Adobe PDF Security—Understanding and Using Security Features with Adobe Reader and Adobe Acrobat

TABLE OF CONTENTS

Why is electronic document security important?

Most people view paper as inherently trustworthy. Bank statements, correspondence, and contracts arrive on corporate letterhead inside corporate envelopes. Loan documents have original signatures.

Every day, however, more businesses are distributing electronic versions of these documents—and asking customers to accept and act upon them with the same confidence that they bring to paper.

Relying on electronic documents instead of paper can speed up processes, improve the distribution of information, and lower costs for both customers and business. Unfortunately, computer-savvy cyber-criminals also use electronic documents as tools for fraud. They attempt to forge press releases, alter stock reports, and use "phishing" scams to dupe people into disclosing personal information in order to steal their identities. These types of crimes have some people wary of trusting and using electronic documents.

Enhancing security by using Adobe PDF documents

If you receive electronic documents, you need assurance that a document you download or receive is genuine and unaltered. If your organization creates electronic documents, you need ways to protect the confidentiality of the information, as well as ways to protect the documents from unauthorized modification or use.

Fortunately, these tasks are easier when the document is in Adobe® Portable Document Format (PDF). Adobe PDF enables a more secure, reliable electronic document distribution and exchange. By saving documents in PDF, organizations can preserve the look and design integrity of their original documents while also enabling recipients to use Adobe Acrobat® or the free Adobe Reader® software to view and work with them.

Both Adobe Reader and Acrobat have numerous features that can help you, as a recipient, decide for yourself whether a specific PDF document is genuine and which features (such as printing or copying) have been restricted by the document's author. The applications also enable you to digitally sign PDF documents, such as forms that you might receive from a business or government agency.

If you create PDF documents, you can use additional Acrobat features to help protect documents from unauthorized access, modification, and use. Acrobat enables you to apply digital signatures to help provide assurance to users that the PDF document is genuine and unmodified. As the author, you can also manage and audit how your PDF documents are used.

The next two sections of this guide discuss the security features of Adobe Reader 7.0 and Acrobat 7.0 in more detail and are primarily for those who receive PDF documents. The last section describes the security features of Acrobat that authors can use to help secure their documents and provide a greater assurance to recipients that a document is the genuine article.

Terms that are *italic* on their first occurrence are defined in the glossary at the end of the guide.

Don't be caught by a phisher!
In phishing scams, criminals send e-mail messages that appear to be from legitimate sources, such as financial institutions and government agencies, to trick consumers into divulging sensitive personal information. They then use that information to open credit card accounts, take out loans, and perform other forms of identity theft.

To help protect yourself from identity theft, find out more about phishing and current phishing scams from the Anti-Phishing Working Group, www.antiphishing.org.

Adobe

How do I decide whether to trust a specific Adobe PDF document?

Say you've just received an Adobe PDF form via e-mail that appears to be from your bank or credit card company, and the form is requesting that you update your contact information on an account. To trust this document enough to enter your information and return the form, you'd want to know:

> *Is this document really from my bank or credit card company? Or is it a forgery from a thief who wants to steal my personal information and identity?*

One of the best ways to help assure yourself that a PDF document is genuine is to check whether the *digital signatures* (if any) within it are authentic. For simplicity, think of a digital signature as an electronic identification card that contains certain information about the person or entity that has digitally signed the PDF document. A PDF document can have two kinds of digital signatures:

- **A certification signature**, which can be applied by the document's author. Adobe Reader or Acrobat automatically checks the authenticity of this signature when you open the document, and then displays a window that indicates whether the signature is valid (that is, authentic and current). This guide also refers to the certification signature as the "author's digital signature."
- **A standard signature**, which can be applied by anyone who has permission to digitally sign the document. Adobe Reader or Acrobat can automatically check the authenticity of standard signatures when you open the document, or you can check them manually from within the application.

Note: *Adobe Reader or Acrobat must have access to the Internet to check digital signatures.*

