



Quickstart Guide

OpenLimit Reader 2.5.0.2

Date: 02.03.2010

Contents

1	System requirements	3
1.1	Operating systems	3
1.2	Hardware	3
1.3	Software	3
2	Installation	4
3	Signature verification	5
3.1	Signature verification dialog	6
4	Certificate revocation list update	9
5	Security trust list update	10
6	Product update	10
7	Signature creation	11
8	Service and Support	11



1 System requirements

1.1 Operating systems

- Windows 2000 from Service Pack 4
- Windows 2003
- Windows 2003 64Bit Edition
- Windows XP from Service Pack 2
- Windows XP 64Bit Edition
- Windows XP Tablet PC Edition
- Windows Vista
- Windows Vista 64Bit Edition
- Windows 2008
- Windows 2008 64Bit Edition
- Windows 7 32 Bit and 64 Bit Edition

1.2 Hardware

- Intel 586 compatible Processor
- minimum 200 MB free hard disk space
- minimum 256 MB free available RAM

1.3 Software

- Internet Explorer from Version 5.01, Mozilla from version 1.6 (corresponds to Netscape from version 7.1, Firefox from version 1.0.4)
- JRE (Java Runtime Environment) from version 1.4.2_08
- JAI (Java Advanced Imaging)
- Optional: Adobe Reader / Adobe Acrobat from 7.0.8 (for OpenLimit PDF Plug-In)

2 Installation

Preparation

- I. Please read the end-user license agreement (EULA) prior to the installation.
You can find these on the internet at:
http://www.openlimit.com/assets/files/extras/OpenLimit_EULA-eng.pdf
- II. Please ensure that the system requirements are fulfilled before you start the installation of the OpenLimit software.
- III. Please close all other applications.

Installation

Start the installation of the OpenLimit Reader 2.5.0.2 by running the setup file „**OLReader2502_EN.exe**“ and follow the instructions on the screen.

Choose the language and click „**OK**“.

Read the information in the installation wizard of the OpenLimit Reader and click „**Next >**“.

In the installation wizard you can change the target folder for the program files.

The setup verifies the installation environment and can make essential operating system updates (like the Microsoft Windows Smart Card Base Components, the Microsoft Installer or the ActiveX Control Library, for example) if necessary.

Therefore it is recommended to select the option „**Standard Setup**“ in the installation wizard.

Perhaps it is necessary to **reboot** the system during the installation. After the reboot the installation continues automatically.

After the completion of the setup you can utilize the OpenLimit Reader.



3 Signature verification

The signature verification requires best care and attention. The following points should be verified:

- Is the document really unchanged?
- Is the holder of the signature genuine?
- Has the certificate been revoked?

The software automatically processes certain verification steps. It is the responsibility of the user to decide whether or not a certificate is trustworthy. Qualified signatures in accordance with the German Signature Law are fully traceable to the German Federal Network Agency (Bundesnetzagentur). The issuer certificate of the German Federal Network Agency is integrated into the software. This certification path must be mathematically correct and complete. Other root certificates can, however, also be defined in the operating system as being trustworthy.

It is thus basically up to you, the user to decide which certificates you consider trustworthy and which not.

Further information pertaining to the signature verification procedures and the public key infrastructure is provided in the **OpenLimit User Guide** in the chapter „[Basic Principles of the Electronic Signature](#)“ or in the **User Documentation** under „[Signature verification](#)“.

There are three ways to verify a signature:


Signature verification with the Windows Shell Extension

With the OpenLimit plug-in for the Windows Explorer Shell Extension you can verify attached and detached PKCS#7 signatures. After a right-click on a signature file or a signed file choose „**OpenLimit SignCubes > Verify signature(s)**“ in the shell menu. The signature verification dialog is displayed.

Signature verification with the Adobe Acrobat or Adobe Reader

If you open a PDF file with an embedded PDF signature with the Adobe Acrobat or Adobe Reader you can verify the signature directly from within the Adobe program using the **OpenLimit Adobe Plug-In**.

Embedded PDF signatures can be filed in the document as visible signatures using signature fields or as invisible signatures.

Depending on the Adobe version you will find the signatures in the tab-menu on the left-hand side under the tab „**Signatures**“ or under the icon 

Click with the right mouse button on a filled signature field or on a signature in the left tab-menu and select „Verify signature“. The signature verification dialog is displayed.

