



Aloaha Multisignator EN

© 2010 Wrocklage Intermedia GmbH

Aloaha Multisignator EN

© 2010 Wrocklage Intermedia GmbH

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: Juni 2010

Table of Contents

	Page
1. Introduction	4
2. Usage	5
3. Installation	7
3.1 System requirement	7
3.2 Installation	8
4. Configuration	10
4.1 Settings	11
4.1.1 Digital Signature	12
4.1.2 Automailer	18
4.1.3 Global Settings	19
4.1.4 Directory Picker	20
4.1.5 POP3 Settings	21
5. Digitally Sign	22
6. Language.ini	24
7. Aloaha signature service	25
8. Aloaha Commandline Signator	27
9. CryptoAPI	27
10. Technical Informations	28
11. FAQ Multisignator	30
Index	32

1. Introduction



Generate serversided mass signatures for the electronic calculation position. Use the immense saving potential by legal-compliant electronic calculation lapping!

Save in future high costs by savings in working hours, writing paper, envelopes, printing and postage costs. By the electronic calculation dispatch the delivery time and the payment destination becomes shorter.

Persuasive arguments to switch over to electronic calculation position.

Therefore you need professional software like the Aloaha Multisignator which is compatible to your accountancy system and provides the outgoing E-calculations automatically with certified signatures.

Other advantage: Also the archiving costs fall off with electronic calculation position.

In contrast to other mass signature solutions a huge number of certified signature cards as well as software certificates were supported by the Aloaha Multisignator.
Additional card drivers are dispensable with the Aloaha Multisignator!

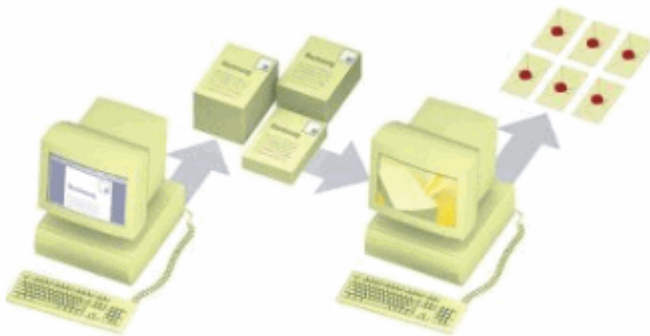
2. Usage

The Aloaha Multisignator was developed to carry out mass signatures and save resources.

Thus functions of the Aloaha Multisignator

The source calculations to be signed are simply copied in a folder of the computer. This can automatically happen by your accountancy software. The Aloaha Multisignator provides each of these files with an electronic signature and dispatches them afterwards by e-mail. The e-mail addresses can be read out either from the PDF themselves, or be passed by means of a command file generated by the accountancy. If requested e-mail itself can be still signed. For the rise of the productiveness several signature cards can be selected parallel.