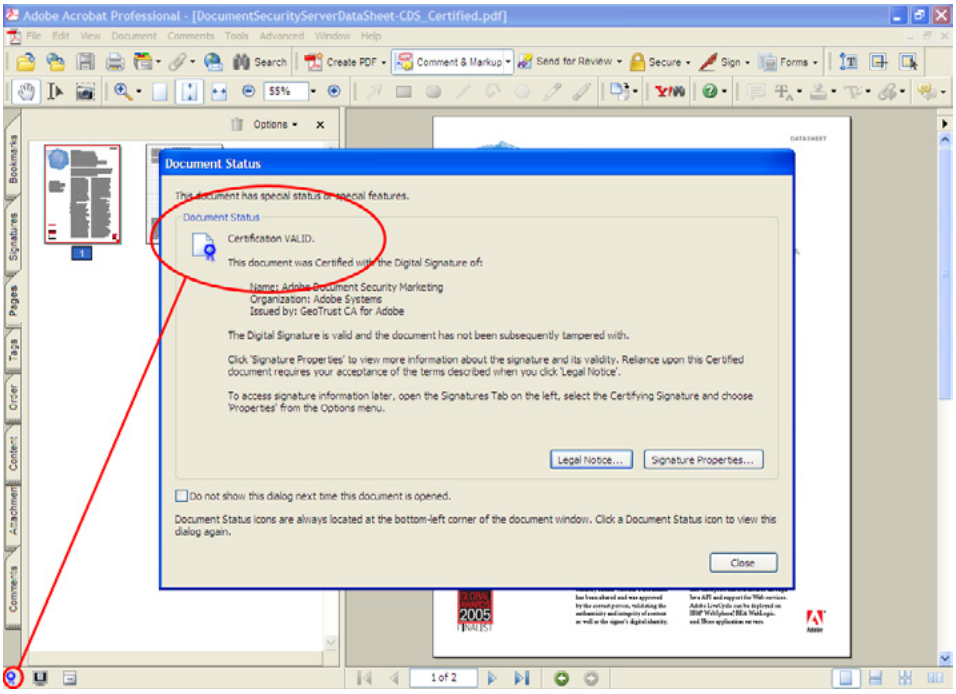
Checking the certification signature

Immediately after you open a *certified Adobe PDF document*, Adobe Reader or Acrobat automatically checks for unauthorized modifications to the document and checks the authenticity of the certification signature. The software then opens a Document Status window that shows one of three results, discussed in more detail below:

- **Certification Valid**, with a blue ribbon
- **Validation Of Author Not Confirmed**, with a blue question mark next to a person
- **Certification Invalid**, with a red X

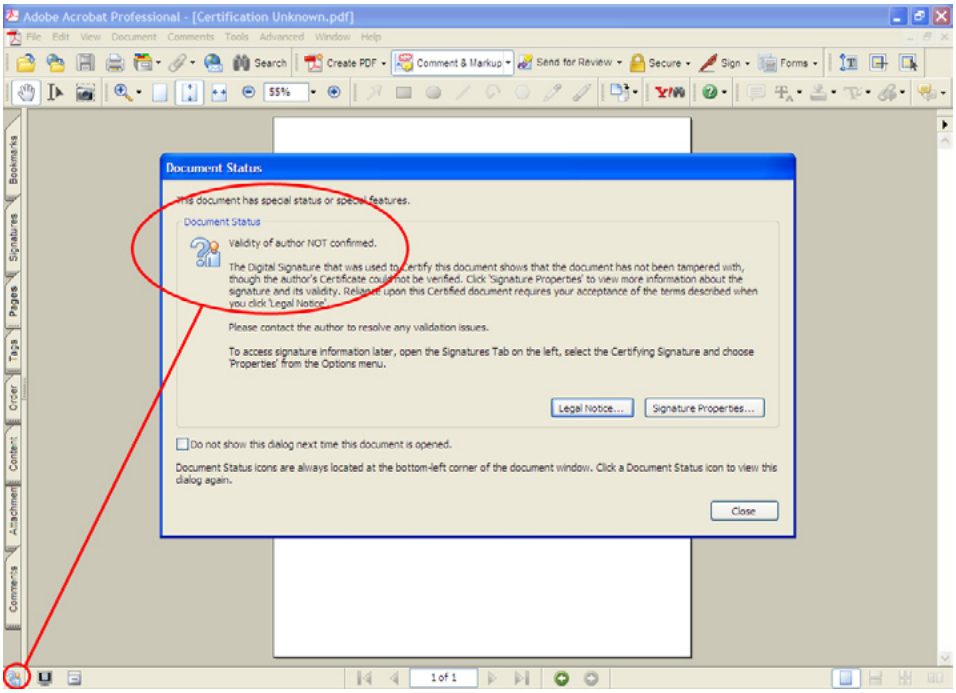
Certification Valid. A result of Valid and a blue ribbon in the lower left corner of the main window mean that the software has performed two primary tasks. First, it has connected to a server to check the signer's *Digital ID* and confirmed that the Digital ID is valid and current. Second, it has done a bit-for-bit comparison of the document as it was at the time of signing against the document as it was at the time of the validation check, and it has found these two versions to be identical. A result of Valid can provide strong assurance that the document has not been modified and that the document is genuine.

Note: *Each entity that issues a Digital ID has different requirements and processes for confirming that the information contained within the Digital ID is true and accurate. The level of trust associated with each Digital ID is often a reflection of these requirements and processes. Generally speaking, the stricter the requirements and the more involved the processes, the higher the level of trust than can be associated with the Digital ID. For more information about Digital IDs and trust, see "Establishing trust for unconfirmed digital signatures" later in this guide.*



