

Certifying Documents with Future Signature Fields in Adobe Acrobat 8

Overview

The ability to certify a document in Adobe Acrobat offers many security-related benefits. For example, certifying a PDF document allows a user to specify exactly what types of changes (if any) are allowed. If any modifications are made outside of those specified during certification, the document will lose its certified status. This allows other users to be confident that the document has not been modified in a way the author did not intend.

In Adobe Acrobat 8, adding a new signature when one or more other signatures have already been applied will cause Acrobat to display a warning to indicate that the document has been modified since the previous signatures were applied. In situations where multiple signatures need to be added to a document, especially if the document contains form data that must be entered by a signer, it is preferable to first certify the document to allow these changes. Additional signatures on a certified document do not produce these warnings.

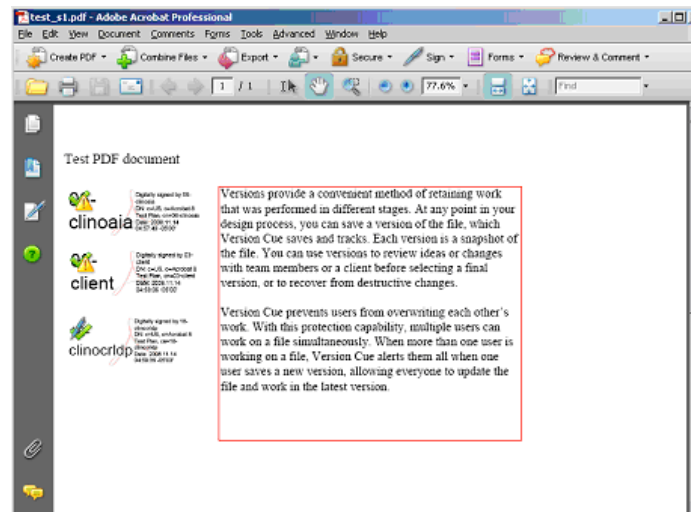


Figure 1: Digital signatures added to an uncertified document result in yellow warning symbols.

These “subsequent changes” notifications, although not particularly harmful, are often undesirable in final versions of a document. Adding blank signature form fields and subsequently certifying the document to permit digital signatures will completely resolve the issue.

Creating Form Signature Fields

Before certifying, all of the form signature fields must be added to the document. The number of signature fields added to the document before certifying is the maximum number of signatures that can be applied. Users are not permitted to add new fields to a certified document.

- 1) Open the document.
- 2) On the menu bar, select **Tools->Forms->Digital Signature Tool**.
- 3) For each time the document is expected to be digitally signed, draw one rectangular digital signature field with the mouse. (Remember, more fields **cannot** be added later.)

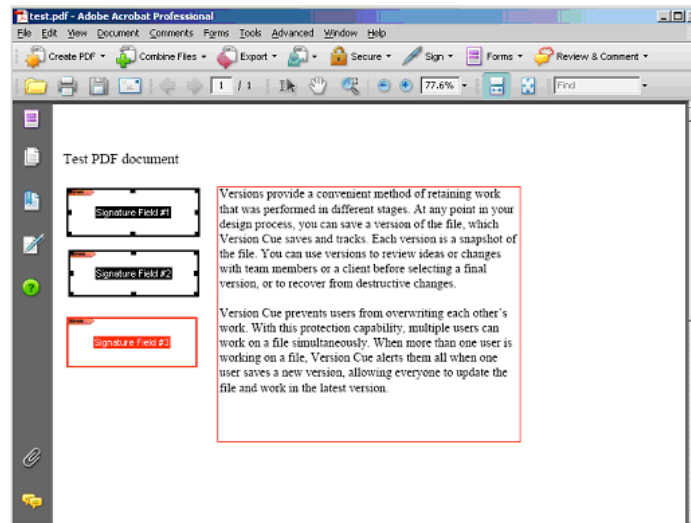


Figure 2: Three digital signature form fields have been added to a PDF document.

Enabling Acrobat Reader Functionality

By default, Adobe Reader will not allow a user to sign a signature field on a PDF. If the document is intended to be signed using Adobe Reader, it will be necessary to Reader-enable the document. It is possible to Reader-enable a PDF both before and after it has been certified. To activate this option:

- 1) On the menu bar, select **Advanced->Enable Usage Rights in Adobe Reader...**
- 2) A window will appear informing you of any changes the document will undergo to become Reader-enabled. Click "Save Now."
- 3) Another window will appear asking you to save the document. After clicking "Save" again, the document will be Reader-enabled.