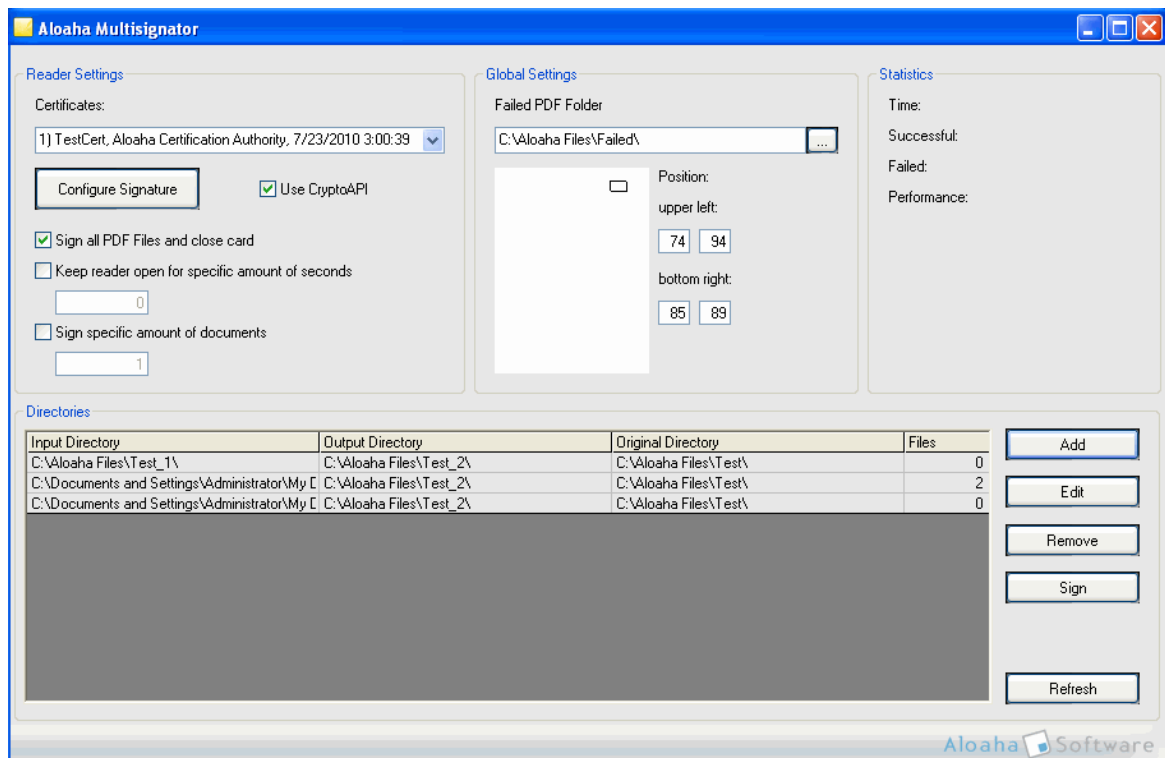
With incoming invoices an automatic signature check carries out of the Aloaha Multisignator. In negative check the system automatically informs.



Preparation

Before you begin with mass signatures, after end of the Installation some settings must be carried out.

After the start of the program you see the below shown display.



First the suitable directories must be laid out for the documents to be processed.

Furthermore the reader settings should be set up for the card reader(s) and the signature be configured.

Depending on whether you liked to sign documents about a period or a certain number the suitable field is to be activated.

If you liked to apply none of these options, activate "Signs all PDF documents and closes card". With this command all documents are signed without limitation.

In the global settings you fix the directory for failed documents. Here documents are saved which must be edited again, because there have been problems with the mass signature. Furthermore the position and size of the signature field is to be fixed here.

For statistical purposes following parametres of the occurred mass signature are indicated:

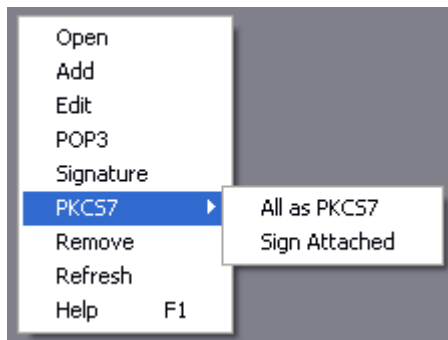
Time:

Successfull:

Failed:

Performance:

If you click with the right mouse button on an input directory you could select under PKCS7 whether all or only the not pdf files of the PKCS7 folder files should be signed. Furthermore you can select whether an envelope should be created or an external signature file.



3. Installation



- Systemrequirement
- Installation

3.1 System requirement

- Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Windows 7
- **No Adobe Reader necessary!**