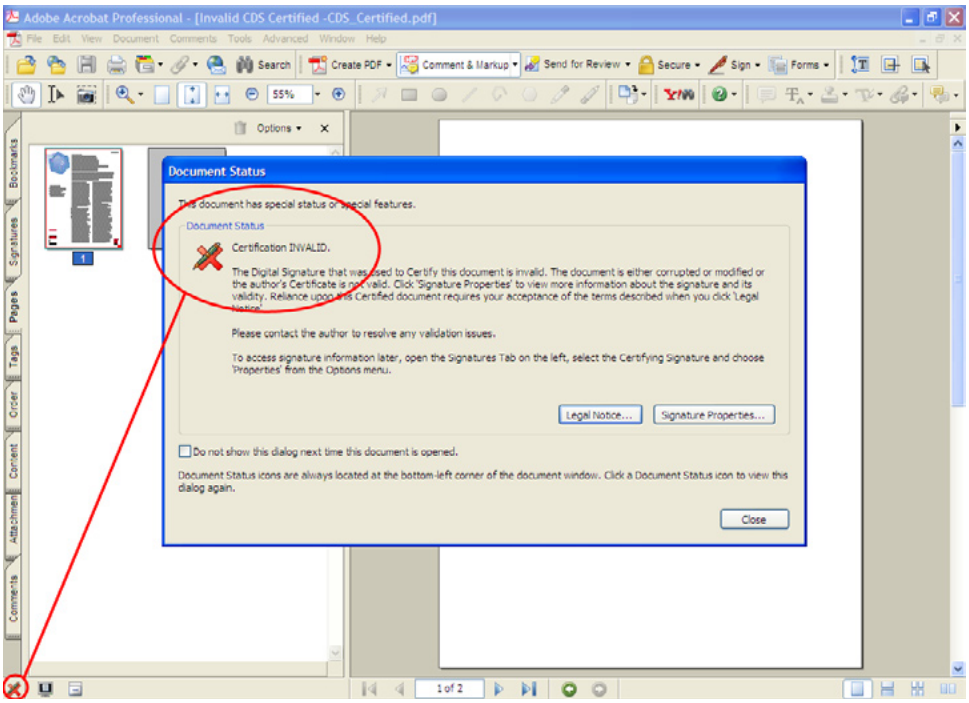
A status of Valid in the Document Status window of Adobe Reader or Acrobat helps provide assurance that the certified PDF document is authentic and unmodified. Always double-check that a blue ribbon also appears in the lower left corner of the main window.

Validity Of Author Not Confirmed. A result of Not Confirmed and a question mark next to the image of a person in the lower left corner of the main window mean that Adobe Reader or Acrobat could not verify the authenticity of the author's digital signature. Before relying on this signature, you should establish trust for the signature's Digital ID, as described in "Establishing trust for unconfirmed digital signatures" later in this guide.



A status of Validity Of Author Not Confirmed in the Document Status window of Adobe Reader or Acrobat indicates that the Digital ID of the signer of the certified PDF document is in question. A blue question mark next to the image of a person appears in the lower left corner of the main window.

Certification Invalid. A result of Invalid and a red X in the lower left corner of the main window indicate that the document has been altered in some way, or that the Digital ID that the author used to certify the document has expired or been canceled (revoked). A PDF document that has an Invalid certification status cannot be trusted and should not be used.



A status of Invalid in the Document Status window of Adobe Reader or Acrobat indicates that the certified PDF document has been modified or the certification signature is no longer current. A red X also appears in the lower left corner of the main window.

Checking the other signatures

Besides a certification signature, an Adobe PDF document may contain one or more standard signatures that others added before you received the document. You might, for instance, receive a PDF version of a mortgage document that has a digital signature from your loan officer. When you add your own digital signature to a document, you are adding a standard signature too.

Just as you do for a certification signature, you must decide whether to trust standard signatures by checking their authenticity. To do this, first make sure that you are connected to the Internet, so that Adobe Reader or Acrobat can check the digital signatures. Next, view the Signatures tab of the navigation pane (this shows all the signatures for a document). Then choose Options > Validate Signatures (on the Signatures tab) to have the software check the signatures.

Adobe Reader or Acrobat then displays one of several results for each entry in the Signatures tab. Typical results include:

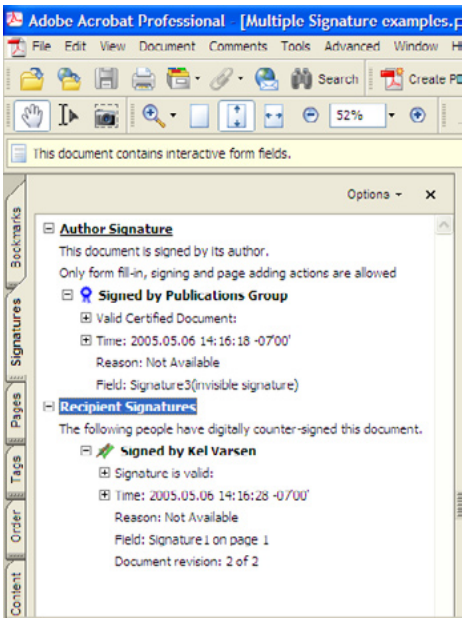
/alid signature | Unknown signature | Invalid signature | Valid signature, modified document

Some of the status icons that Adobe Reader or Acrobat may display when you validate signatures.

