

## How-To Guide

## Use of Certificates in Adobe Acrobat with Captured Handwritten Signatures

(Windows)

Copyright © 2021 Topaz Systems Inc. All rights reserved.

For Topaz Systems, Inc. trademarks and patents, visit <u>www.topazsystems.com/legal</u>.



## **Overview**

PDF documents signed using Topaz signature pads and software can be viewed with Adobe Acrobat or Reader. To accomplish this, Topaz software uses a certificate which Adobe refers to as a "signature", but this certificate-based digital signature is not the person's handwritten signature, and is only incidental to the Topaz handwritten signature capture process. The key to decoding the meaning of this certificate status in Acrobat under various conditions is provided below:



A red "X" means the certificate is no longer valid. This can be due to a certificate having expired or been revoked by the certificate trust authorities.

	CI2	٦٢		$\sim$	
<u>ℓ</u> <sup>4</sup>	t least of yped into	ne signa o this fo	iture has rm.	problem	ns.
ß	Sign	atures			

A yellow "!" or "Unknown" message means software and settings to check the validity of the certificate are not currently installed on the computer.



A green tick or "Valid" message means the certificate used in the process is current and the software and settings used to provide this function have been installed and configured.

To provide the option of certificate-only signing without a signature pad in some settings, Adobe Acrobat and Reader have their own certificate trust stores. Additionally, various browser vendors and Microsoft have created lists of trusted identities (CA root certificates), which are already, or can be installed on your Windows PC.

To add the certificates built into Windows, users of Adobe products can include root certificates from the Windows Certificate Store. This option, called "Windows integration", allows Adobe Acrobat and Reader to use certificates in the Trusted Windows Certificate Store when validating the certificate trust chain.

In addition to checking the status of certificates, Adobe software can report whether or not a document has been altered after a signature has been captured. This function is independent of the current status of the certificate validity.



## Adobe Certificate Trust Guide in Windows

End users can configure Adobe Acrobat and Reader for Windows integration through the application's **Preference** panel.

Digital Signatures Creation & Appearance	Signature Verification Preferences		×
Digital Signatures Creation & Appearance	Verify signatures when the document is opened		
Creation & Appearance	verify signatures when the document is opened		
	When document has valid but untrusted signatures of	rompt to review and trust signers	
Control options for signature creation     Set the appearance of signatures within a document	Verification Behavior When Verifying: Ouse the document-specified method; prompt if unavailable Ouse the document-specified method; if unavailable, use default method Outputs the default method; document-specified method; security		
Verification  • Control how and when signatures are verified			
Identities & Trusted Certificates <ul> <li>Create and manage identities for signing</li> </ul>	Require certificate revocation checking to succeed     Use expired timestamps     Ignore document validation information	I whenever possible during signature verification	
Manage credentials used to trust documents Document Timestamping     Configure timestamp server settings	Verification Time Verify Signatures Using:	Verification Information Automatically add verification information when saving signed PDF:	
	Current time	O Never	
	Trugt Het foot certificates in the Windows Certificate Validating Signatures Validating Certified Documents Selecting either of these options may result in ar Take care before enabling these features.	Store for: bitrary material being treated as trusted content.	
	Help	OK Cancel	]
	Verification  • Control how and when signatures are verified  Identities & Trusted Certificates  • Create and manage identities for signing • Manage credentials used to trust documents  Document Timestamping • Configure timestamp server settings	Verification       © Ore the document-specified method; if unavailable         • Control how and when signatures are verified       © Use the document-specified method; if unavailable         Identities & Trusted Certificates       • Cheate and manage identities for signing         • Cheate and manage identities for signing       • Manage credentials used to trust documents         Document Timestamping       • Configure timestamp server settings         • Configure timestamp server settings       • Time at which the signature was created         • Secure time (timestamp) embedded       • Current time         Windows Integration       Trust et root certificates in the Windows Certificate         • Validating Signatures       • Validating Certified Documents         • Validating Certified Documents       • Help	Verification         • Control how and when signatures are verified         Identities & Trusted Certificates         • Create and manage identities for signing         • Manage credentials used to trust documents         Document Timestamping         • Configure timestamp server settings         • Configure timestamp server settings         • Current time         • Mindows Integration         • Validating Signatures         • Validatin

**NOTE:** When changing Preference options in Adobe products, always close and reopen the application for the changes to take effect.