3.2 Installation

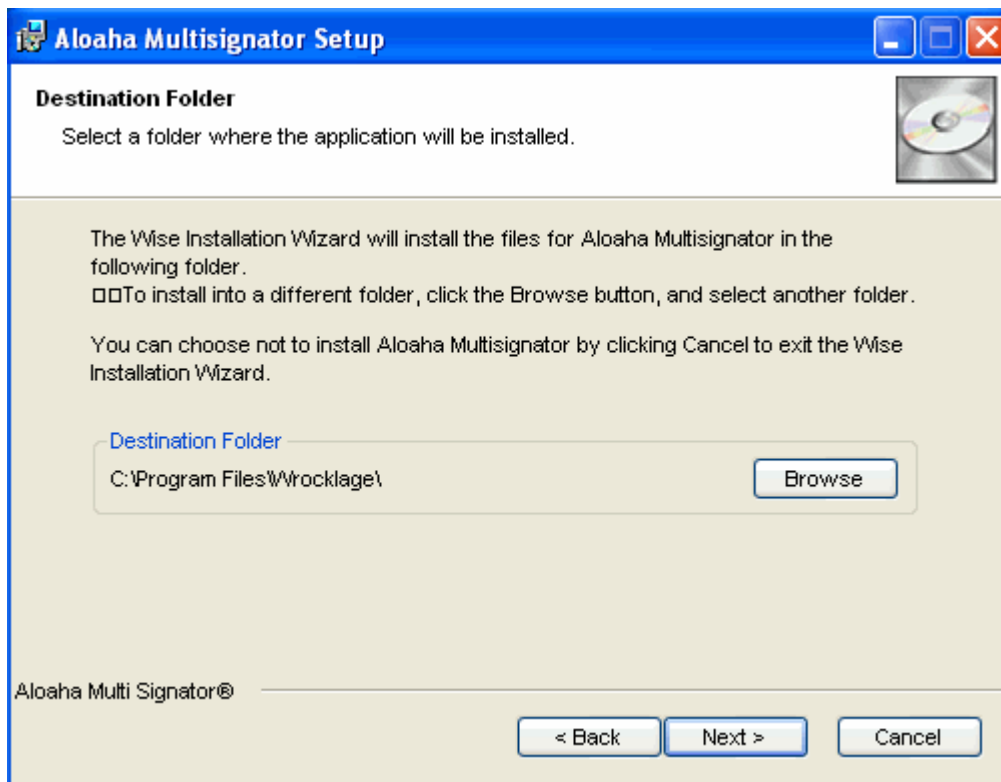
You can download the Aloaha PDF Multisignator to yourselves directly from the Internet under http://www.aloaha.com/download/aloaha_multisignator.zip.

Save the file directly on your hard disk. As soon as the download is quit, unpack it and double-click on "multisignator.exe".

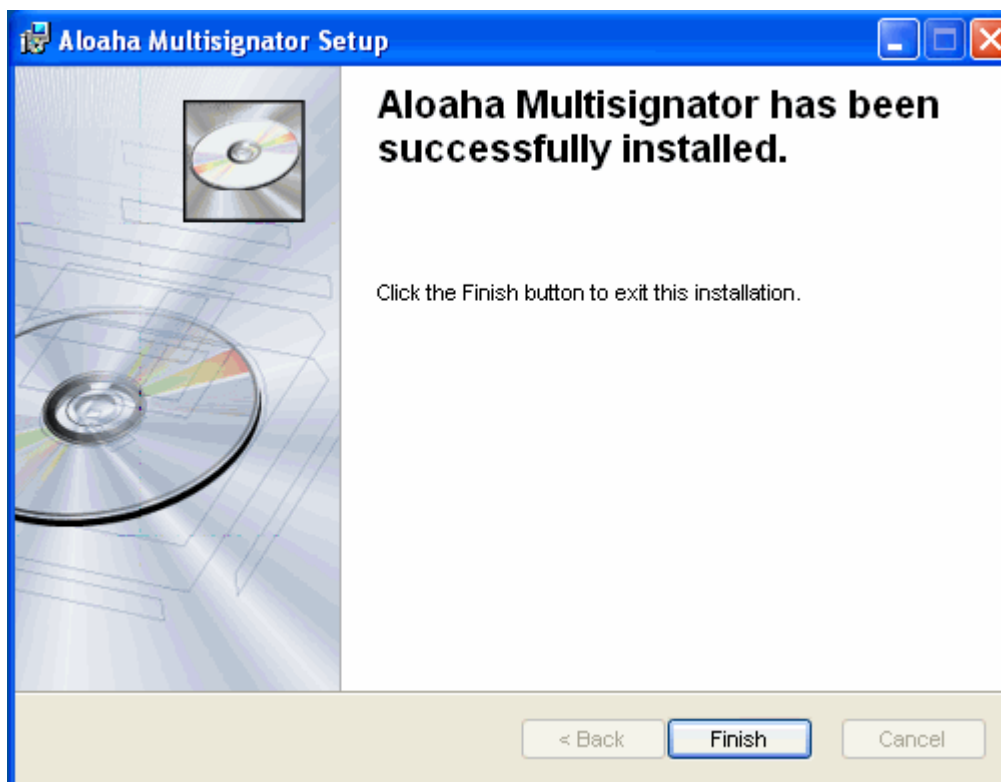
Afterwards you start to install the software.