- **A green check mark (Valid)** indicates that the software has connected to a server to check the signer's Digital ID and found it to be valid and current.
- **A blue question mark next to a person (Signature Validity Is Unknown)** indicates that Adobe Reader or Acrobat can't validate the Digital ID that was used to sign the document. Before relying on this signature, you should establish trust for the signature's Digital ID, as described in "Establishing trust for unconfirmed digital signatures" later in this guide.
- **A red X (Invalid)** indicates that the Digital ID that was used to apply the digital signature is not valid because it has expired or been canceled (revoked).

Note: *The above icons may also include a yellow warning triangle as part of the mark. This triangle indicates that the document has been altered since that signature was applied. Adobe Reader or Acrobat provides several features for viewing and comparing signed versions, as well as for detecting modifications. See "Validating signatures" in Adobe Reader Help or Acrobat Help for more details.*

For each signature, Adobe Reader or Acrobat also displays when the document was signed and whether it was modified after any of the signers had last signed the document. These additional pieces of information can help you assess the trustworthiness of the document.

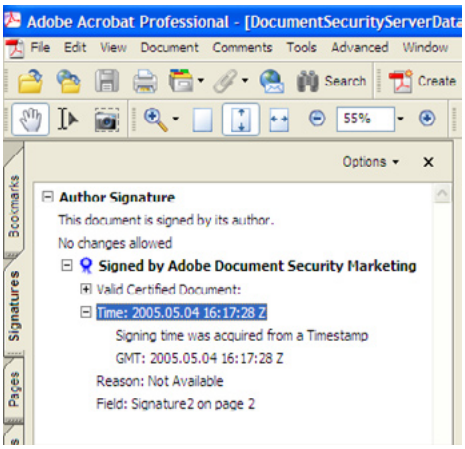


You can view all digital signatures in a PDF document in the Signatures tab of the navigation pane. The Options menu on the tab enables you to validate the signatures and to view the source of their underlying Digital IDs.

Checking when the document was signed

The time and date of a digital signature, called a *time stamp*, can be important when you are working with time-sensitive documents (such as contracts, real estate offers, loan applications, and payments). For example, the time stamp can indicate when offers or counteroffers were made, or whether a document was signed before a deadline.

In Adobe Reader or Acrobat, you can view the time stamps of signatures by opening the Signatures tab of the navigation pane, and then clicking the plus signs to expand the information for a particular signature.



To show more information about the signature (such as when a particular digital signature was applied), open the Signatures tab of the navigation pane, and then click the plus sign next to the signer's name.

Handling documents that aren't certified or signed

Some Adobe PDF documents you receive may not be certified or signed. These may include forms and applications, brochures, special offers, announcements of service changes, and so on. How do you know whether to trust these documents as authentic and unmodified?

In this case, consider how you obtained the document and whether you can trust its source. For instance:

- **Did you go to the organization's website yourself and download the document?** Then it's more likely to be authentic and unmodified.
- **Was the document e-mailed to you?** There's generally no reliable way to know whether this document is authentic without contacting the sender and asking them.
- **Did the document or its link come to you in an unsolicited fashion or from an unknown source?** Be wary—the document may lead you to bogus phone numbers and websites. When in doubt, use a known phone number or website to contact the business who supposedly provided the document, and ask their customer service department if the document is legitimate.

Establishing trust for unconfirmed digital signatures

Any time that Adobe Reader or Acrobat reports that a digital signature has a status of Validity Of Author Not Confirmed or Signature Validity Is Unknown, you must decide whether to establish trust for that signature. This task involves three basic steps:

1. Obtain a *certificate* for the digital signature from a known, trusted individual or website. If you are at work, request this certificate from your company's IT department. A certificate is an electronic counterpart to driver licenses, passports, membership cards, etc. Certificates are electronic files containing information about an individual or organization that is used to establish their digital identity.
2. Add the certificate in Adobe Reader or Acrobat, and then set the trust level for the certificate in the application.
3. Revalidate the signature.

Usually, your computer administrator will provide this setup information for you. For general instructions on how to build a list of trusted identities, see "Digital IDs and certification methods" in Adobe Reader Help or Acrobat Help. If you need additional assistance, consult someone who has technical experience in security and the security features of Adobe Reader or Acrobat.

Be aware that establishing trust for a certificate involves a certain amount of risk. In general, you should only configure Adobe Reader or Acrobat to trust a certificate that you personally download from a known and trusted website, or that you receive directly from a trusted individual (after confirming in person or on the phone that he or she indeed sent the certificate).

You may want to consider establishing trust for a certificate if you are likely to receive multiple documents that are signed by the same author or company. Then each time you choose Validate Signatures, Adobe Reader or Acrobat can check against your list of trusted signatures for a match.

How am I allowed to use the Adobe PDF document?

"Why can't I open this PDF document?"

"Why can I print this document but not that other one?"

"Why are Copy and Paste grayed out on the menu?"

"Why can I sometimes save information in forms using Adobe Reader, and sometimes I can't?"

"How do I electronically sign this loan form once I fill it out?"

Depending on how the author of the Adobe PDF document chose to protect the contents, you may come across certain restrictions as you work with PDF documents. For instance, the author may have set specific permissions to prevent unauthorized opening or use of the document. Organizations may have configured a PDF document so that when you open it, functionality that is usually not available in Adobe Reader, such as saving information that you enter into a form, is temporarily activated for use within that document. Or, if the document is a form, the author may have prepared the document to receive your digital signature.