Certifying a Document

After signature fields have been applied, the document should be certified. This requires the user to have an Adobe Acrobat Digital ID capable of being used to sign documents. Digital IDs can be added in the Security Settings menu (under **Advanced->Security Settings...**).

- 1) On the menu bar, select **Advanced->Sign & Certify->Certify with Visible Signature**

- 2) Draw a rectangle with the mouse where you want the certification status to appear. It is also possible to select “Certify Without Visible Signature,” although this will cause the certification status field to not be displayed within the content area of the document.
- 3) A window will appear asking you to select the Digital ID to use to certify the document. Select the desired Digital ID and enter its password.

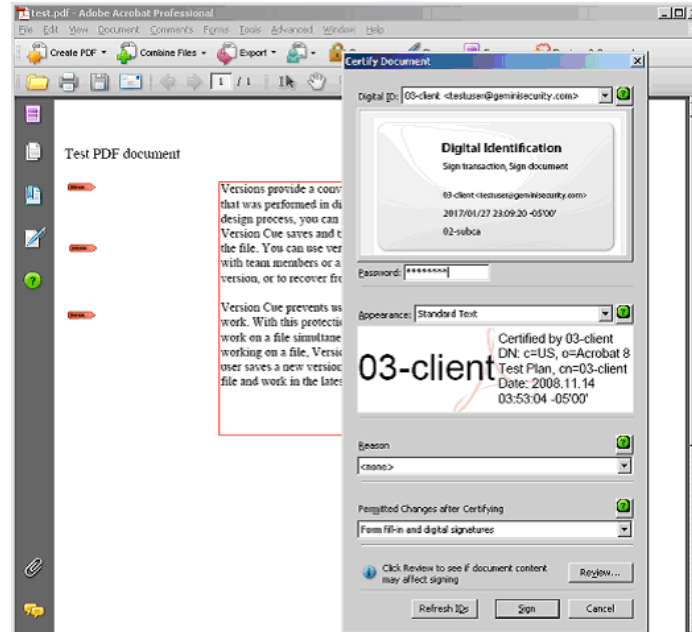


Figure 3: The user selects a Digital ID for certifying.

- 4) Select the “Form fill-in and digital signatures” option under the “Permitted Changes after Certifying” dropdown menu.
- 5) Click “Sign.”
- 6) You will be asked to save the newly certified document. Once it is saved, you should see a ribbon indicating to users that the document has been successfully certified.

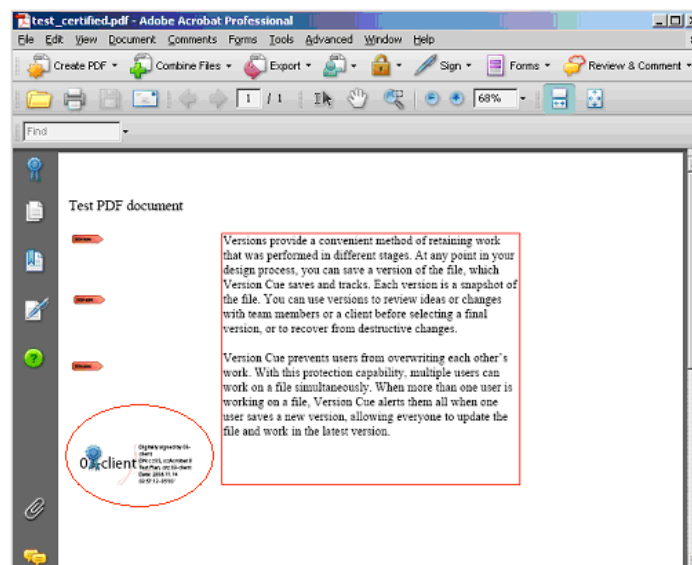


Figure 4: A ribbon appears, indicating that the document has been certified.

Signing a Certified Document

After a document has been certified, it can be signed if and only if it contains blank signature form fields AND digital signatures are permitted. Digital signatures also require the use of an Adobe Acrobat Digital ID, so one should be useable before beginning the signing process. It is also possible to use any credentials kept in the Windows CAPI store.

- 1) Either click on a blank signature field OR go to **Advanced->Sign & Certify->Sign Document** on the menu bar. In Adobe Reader, the menu option is in **Document->Digital Signatures->Sign this Document**. If multiple signature fields are present when using the menu option, Reader will require you to manually select one of them.
- 2) A window will appear asking you to select the Digital ID to use to sign the document. Select the desired Digital ID and enter its password.