Click on Next. In the next dialog you select the installation directory. Normally this is up c:\programme\wrocklage preset.



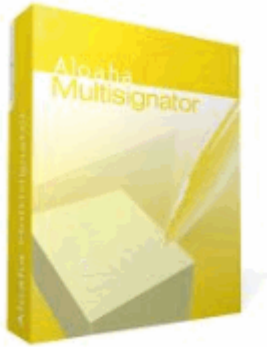
At this point of the installation you can select whether you would like to return 1 step back or if the installation should begin. Click in addition on back or further.



After the successful installation you conclude the installation process with "Finish".

Now you can use the Aloaha Multisignator. You will find a shortcut for launching the program in the top menu **Start>All programs>Aloaha**.

4. Configuration



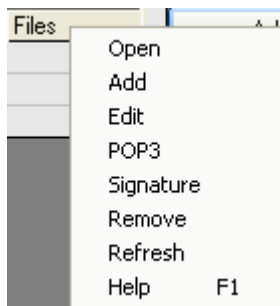
- Settings
- CryptoAPI
- Sign Digitaly
- Language.ini
- FAQ
- Aloaha signature service
- Technical Informations
- Aloaha Commandline Signer

4.1 Settings



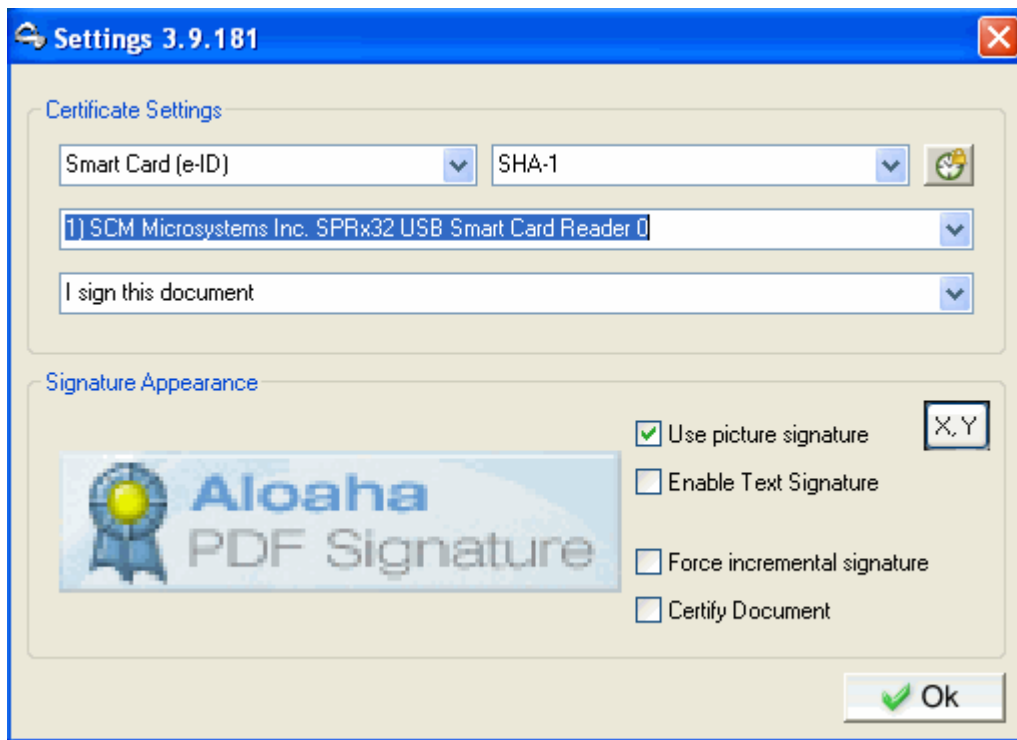
- Digital Signature
- Automailer
- Global Settings
- Directory Picker
- POP3 Settings

All settings can also be called by click with the right mouse button on the field Directories.