Using hidden functionality in Adobe Reader

Certain Adobe PDF documents that you receive will enable you to perform tasks in Adobe Reader that you can't perform all the time. This is because authors can use Adobe LiveCycle Reader Extensions to create PDF documents that can, on a case-by-case basis, activate functionality that is usually not available in Adobe Reader. This functionality can include the ability to:

- Save a form to your hard drive after you have completed it.
- Submit a completed form over the Internet.
- Digitally sign a document.
- Comment on and review a document.

To gain access to these features for all PDF documents (as well as the ability to create PDF documents), upgrade to Acrobat Standard or Acrobat Professional.

The rest of this section describes the typical ways that authors restrict access and how you can determine the types of permissions you have been granted for a specific PDF document. It also describes how to apply a signature to a document that you're allowed to sign digitally.

Determining restrictions on opening the document

You may occasionally receive an Adobe PDF document that you can't open. If you receive a message that the document requires a newer version of Adobe Reader or Acrobat, go to www.adobe.com/products/acrobat/readstep2.html and download the most recent version of the free Adobe Reader.

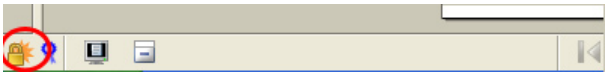
If you receive a message asking you to provide a password and/or a user ID, the author has restricted access in order to protect the confidentiality of the document's information. For instance, authors may require that you:

- **Type a password** to open or use the document. If the document is password-protected, contact the author for password information.
- **Provide a password and user ID** that can be authenticated with *Adobe LiveCycle™ Policy Server* before you can open or use the document. Contact the author for information on obtaining a user name and password if you don't already have that information.

About Adobe LiveCycle Policy Server. Authors who protect their documents with Adobe LiveCycle Policy Server can audit what is done with each copy of the document (such as opening, printing, and editing). They can also change or revoke access rights at any time. If an author has revoked access to a document that is protected by Adobe LiveCycle Policy Server, Adobe Reader or Acrobat informs you that your access rights have been removed the next time you try to open the document.

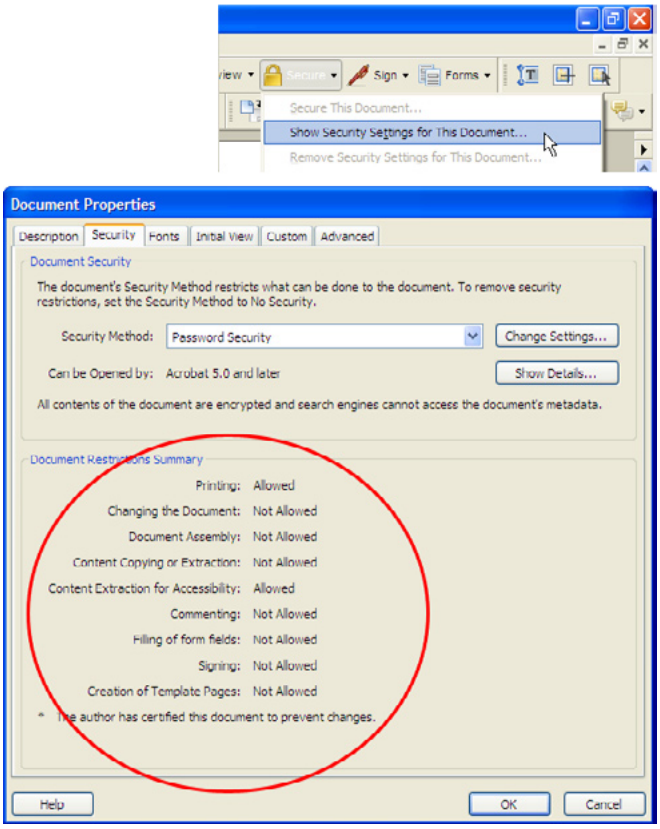
Determining other restrictions on an Adobe PDF document

One quick way to check for restrictions on a specific Adobe PDF document is to look for a padlock icon in the lower left corner of the main window in Adobe Reader or Acrobat. You can hover the mouse over this padlock to view a summary of the tasks that the author has granted or disallowed.



A padlock in the lower left corner of a PDF document indicates that the document restricts how you can use it.

To view specific permissions and restrictions for a document, either use the Secure menu on the Tasks toolbar and choose Show Security Settings For This Document, or open the Document Properties dialog box (File > Document Properties) and select the Security tab. (On Windows®, you can also right-click the padlock in the lower left corner and then select Document Security.)



In Adobe Reader or Acrobat, use the Secure menu on the Tasks toolbar (top) to examine the security settings of the Document Properties dialog box (bottom). Here, you can view detailed information about the permissions and restrictions for the document. (You can also open this dialog box by choosing File > Document Properties, and then selecting the Security tab.)