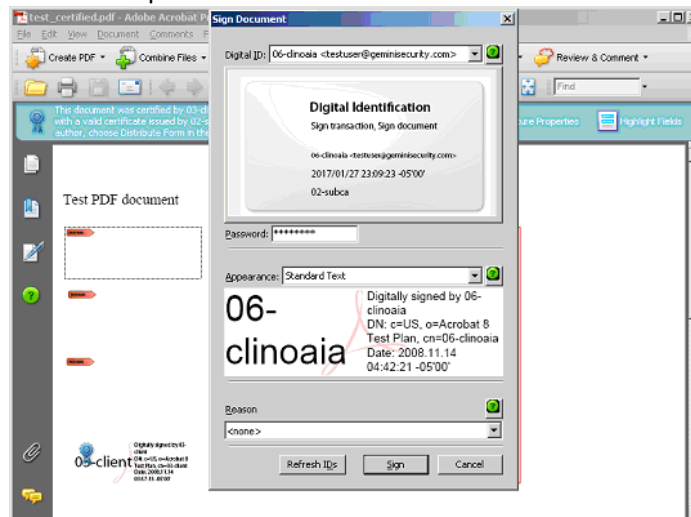


Figure 5: The user selects a Digital ID for signing.

- 3) Click "Sign."
- 4) You will be asked to save the newly signed document. Once it is saved, you should see a checkmark indicating to users that the document has been successfully signed.

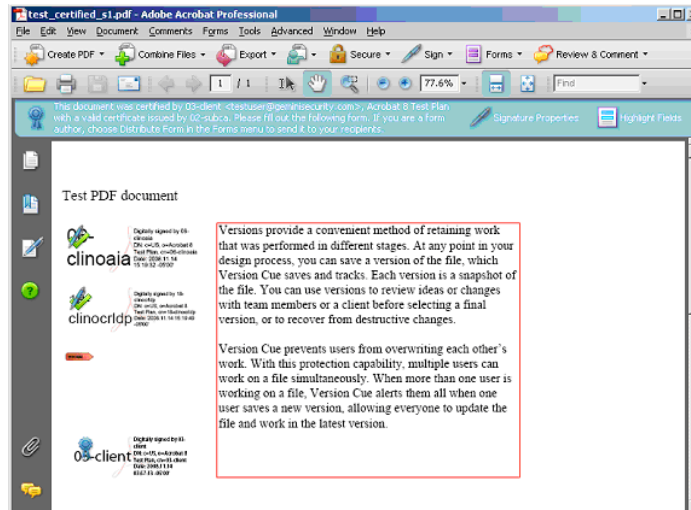


Figure 6: A checkmark appears, indicating that the document has been signed. (Notice that multiple signatures do not have a “subsequent change” warning icon.)

Failed Certification

It is important to note that the green check will only appear if no other significant issues or problems are found. Errors in revocation can cause a certificate to display something other than the green check if revocation checking is required (configurable in the security settings menu). This includes situations where a document is signed with a revoked certificate as well as when Acrobat/Reader is incapable of checking the revocation status due to network problems or missing/invalid information available from the Certification Authority. The status symbol is also affected by tampering/modification outside that which is allowed.

Additionally, errors related to timestamps may appear if any of the relevant certificates in the timestamp server’s certificate chain are invalid. In most cases, any issues or warnings are display in the “Signature Properties” window. If you are unable to produce green checkmark icons on newly added signatures, the problem might be related to one of these potential issues. In addition, any problems with the document certification can also prevent successful signature validation. In general, certification signatures should be successfully validated before a form is distributed.

Below are some common certification statuses that indicate an underlying problem, possibly preventing a document from being fully validated:

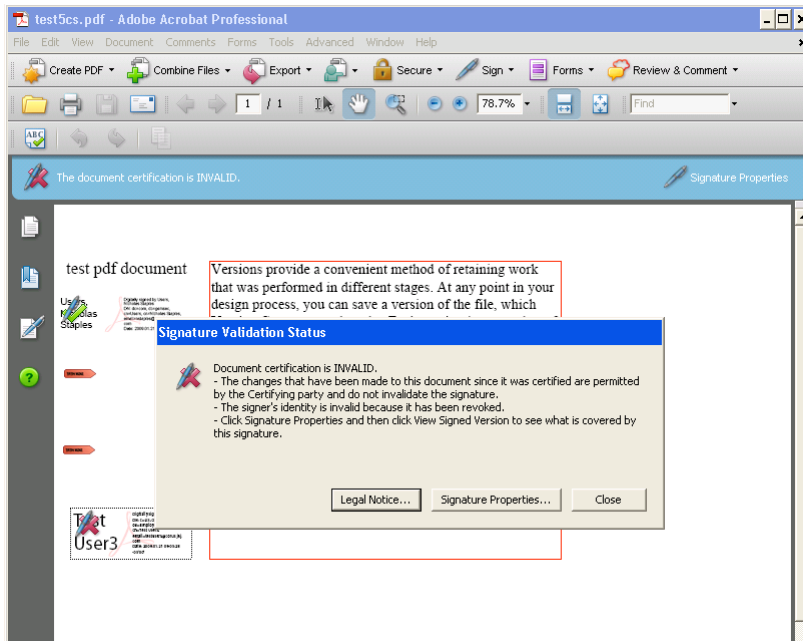


Figure 7: A revoked status results in a red “X” icon. The signature status indicates that the certifying certificate has been revoked.

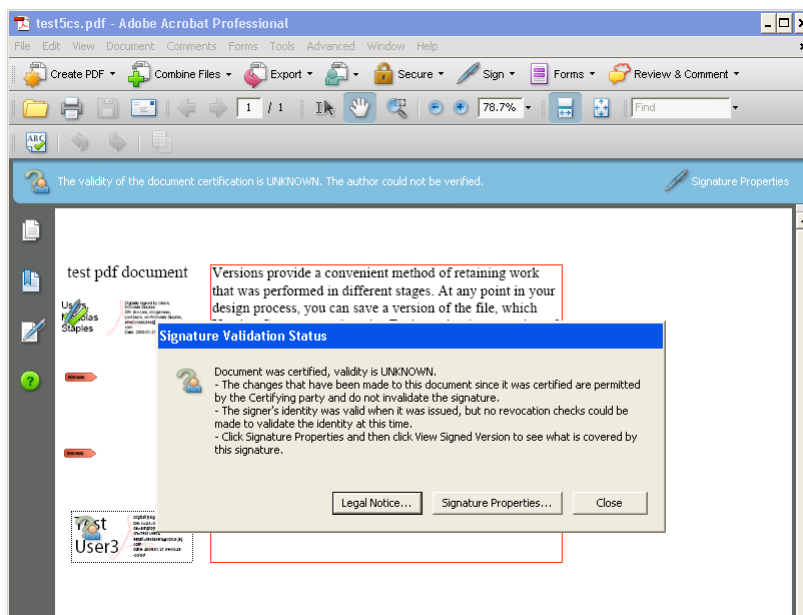


Figure 8: If the “require revocation checking” option is enabled and Adobe fails to communicate with a specified source of revocation information (OCSP, online CRL, etc) this icon is displayed.

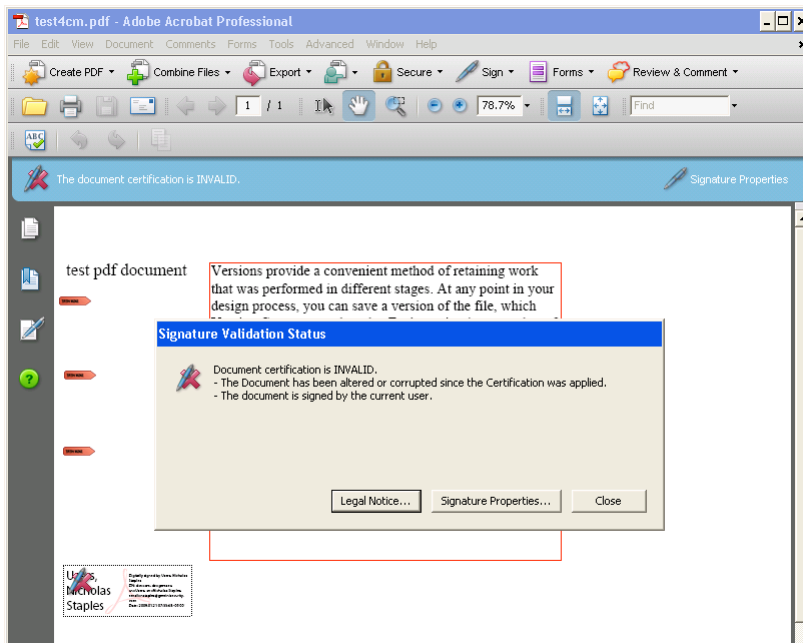


Figure 9: When a document has been modified outside the scope of allowable changes, the red “X” icon appears. When troubleshooting problems, it is important the check the signature properties to understand the nature of the problem (as many potential problems can lead to a red “X” icon).

