Verification of digitally signed PDFs

Configuring Adobe Reader to verify digitally signed PDFs

This document is freely redistributable.
You can find the latest version at:
http://www.netlock.hu/USEREN

1. Contents

Steps for the PDF document receiver

2. System requirements

Minimum operating system requirement:

- Windows XP SP3

Requirements when using SHA2 hash algorithm family:

- Operating system:
  - Windows XP SP3 or Windows Vista SP1
- Adobe Reader version:
  - Adobe Reader 9.1

The program was not tested on 64 bit operating systems.

3. What is needed for verification?

Adobe Reader is required for viewing PDF files, which is already installed on most computers, because the popularity of the PDFs.

The software can be downloaded and used for free.

- It is always recommended to **use the latest version of the Reader**!

You can download the software from the website of Adobe:

- www.adobe.com

Direct download link for this software:

- http://get.adobe.com/reader/otherversions/

4. Preparation steps

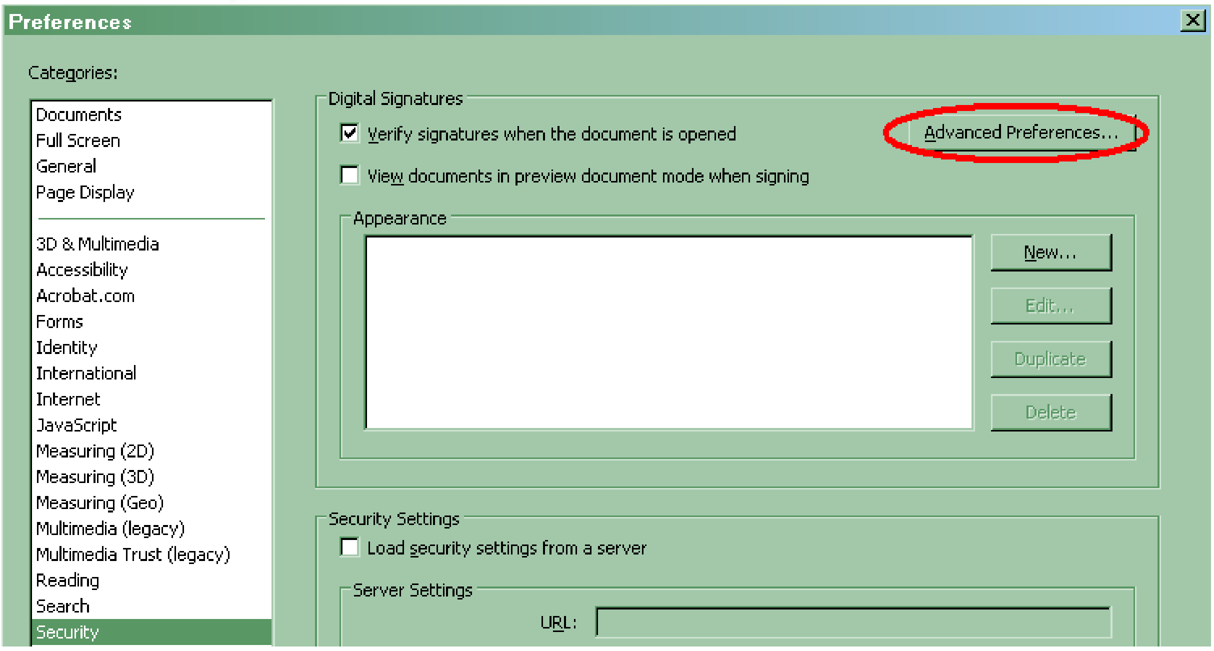
If you are using Adobe Reader for the first time, or encounter an error during certificate verification, you should follow the following steps.

4.1. Setting up Acrobat Reader

The Adobe Acrobat Reader has internal and Windows integrated certificate handling function, too. You need to enable integration with Windows after installing Adobe Reader.