When you are using Adobe Reader in a web browser, you can view security settings by clicking the triangle that is above the vertical scroll bar. In the pop-up menu, choose Document Properties, and then view the Securities tab.

Any commands or options that are related to restricted usage are also dimmed throughout the Adobe Reader or Acrobat user interface.

Signing an Adobe PDF document

To add a digital signature to an Adobe PDF document, you must first obtain a Digital ID for yourself.

Note: *Both Adobe Reader and Acrobat support digitally signing a document. However, you can use Adobe Reader to sign documents only if the author has used Adobe LiveCycle Reader Extensions to activate that functionality in Adobe Reader.*

Obtaining a digital ID. You can obtain a digital ID in several ways:

- **Go to a Certified Document Services (CDS) vendor, such as GeoTrust.** *Certified Document Services (CDS)* vendors will ask you to prove your identity before granting you a *CDS Digital ID.* A CDS Digital ID provides high assurance of your identity. Adobe Reader or Acrobat automatically attempts to validate any signature that has been created with a CDS Digital ID; this validity check does not require any change to the computer system by the recipient.
- **Go to a Certificate Authority (CA) vendor, such as GeoTrust, VeriSign, or Entrust.** *Certificate Authority (CA)* vendors vary in how much information they ask you to provide to prove your identity.
- **Obtain a Digital ID from your employer's IT group.** Some IT groups refer to a Digital ID as a "signing certificate," an "e-mail certificate," or an "identity certificate."
- **Create a self-signed Digital ID.** You can create a self-signed Digital ID using Adobe Reader or Acrobat.

Designer signatures
In Adobe Reader and Acrobat, you can change the appearance of a signature that you apply to a PDF document. For instance, you might want to add a graphic, such as a scan of your handwritten signature or a graphic of your company logo. See "Changing signature appearance" in Adobe Reader Help or Acrobat Help for instructions.

Signing the document. You may digitally sign a PDF document only if the author has granted permission for you to do so. You can apply a digital signature in several ways, including:

- Click an unsigned signature field that the author has added to a page.
- Choose Sign This Document from the Sign menu on the Tasks toolbar.

If Adobe Reader or Acrobat does not allow you to sign the document (for instance, the Sign menu is not available in the Tasks toolbar or the Sign This Document command is grayed out), you have not been granted permission to sign the document digitally.

Note: *For instructions on obtaining a Digital ID, creating digital signatures, and signing documents, see "Digitally signing Adobe PDF documents" in Adobe Reader Help or Acrobat Help.*

How do I manage trust for Adobe PDF documents as an author?

As an author who is concerned about security, you typically want to protect your Adobe PDF documents in several ways. For instance, you may want to:

- Authorize specific access and use, to keep sensitive information confidential and protect it from alteration
- Protect access with passwords and user IDs, and control and audit document usage
- Provide assurance to recipients, such as customers, that the PDF documents you distribute are authentic and unaltered
- Prepare a PDF document for recipients to sign

This section describes the security features that are available in Acrobat for performing these tasks.

Authorizing access and use

You can restrict an Adobe PDF document from unauthorized access or use by assigning permissions. Depending on the situation and document, you can authorize which users may access the document and how they may work with it. Permissions that you can set in Acrobat include the authorization to:

- Open the document
- Extract material from the document (for instance, to copy text, graphics, or pages for redistribution)
- Change the document (such as to add or remove pages, reorder pages, or add form and digital signature fields)
- Complete interactive forms and digitally sign the document
- Add comments to the document
- Print the document at low or high resolution

You can save multiple permissions settings as a single *security policy* for repeated use. If you are using Acrobat along with Adobe LiveCycle Policy Server, you can also assign different permissions for each user or group who can access the PDF document.

Protecting access and controlling and auditing usage

As part of the process of assigning permissions, Acrobat supports multiple mechanisms for protecting access to the Adobe PDF document and its security settings. The two methods discussed in this guide are password security and Adobe LiveCycle Policy Server. Organizations will find that Adobe LiveCycle Policy Server enables them to more easily control access for large sets of users, dynamically change access permissions, and audit usage of specific documents.

Using password security. In Acrobat, you can set three types of passwords that apply to all users of the PDF document:

- **Document Open** password to prohibit unauthorized viewing of the document

- **Permissions** password to prohibit unauthorized changes to the access rights
- **File Attachment** password to prohibit unauthorized opening of files that are attached to the PDF document

The best practice for creating passwords is to use a combination of letters and numbers. Don't use words or phrases that someone might easily decipher from knowing you, such as a pet's name or an anniversary date.

While password security is the fastest way to protect access to a document, you can achieve greater protection by using Adobe LiveCycle Policy Server.