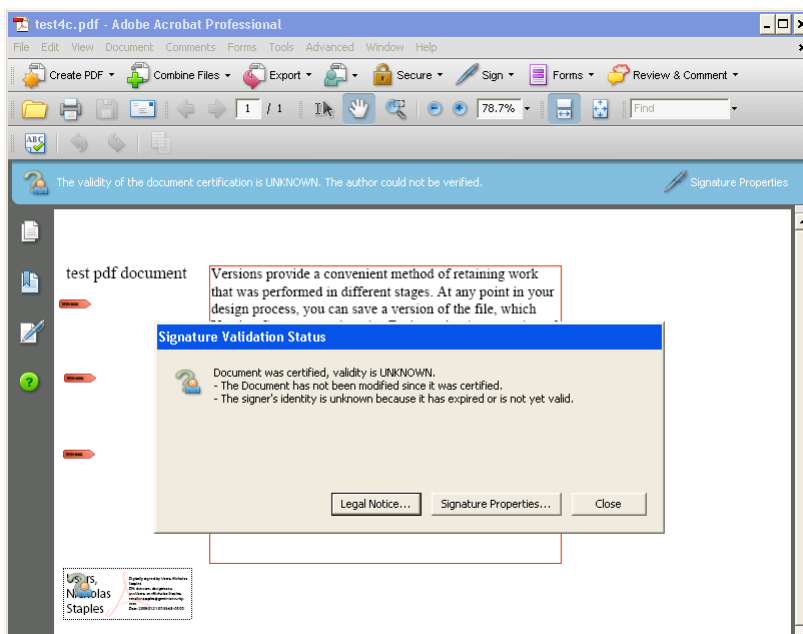


Figure 10: Expired certificates result in a “?” icon. This typically means that the current date/time does not fall within the bounds of the certificate’s validity period.

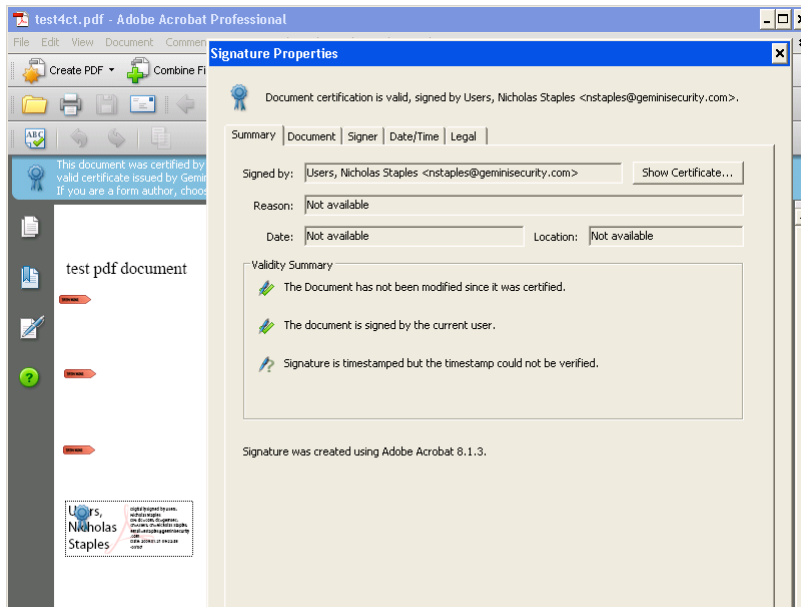


Figure 11: Invalid timestamps may or may not cause the icon to change. This depends on whether the certificates in the timestamp server chain are valid at the current system time. An inspection of the signature properties indicates any errors in verifying the timestamp.

For More Information

If you have any questions about the contents of this document, or are interested in learning more about digital signatures, or ways to reduce paper and improve processes in your organization, please contact: Peter Hesse (pmhesse@geminisecurity.com)

Gemini Security Solutions, Inc.
4451 Brookfield Corporate Dr. Suite 200
Chantilly, VA 20151
703-378-5808
<http://geminisecurity.com>

About Gemini Security Solutions

Gemini Security Solutions, Inc. provides impartial information security consulting services that ensure the confidentiality, integrity, and availability of critical business information and resources. Our value is centered on our ability to deliver the right expertise and the right experience, at the right time.

Founded in 2001, and with decades of experience, our certified team of experts assists organizations to assess and deliver security solutions in compliance with business strategy, policy and regulatory requirements. Our services include risk analysis and management, regulatory compliance, identity access and management, operations security, and security software development.

Gemini Security Solutions is focused on providing big business experience with a small business approach. Working with you every step of the way, Gemini Security Solutions enables secure business operations with vigor, agility and a commitment to excellence.