4.1.1 Digital Signature

If you want to sign documents with the Aloaha Multisignator digitally, you have to carry out some settings before.

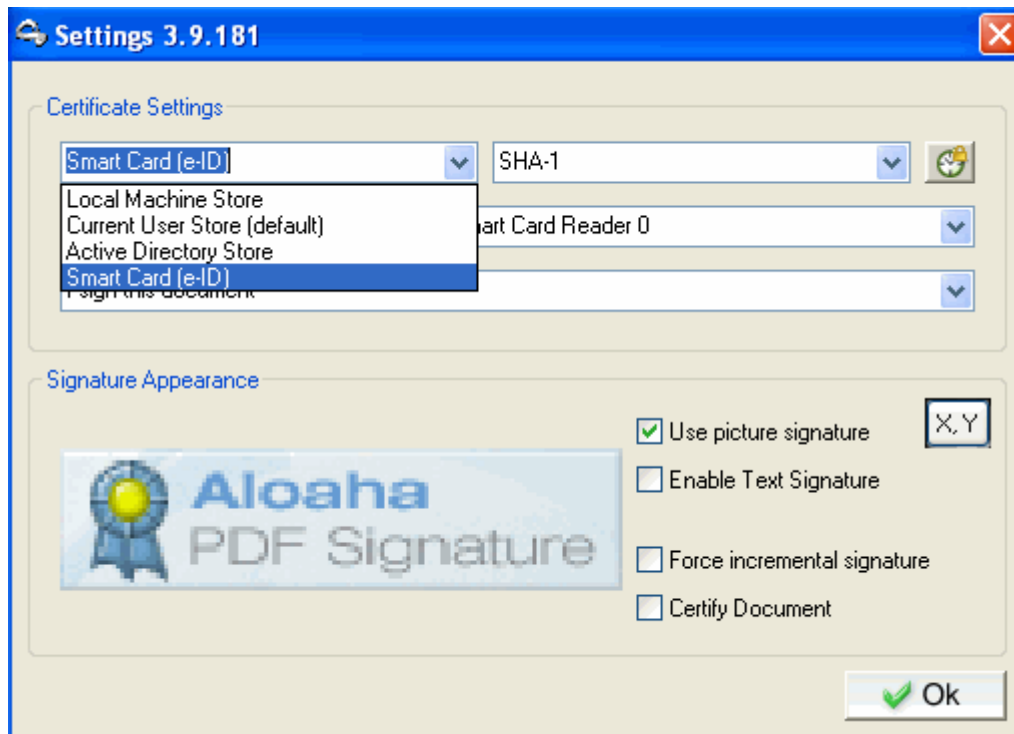


1. Certificate source

Here you can select between different kinds of certificates which you would like to use for signing of your PDF files.

To be available:

- **Local Machine Store**
All certificates which are associated to the computer are indicated in the certificate list.
- **Current User Store (default)**
All certificates which are associated to the actual user are indicated in the certificate list.
- **Active Directory certificates**
All certificates which are available in the Active Directory are indicated in the certificate list.
- **SmartCard (e-ID)**
All connected card readers are indicated in the certificate list.