Signature verification with the OpenLimit Viewer

With the integrated OpenLimit Viewer of the free OpenLimit Reader only **text and TIFF files** can be opened. With the full version (subject to charge) it is also possible to open and analyze PDF files.

After opening a signed file select „Verify signature“ from the „Edit“ menu or click the toolbar icon „Verify signature“:

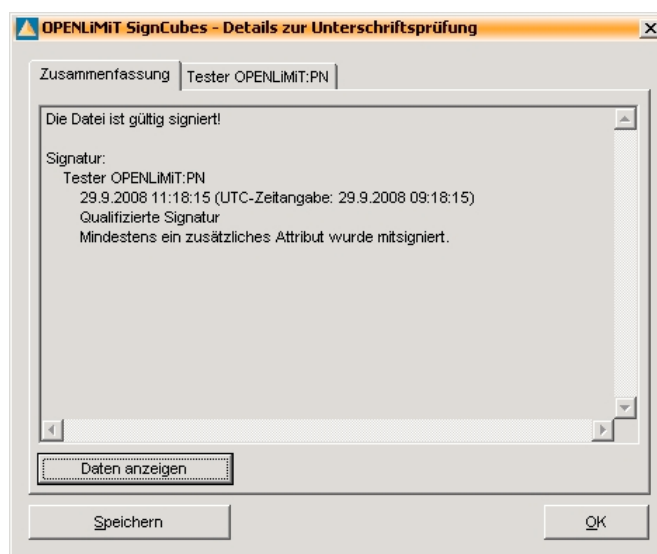


The signature verification dialog is displayed.

3.1 Signature verification dialog

Summary

After clicking **Verify signature(s)** the signature verification dialog is displayed.



In the signature verification summary is stated, whether the signature is **valid, invalid** or **mathematically correct**.

➔ **The file signature is valid!**

The signature verification indicates that the document hasn't been changed since signature creation, the signature data hasn't been manipulated and that the used certificate was valid at the point of signature creation.

➔ **The signature for the file is mathematically correct.**

Mathematically correct means, that the file hasn't been changed since signature creation. Furthermore, the signature data itself hasn't been altered. Most likely it was not possible to completely verify the certificate status. In this case it is recommended to accomplish an OCSP request to verify the validity of the signature. To do so, select the tab with the name of the signer and click „**Online status**“.

Also very common is the fact, that the certificate status cannot be completely verified, because of missing or outdated revocation lists. Here you should perform a revocation list update (see chapter 4 - [Certificate revocation list update](#)) and verify the signature again.

➔ **The signature for the file is invalid!**

A signature is invalid, if the data or the signature has been changed, the certificate is invalid or the signature data is defective.

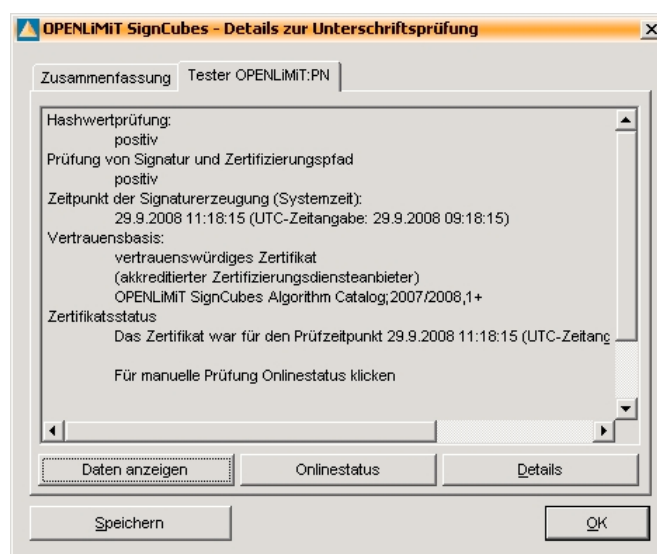
You will find details to the reasons for this statement on the tab with the name of the signer.

You cannot trust this signature.

Signature details

You will find all details of a signature under the tab with the name of the signer.

If a hash algorithm was used that isn't suitable for the creation of qualified electronic signatures (e.g. SHA-1) or the used keys do not have the required minimum length (more than 1024 bit) a note is shown here.