You can do this with the following steps:

Edit > Preferences > Security



Preferences

Categories: Security

Digital Signatures

☑ Verify signatures when the document is opened

☐ View documents in preview document mode when signing

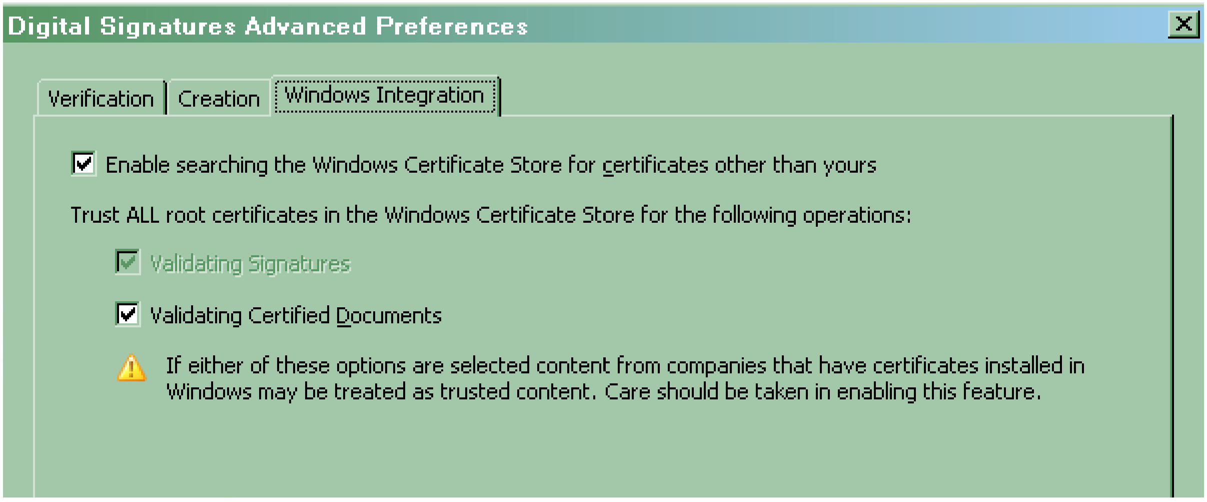
Security Settings

☐ Load security settings from a server

Server Settings

URL:

- Check all the possible checkboxes at the Advanced Preferences menu on the Windows integration tab.



Digital Signatures Advanced Preferences

☑ Enable searching the Windows Certificate Store for certificates other than yours

Trust ALL root certificates in the Windows Certificate Store for the following operations:

☑ Validating Signatures

☑ Validating Certified Documents

⚠ If either of these options are selected content from companies that have certificates installed in Windows may be treated as trusted content. Care should be taken in enabling this feature.

- Click on OK after the configuration.

4.2. Registering certificates in the operating system

If no certificates are used from the qualified root because of the lack of correct integration with the Crypt32 operating system component, you have to manually open a certificate to start the Root Update component on the Windows host.

If you get a message that a signed document or timestamp is invalid, please do the following steps at first:

1. Start a browser and open the following links::
   - http://www.netlock.hu/index.cgi?ca=gold
   - http://www.netlock.hu/index.cgi?ca=cqlca
   - http://www.netlock.hu/index.cgi?ca=cblca
   - http://www.netlock.hu/index.cgi?ca=cclca
2. In the next window, click on the Open button.
3. You can then see the datasheet of the root certificate. In the background the certificate gets downloaded silently from the Microsoft.
4. Close the opened windows.