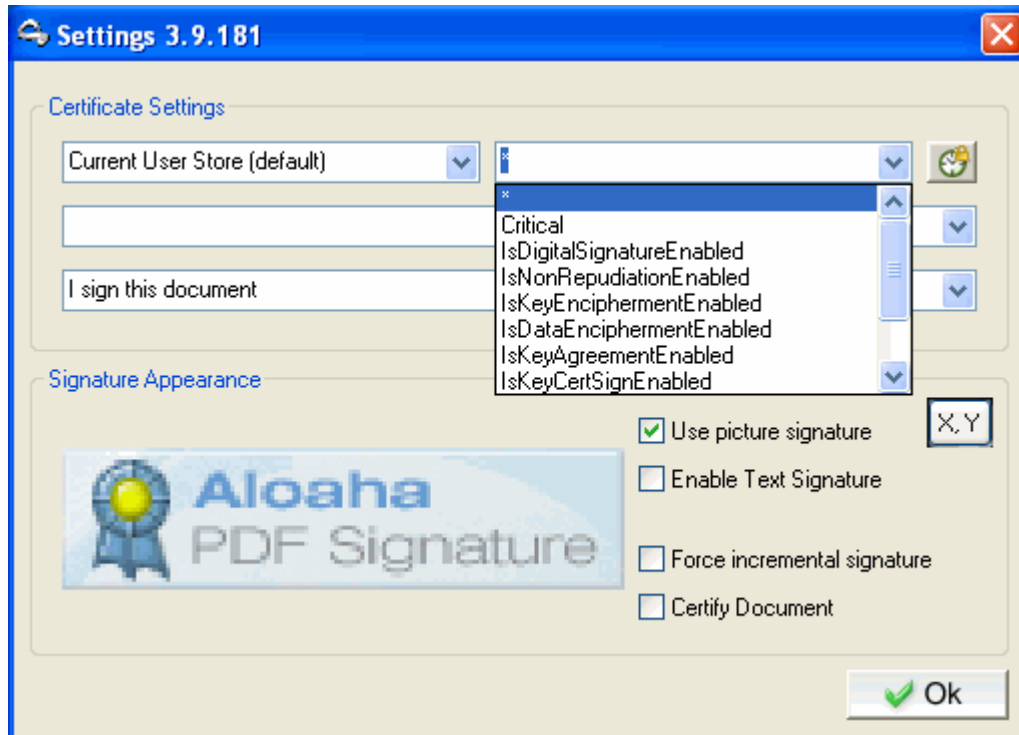


2. Certificate Filter


Here you can filter the certificate list of the indicated certificates after special attributes.

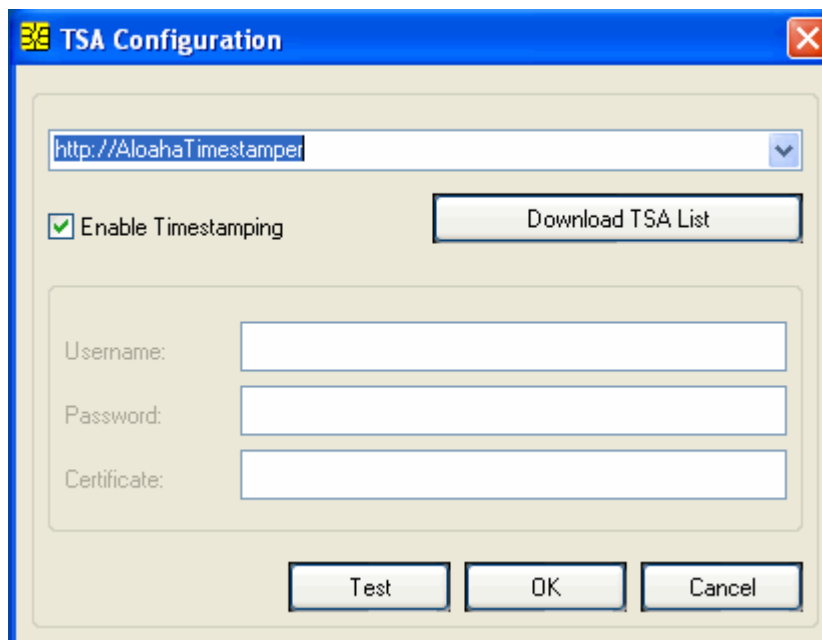
If as a certificate source "Smartcard" is selected, you can select between SHA-1 and SHA-256 as a signature algorithm.

SHA-256 is more safe and longer valid, but not all cards with electronic chip can serve this algorithm.