Using Adobe LiveCycle Policy Server for control and auditing. Adobe LiveCycle Policy Server provides greater access protection than a password (because it requires both a user ID and a password that are specific to each user), and it adds the ability to manage the use of an Adobe PDF document throughout its life cycle. Adobe LiveCycle Policy Server is designed for enterprises and gives authors additional security capabilities beyond Acrobat. With Adobe LiveCycle Policy Server, an organization can:

- Easily manage access for large groups of users (such as employees, customers, or constituents)
- Apply time-based access control, such as setting the start and end dates for access to a document
- Revoke access to distributed documents—for instance, to maintain version control by canceling the rights of specific users to open older versions of a document that they already have in their possession
- Easily define and apply your own security policies for different purposes, individual users, or entire groups
- Batch-process the access rights for multiple PDF documents at once
- Audit how the documents are used, such as when authorized recipients have received, opened, signed, or modified a PDF document

Adobe LiveCycle Policy Server works by requiring recipients of your PDF documents to have an account on your Adobe LiveCycle Policy Server in order to open and use the PDF documents that the server manages. Internal users provide their organization user name and password to log into the server. External users, such as customers, use their e-mail address and password.

Using e-mail and Adobe LiveCycle Policy Server to grant access to multiple people at once
If your enterprise uses Adobe LiveCycle Policy Server and Microsoft® Outlook for Windows®, you can simultaneously e-mail a PDF document and assign a security policy for all recipients at once. Just compose the message and then select Attach As Secure Adobe PDF from the toolbar.

Providing assurance of a document's authenticity and integrity (certifying the document)
Setting permissions and access protections is necessary for helping to shield document content and confidentiality. These precautions alone, however, can't prevent someone from creating a forgery that replicates the look and feel of your document but uses different information, and then sending out the fake document as though it came from you.

To help assure recipients of your document's *authenticity* and *integrity*, you should *certify* the Adobe PDF document in Acrobat. Certification promotes trust in two ways:

- First, the act of certifying applies a digital signature that Adobe Reader or Acrobat automatically checks for its authenticity. This process can help recipients ascertain whether the document is really from your company as they open the file.
- Second, during certification, you can specify that certain kinds of changes cannot be made without also affecting the validity of the certification. If someone makes these changes to the document, Adobe Reader and Acrobat would alert the recipient that the document has been modified and would flag the certification as Invalid.

Because changes that you make to a PDF document can invalidate the certification, you should wait until the document is complete before you certify it. To certify a document, use File > Save As Certified Document.

Note: *Do not sign the PDF document before you certify it. Once you sign the document, the Save As Certified Document command is no longer available, and the document cannot be certified.*

Using Adobe Certified Document Services. To promote a greater level of trust in your Adobe PDF documents, you can apply digital signatures that are issued by Adobe Certified Document Services (CDS). CDS is a partnership between Adobe and specific Certificate Authorities who use a strict *vetting* process to validate the identities of individuals and organizations that request Digital IDs from CDS. Digital IDs from CDS are stored on security hardware (such as a USB device) to help protect against unauthorized use or theft.

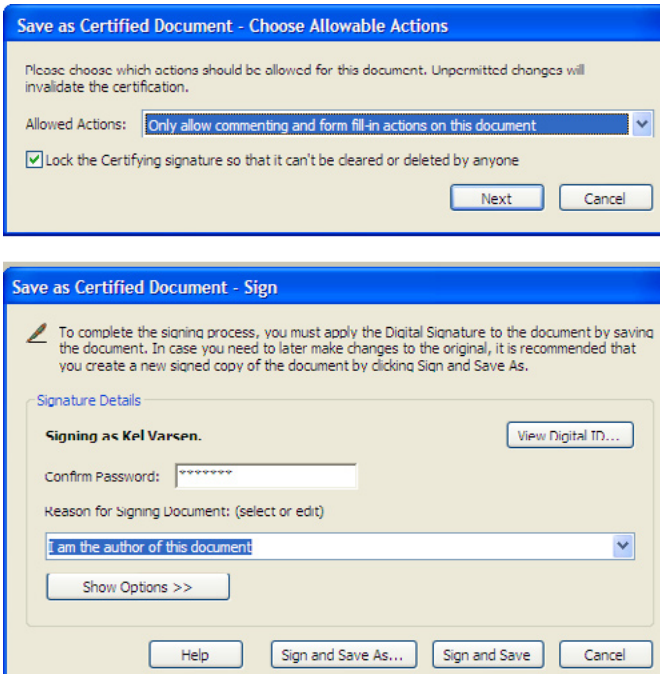
Comparison of Adobe Reader and Acrobat security features

TASK	ADOBE READER	ACROBAT
Features for helping to assure users of the authenticity and integrity of the document:		
Certify PDF documents		x
Automatically check certification signatures	x	x
Apply standard digital signatures	x*	x
Manually check digital signatures	x	x
Features for helping to assure confidentiality and protect access rights		
Set permissions using password security		x
Set permissions using certificate security (PKI)		x
Set permissions using Adobe LiveCycle Policy Server		Version 7.0 or higher
Features for auditing usage and managing (granting and revoking) access rights after distribution		
Apply protection using Adobe LiveCycle Policy Server		Version 7.0 or higher
Access PDF documents that are protected by Adobe LiveCycle Policy Server	Version 7.0 or higher	Version 7.0 or higher

* Authors can activate this Adobe Reader feature for specific PDF documents by using Adobe LiveCycle Reader Extensions.