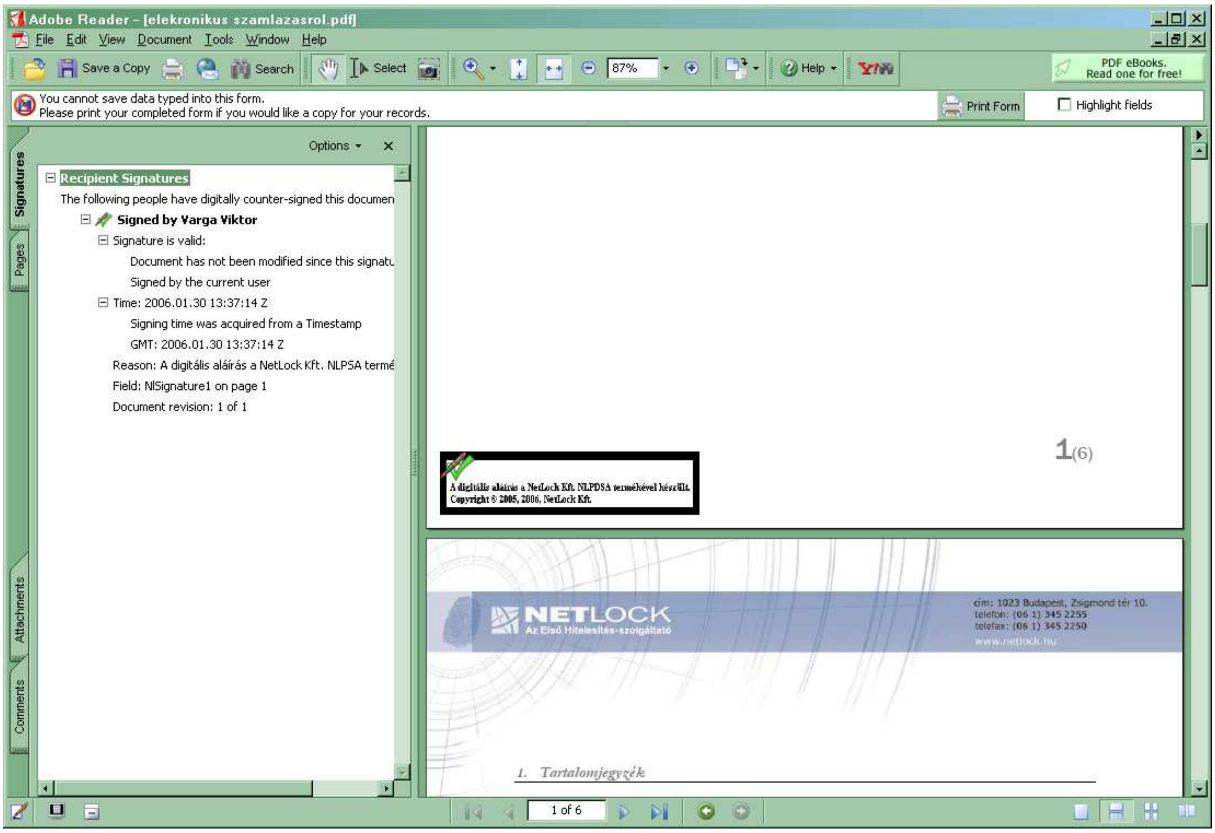
5. Verifying the signature

To verify the PDF file:

1. Open it with Adobe Reader.
   - On the left panel under Signatures you can read the detailed data of the signature,
   - If the PDFSigno product was used to sign the original PDF you will see the stamp on it too. If you click on this picture, you will get more detailed signature info.
2. **A PDF document is automatically verified when opened, so you don't need any additional steps.**

If this verification was unsuccessful you can start a new verification:

- Right click on the signature then click on the **Validate signature** option.



You cannot save data typed into this form.
Please print your completed form if you would like a copy for your records.

Recipient Signatures

The following people have digitally counter-signed this documen

Signed by Varga Viktor

Signature is valid:

Document has not been modified since this signatu

Signed by the current user

Time: 2006.01.30 13:37:14 Z

Signing time was acquired from a Timestamp

GMT: 2006.01.30 13:37:14 Z

Reason: A digitális aláírás a NetLock Kft. NLPSA termé

Field: NlSignature1 on page 1

Document revision: 1 of 1

A digitális aláírás a NetLock Kft. NLPDSA termékével készült.
Copyright © 2005, 2006, NetLock Kft.