3. Time stamp settings

If you click on the watch icon  in the signature-configuration menu a new window opens for the time stamp settings:

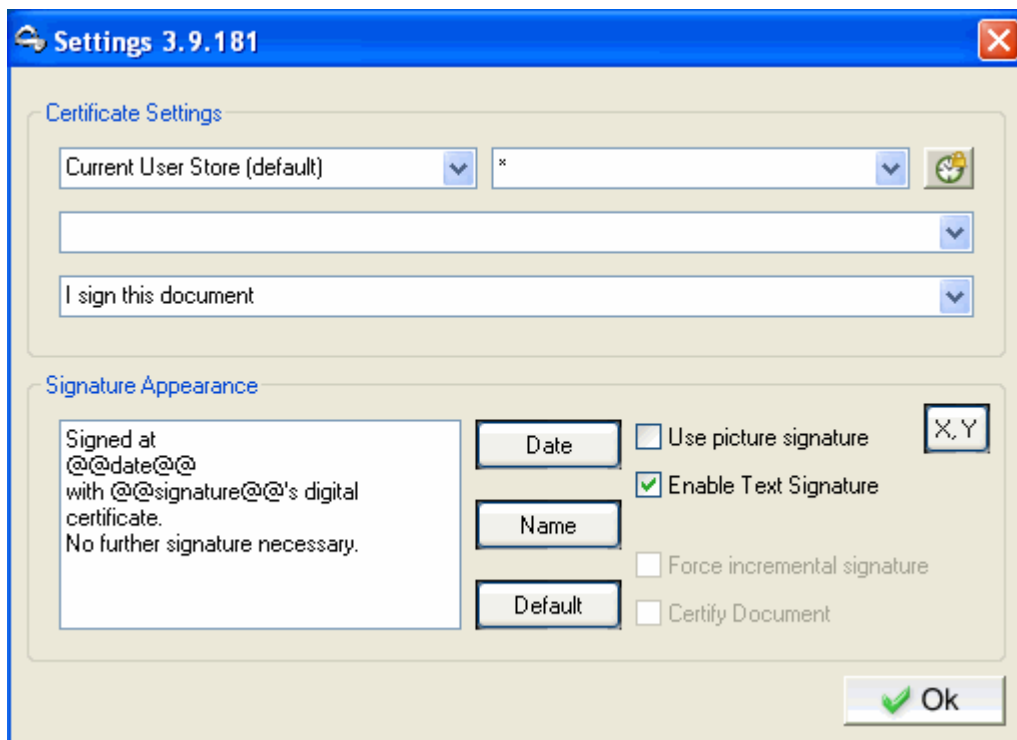


Here you can customise the settings for the integrated RFC 3161 compatible time stamp client.

In the upper field you select an available time stamp server. If the field is empty, you can download a list of possible time stamp servers by click into the button "Download TSA list" from the Aloaha web page. If you select <http://AloahaTimestamp.com>, the TimeStamp server is used. On this occasion, the local system time is taken as a basis for the time stamp.

4. Certificate select

This menu depends on the certificate source. If you select "current user store", you receive a listing of all user's certificates on your PC and can select the suitable certificate. Select as a certificate the SmartCard (e-ID), a listing of all installed SmartCard readers appears. The Aloaha Multisignator recognises independently the Smart-Card inserted in the card reader and reads the certificates of supported cards.