Unlike other Digital IDs, CDS Digital IDs do not require recipients of your PDF documents to manually configure their systems to establish trust for your Digital ID. Instead, Adobe Reader and Acrobat have been designed to recognize CDS Digital IDs and to automatically report whether the signature is Valid or Invalid. (For Digital IDs that come from non-CDS sources, users must interpret and assess the trustworthiness of the Digital ID on their own, and then manually configure their computers and Adobe Reader or Acrobat to trust the Digital ID.)

If you want your documents to be broadly trusted without requiring recipients to reconfigure their computers, obtain a Digital ID from a CDS partner and use it to certify and sign your PDF documents. The list of Adobe CDS partners is available at www.adobe.com/security/partners_cds.html.



When certifying a PDF document, you can choose allowable actions that won't invalidate the certification (top) and provide a reason for signing the document (bottom).

Preparing an Adobe PDF document for signatures

To enable customers and employees to apply digital signatures to an Adobe PDF document, you should create a form field for each signatory before certifying the document and distributing it. In essence, you are turning the PDF document into a fillable, electronic PDF form.

If you intend the document to be signed by people who will be using the free Adobe Reader (as is typically the case with customers), you must use Adobe LiveCycle Reader Extensions to prepare the PDF document for signing.

Using Adobe LiveCycle Reader Extensions. Using Adobe LiveCycle Reader Extensions enables you to assign usage rights to an Adobe PDF document and have those usage rights temporarily activate hidden functionality in Adobe Reader each time the document is opened. For instance, you can enable anyone to use the free Adobe Reader software to:

- Save information in forms locally on their computer
- Digitally sign forms and documents
- Add comments
- Submit or route the PDF document over the Internet

When a user finishes with that specific PDF document, the functionality is turned off in Adobe Reader until the user receives another rights-enabled PDF document. By using Adobe LiveCycle Reader Extensions to prepare PDF documents, you can streamline collaboration with employees and customers.

Glossary

Adobe LiveCycle Policy Server—A server offering from Adobe that enables businesses to manage information access more securely with dynamic, persistent document control.

authenticity—The assurance that a document is genuine and from the party that it says it's from.

CDS Digital ID—See *Certified Document Services (CDS)*.

certificate—In the context of a PDF document, the public half of a Digital ID. Also known as a public key certificate. See also *Digital ID*.

Certificate Authority (CA)—Someone who issues Digital IDs. For example, a CA can be an organization that sells Digital IDs (such as GeoTrust, VeriSign, or Entrust), the IT department of a larger company (such as a bank or insurance company), or a government department or agency that issues Digital IDs.

certified Adobe PDF document—A document that contains a certification (author's) signature.

Certified Document Services (CDS)—A joint solution offered by Adobe and its security partners that can help recipients trust a PDF document. CDS can help provide assurance of the author's identity (validating the document's authenticity) while also showing that the PDF document has not been modified (validating the document's integrity). CDS is the only security solution that provides automatic validation of these attributes in Adobe Reader or Acrobat, without also requiring additional software or configuration changes by the recipients.

certify—To apply a digital signature to a PDF document in order to help assure recipients that the document is from a genuine source (that the document has authenticity), and that unauthorized changes have not been made to its content (that the document has integrity).

Digital ID—An electronic identity that lets you create a digital signature. A Digital ID can be stored in a password-protected file on your computer or, for greater security, on a USB token, smart card, or other security hardware device. Also referred to as a private key, a credential, a profile, signing certificate, identity certificate, or e-mail certificate.

digital signature—An electronic representation of someone's signature that has been created with a Digital ID.

integrity—The assurance that a document has not been tampered with or modified in an unauthorized way.

security policy—A predefined set of access rights that you can save for later use.

time stamp—The part of a digital signature that indicates the date and time that the signature was created; the time stamp is generated from the system clock of the signer's computer or an external secure Time Stamp Server.

vetting—A process that a Certificate Authority (CA) uses to verify an organization's or individual's identity before they issue a Digital ID. The rigor of vetting can vary considerably. Some CAs require a person to enter credit card purchase information on a web page; others require applicants to physically appear at a location and present one or more forms of government-issued identification. Some CAs also include credit report or background checks. The stronger the vetting process that a CA uses, the greater the assurance that a Digital ID issued by that CA is trustworthy.

A Digital ID is private to its owner (like an ATM card) and is used to digitally sign a PDF document. There is a public part of the Digital ID, called a certificate, that is added to every digital signature that is created. The certificate is used to validate that a digital signature was created by its specific Digital ID.

FOR MORE INFORMATION

For more information on:

- Adobe Document Control & Security,see www.adobe.com/security
- Adobe LiveCycle Policy Server, see www.adobe.com/products/server/policy
- Adobe LiveCycle Document Security, see www.adobe.com/products/server/securityserver
- Adobe LiveCycle Reader Extensions, see www.adobe.com/products/server/readerextensions
- Adobe Certified Document Services, see www.adobe.com/misc/pki/cds_cp.html

Adobe Systems Incorporated • 345 Park Avenue, San Jose, CA 95110-2704 USA • *www.adobe.com*

Adobe