Information

Hash verification: (Integrity of the data)

positive: The data has not been modified since signature creation

negative: The hash values do not match, perhaps the data has been altered

Verification of the signature and certification path:

Verification for corruption of the signature and completeness of the certification path (Certificate chain)

Time of creation of signature:

System time of the PC on signature creation

Trust basis:

Indicates the source of the root certificate on which the certificate verification is based upon. Also the algorithm catalog used for the verification is indicated.

Certificate status:

States the revocation status of the signature certificate. Revocation lists can be used to verify whether the certificate has been disabled by revocation. If that cannot be verified here, it is advisable to download the latest revocation lists or to verify the certificate online by clicking the button „**Online status**“.

Options

Show data: Display the signed data with the OpenLimit Viewer

Online status: OCSP-Request for the certificate (validity request at the certificate issuer)

Details: technical details of the signature (certificate details, used algorithms, time of signature creation, possibly included timestamps, etc.)

Save: save a signature verification protocol (PDF/A format) to disc

4 Certificate revocation list update

The certificate status, meaning the information whether a certificate has been revoked at the time of signature creation, can be verified by the certificate issuer: certificate authorities resp. trust centers provide certificate revocation lists (CRLs) for download and/or offer an online status request for the certificate. The CRL lists all the certificates that have been revoked by the certificate authority.

Further information regarding public key infrastructure can be found in the **OpenLimit User Guide** in the chapter „[Basic principles of the electronic signature](#)“.

This is how you download a current revocation list:

1. Click the **OpenLimit Icon** in the taskbar.
2. Choose **Update CRL**.
3. Now the OpenLimit SignCubes CRL Loader opens with a welcome-page, click „**Next >**“ to continue.
4. Choose from the list of certification authorities the desired revocation list providers by clicking the checkboxes or use the button „**Select all**“ and click „**Next >**“
5. The desired revocation lists will be downloaded from the corresponding provider.
6. The progress bar will show you the download progress of the particular file. At the end a list is shown with the results of the download.
7. Click on „**Finish**“ to close the CRL Loader



Please note: To update these revocation lists you need to be connected to the Internet. If no connection could be made the status message will show „Download Error“. Latest CRLs are necessary to successfully verify signatures. If you do not update your CRLs you can not verify the validity of signatures resp. the used signature certificate and the certificate chain.

5 Security trust list update

The root certificates of the certification authorities and the German Federal Network Agency (Bundesnetzagentur) are known to the OpenLimit SignCubes base components 2.5.0.2 by use of signed security trust lists.

Choose the menu item **Update CRL**.

Now the OpenLimit SignCubes CRL Loader opens with a welcome-page, click „**Next >**“ to continue.

In the selection dialog of the CRL Loader you will find a checkbox for the security trust list update in the upper section of the window.

Click the checkbox „**Update security trust list**“.

Please read the previous chapter from point 4. for further steps.

6 Product update

The German Federal Network Agency (Bundesnetzagentur) issues a so-called algorithm catalog each year regulating the use of permitted algorithms for qualified electronic signatures.

This update as well as other product updates you will find under:

➔ <http://www.openlimit.com/updatecheck/>

7 Signature creation

Specific forms that have been created in conjunction with OpenLimit signature applications can be signed with the OpenLimit Reader. Therefore these forms have to be equipped with special document rights. Users of the free OpenLimit Reader can sign electronically directly from within Adobe Reader using a smartcard and a card terminal.

For further information regarding **Smartcards** and **Signature creation** please read OpenLimit User Guide.

8 Service and Support

OpenLimit SignCubes AG
Zugerstrasse 76 b
CH - 6341 Baar
Switzerland
<http://www.openlimit.com>

Tel: +41 41 560 1020

Fax: +41 41 560 1039

Support-Hotline: Monday-Sunday from 8 a.m. to 10 p.m.

Germany: 0900 147 8877

Switzerland: 0900 510 966

Landline: EUR 1,99/min

Mobile: EUR 2,00/min*

Landline: CHF 3,10/min

Mobile: CHF 3,20/min*

* perhaps additional fees are charged by your mobile provider.

Please note: You will find further information regarding our technical support under:

<http://www.openlimit.com/en/support/>

