓ <u>D</u> ynamic content	
Embedded high privilege JavaScript	
<u>Privileged system operations (networking, printing, file access, etc.)</u>	
Certificate Details Help OK Cancel	

After the FDF file is imported, the signature is considered Trusted.

	Import Complete
Import detai	is:
1 issuer cer	tificate(s) imported.
	Or
	UK



5. 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	×
Signature is VALID, signed by Test Certificate <email@email.com>.</email@email.com>	
Summary Document Signer Date/Time Legal	
Signed by: Test Certificate < email@email.com> Show Certificate	
Reason:	
Signing Time: 2014/12/02 12:51:18 + 02'00' Location:	
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'	
<u>V</u> alidate Signature <u>C</u> lose	

Timestamp in not trusted

Go to Date/Time Tab and display the Timestamp Authority certificate.

Signature Properties	×
Signature is VALID, signed by Test Certificate <email@email.com>.</email@email.com>	
Summary Document Signer Date/Time Legal	
Signing Time: 2014/12/02 12:51:18 +02'00'	-
The signature includes an embedded timestamp but it could not be verified.	
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 Show Certificate	
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.	
Validate Signature Close	

Press Add to Trusted Identities button

	Certificate Viewer
his dialog allows you to vie he selected entry.	w the details of a certificate and its entire issuance chain. The details correspond to
Secure Soft TSA	Summary Details Revocation Trust Policies Legal Notice This certificate is not trusted. Trust Settings Image: Sign documents or data Image: Sign documents or data Image: Sign documents or data Image: Certify documents Image: Secure dynamic content that is embedded in a certified document Image: Execute high privilege JavaScripts that are embedded in a certified document Image: Secure high privilege JavaScripts that are embedded in a certified document Image: Perform privileged system operations (networking, printing, file access, etc.) Image: Add to Trusted Identities

Be sure you have checked all checkboxes, as below.

	Import Contact Settings	
Certificate Details		
Subject: Secure Soft T	A	
Issuer: Secure Soft Priv	ate CA	
Usage: Sign transactio	n, Sign document	
Expiration: 7/30/2023	1:32:59 AM	
Trust		
A certificate used to chain up to a trust checking is not per	o sign a document must either be designated as a trust anchor or enchor in order for signature validation to succeed. Revocation formed on or above a trust anchor.	
Use this certification	te as a trusted <u>r</u> oot	
lf signature validati	on succeeds, trust this certificate for:	
Signed docu	ments or data	
✓ Certified do	uments	
	2ynamic content	
✓	mbedded high privilege JavaScript	
	Privileged system operations (networking, printing, file access, etc.)	
Help	OK Cancel	_

After all dialog boxes are closed and the document is re-opened, the timestamp is considered Valid.

		Date/Time l	.egal		
<u>S</u> igned by:	Test Certifica	ate <email@em< td=""><td>ail.com></td><td></td><td>Show Certificate</td></email@em<>	ail.com>		Show Certificate
<u>R</u> eason:					
igning Time:	2014/12/02 1	2:51:18 +02'00'		Location:	
Validity Sum	mary				
🚭 The 🛙	ocument has i	not been modif	ied since this	signature was	applied.
🚭 The d	locument is sig	ned by the cur	rent user.		
all and a					
-		en e		the second second second	
The s 2014/	ignature incluc 12/02 12:51:12	les an embedde +02'00'	ed timestamp	. Timestamp t	time:
The s 2014/	ignature incluc 12/02 12:51:12	les an embeddo +02'00'	ed timestamp	. Timestamp t	time:
Ines 2014/	ignature incluc 12/02 12:51:12	les an embeddo +02'00'	ed timestamp	. Timestamp t	time:
Grature was	ignature incluc 12/02 12:51:12 created using A	les an embeddo +02'00' Adobe Acrobat.	ed timestamp	. Timestamp t	time:
gnature was gnature was 14/12/02 12:	ignature includ 12/02 12:51:12 created using A validated as of 51:12 +02'00'	les an embedde +02'00' Adobe Acrobat. the secure (tim	ed timestamp estamp) time	. Timestamp t	time:
gnature was gnature was 014/12/02 12:	ignature includ 12/02 12:51:12 created using A validated as of 51:12 +02'00'	les an embedde +02'00' Adobe Acrobat. the secure (tim	ed timestamp estamp) time	. Timestamp t	time:
Gignature was ignature was 014/12/02 12:	ignature includ 12/02 12:51:12 created using A validated as of 51:12 +02'00'	les an embedde +02'00' Adobe Acrobat. the secure (tim	ed timestamp estamp) time	. Timestamp t	time:
gnature was gnature was 014/12/02 12:	ignature includ 12/02 12:51:12 created using A validated as of 51:12 +02'00'	les an embedde +02'00' Adobe Acrobat. the secure (tim	ed timestamp estamp) time	. Timestamp t	time:

6. 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:

Contacting http://ocsp.safescrypt.com for OCSP based revocation checkin press ESC to cancel
Cancel

OCSP revocation server is not available

CRL revocation list is not available.

his dialog allows you to view the dene selected entry. Multiple issuance sust anchor.	etails of a certificate and its entire issuance chain. The details corrected chains are being displayed because none of the chains were issued mmary Details Revocation Trust Policies Legal Notice Problem determining whether the selected certificate is valid Details An attempt was made to determine whether the certificate is valid by checking whether it appeared in any Certificate Revocation Lists (CRLs). Click Problems to view the problems that were encountered while performing this revocation check. Signer Details Problems encountered Check revocation Error Information
	Revocation Lists (CRLs). Click Problems to view the problems that were encountered while performing this revocation check. Signer Details Problems encountered Check revocation Error Information
	Error Information
Chain View Text V Chain View Text V CRL parsing CRL pa	View g error: Error encountered while BER decoding: rsing error: Error encountered while BER decoding: g error: Error encountered while BER decoding: g error: Error encountered while BER decoding: rsing error: Error encountered while BER decoding:
<	2

The digital signature is considered not trusted even if the signature is not altered.

File E	Edit View Window Help
	🔁 🔐 📇 🖨 🖂 💿 💽 1 / 1 🗩 🗭 123% 🗸 🔚 🔛 🦻 🦻
-	The validity of the document certification is UNKNOWN. The author could not be verified.
	Signatures 🔹
Q	8∃ ▼ Validate All
	Certified by
15g	No changes are allowed
L	Signature validity is unknown:
	Document has not been modified since it was certified
	Signature is valid, but revocation of the signer's identity could not be c
	T Signature Details
	Last Checked: 2014.12.02.13:03:59 + 02'00'
	Field: Signature1 on page 1
	Signature Properties
	Signatare rioperaes
	Document was certified, validity is UNKNOWN. Summary Document Signer Date/Time Legal
	Signed by: Show Certificate
	Reason: I am approving this document
	Signing Time: 2014/12/01 09:31:44 + 02'00' Location:
	Validity Summary
	The Document has not been modified since it was certified.
	The signer's identity was valid when it was issued, but no revocation checks could be made to validate the identity at this time.
	A Signing time is from the clock on the signer's computer.
	Signature was created using Adobe Acrobat. Signature was validated as of the current time: 2014/12/02 13:03:47 +02'00'

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:

	Preferences				
Categories:					
Commenting	Digital Signatures Verify signatures when the document is opened Advance	ed Preferences			
Full Screen	Vie <u>w</u> documents in preview document mode when signing				
General Page Display	Digital Signatures Advanced Preferences				
3D & Multimedia Accessibility	Verification Creation Windows Integration				
Forms dentity	When Verifying:				
nternational	• Use the document-specified method. Prompt if it is not available.				
nternet	O Use the document-specified method. Use the default method if it is not available.				
Measuring (2D)	Always use the default method (overrides the document-specified method).				
Measuring (3D) Measuring (Geo)	Default Method for Verifying Signatures: Adobe Default Security				
Multimedia (legacy) Multimedia Trust (legacy)	Require certificate revocation checking to succeed whenever possible during signature verification	_			
Online Services	Ignore document validation information	- C			
Reading	Verification Time				
Search	Verify Signatures Using:				
Security Security (Enhanced)	The current time				
Spelling	Secure time (e.g. timestamp) embedded in the signature if available, current time otherwise				
Tracker	O The time at which the signature was created				
Trust Manager Units	Use expired timestamps				

After this settings was saved, the document is considered valid by Adobe.

🔁 File Edit View Window Help						
J	🔁 🖻 🗎 🖨 🛛		/1) 123% 💌		9 🦻
9	Certified by			1	, certificate	issued by SafeScry
	Signatures			٩		
Q	8=-			Validate All		
	🗆 🤶 Certified by					
42	No changes are allowed					
	Valid certified Document:					
	Document has not been modified since it was certified					
	Signature is valid, but revocation of the signer's identity could not be c					
	Signing time is from the clock on the signer's computer.					
	El Signature Details					
	Last Checked: 2014.12.02 13:02:27 +02'00'					
	Field: Signature I on page I					
	Signature Properties					
	Summary Docur	nent Signer Date/T	ïme Legal			
	Signed by:				Show Certificat	e
	Reason: I am approving this document					
	Signing Time:	2014/12/01 09:31:44 -	+ 02'00'	Location:		
	Validity Summary					
	R The Document has not been modified since it was certified.					
	The signer's identity was valid when it was issued, but no revocation checks could be made to validate the identity at this time.					id
	Signature was created using Adobe Acrobat. Signature was validated as of the current time: 2014/12/02 13:02:14 + 02'00'					