6. PDF files with SHA1 signing certificates and SHA256 timestamps

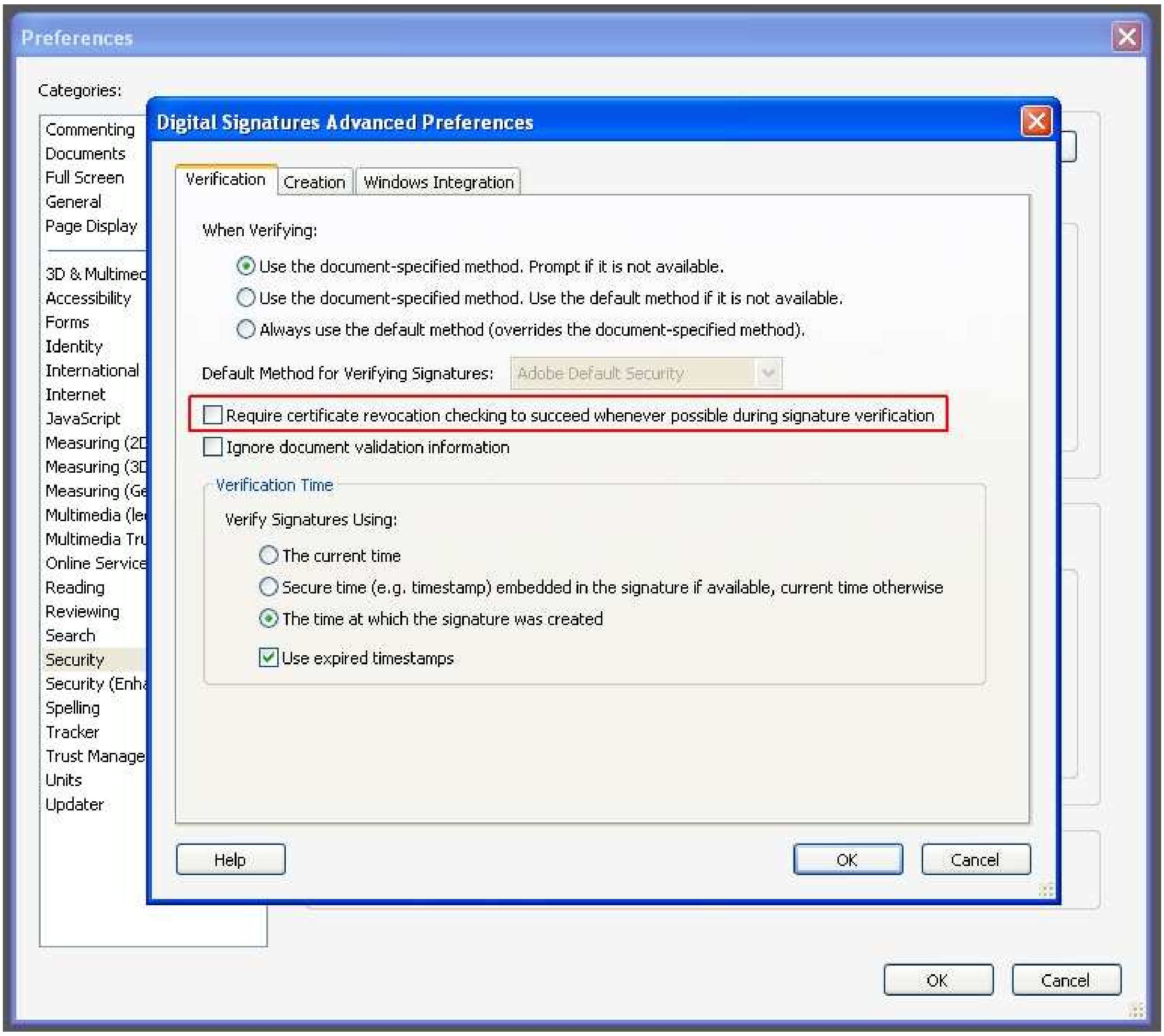
At PDF files with SHA1 signing certificates and SHA256 timestamps, you may get error messages on several occasions.

There is an error when verifying signing certificates in Adobe Reader (it asks for a CRL pertaining to the given time, which is not possible in the standard). The solve the problem, turn off revocation verification, or notification.

To turn off verification:

1. Untick the checkbox "Require certificate revocation…" in the following menu point in Adobe Reader:

   - Edit > Security > Advanced Preferences > **Require certificate revocation…**



When Verifying:

● Use the document-specified method. Prompt if it is not available.

○ Use the document-specified method. Use the default method if it is not available.

○ Always use the default method (overrides the document-specified method).

Default Method for Verifying Signatures: Adobe Default Security

□ Require certificate revocation checking to succeed whenever possible during signature verification

□ Ignore document validation information

Verification Time

Verify Signatures Using:

○ The current time

○ Secure time (e.g. timestamp) embedded in the signature if available, current time otherwise

● The time at which the signature was created

☑ Use expired timestamps

7. Appendix

7.1. About the PDF Signo

The PDF Signo is a client side software which can be used to digitally sign and batch timestamped PDFs: the software can sign a whole batch of files with only one PIN password entry.

This function is a great advantage compared to other programs, which require time consuming successive PIN code entries.

You can read more about this product on the following page:
http://www.netlock.hu/edoc.html (Hungarian page)

7.2. Configuring firewalls

If the local network is protected with firewalls for the validation of the PDFs, the firewall must be configured to allow access for Adobe Reader to the domain *.netlock.hu, as CRL must be downloaded from there.