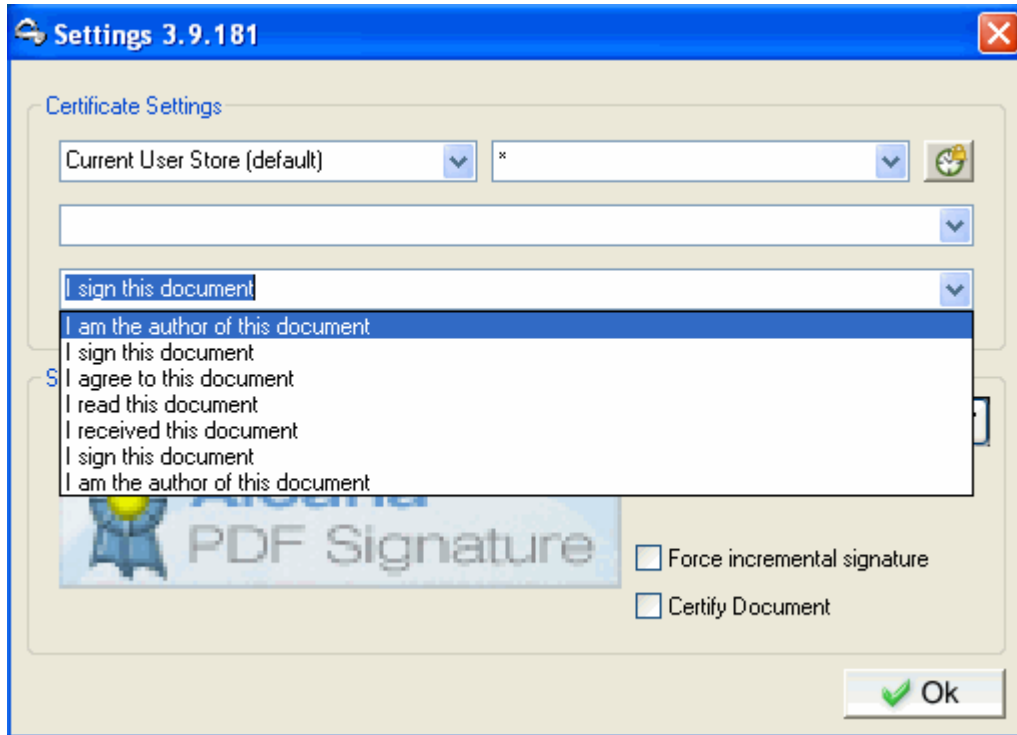


5. Purpose of the signature

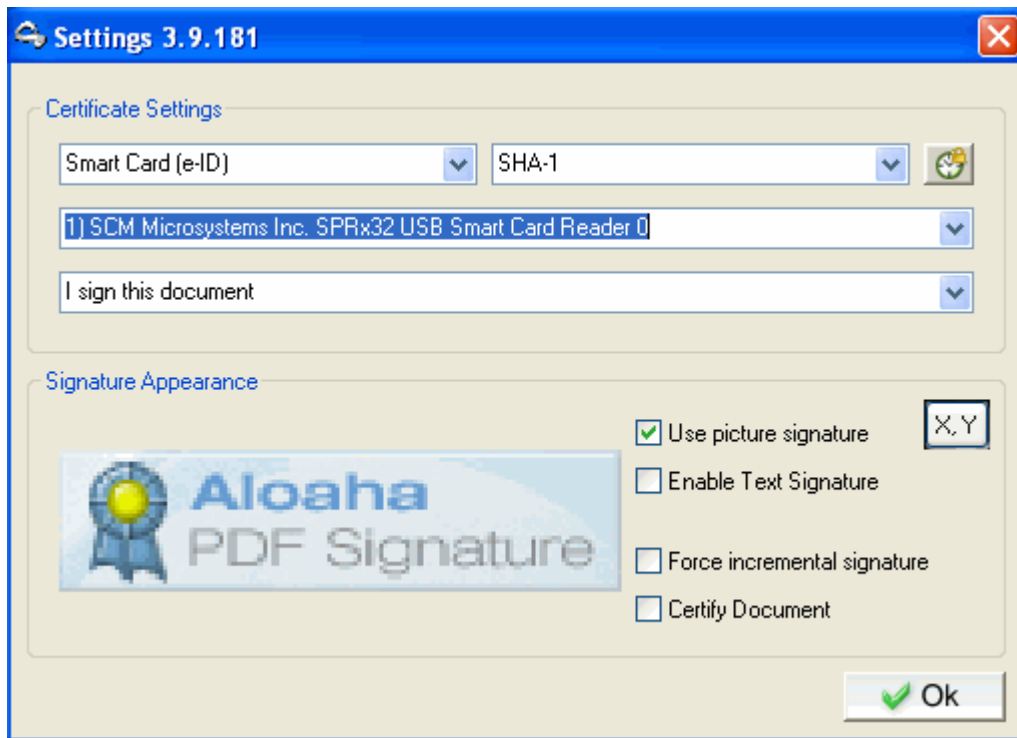
To be available:

- I am the author of this document
- I sign this document
- I agree to this document
- I read this document
- I received this document
-

Note: You can enter of course own text!



6. Appearance of the signature



Use Picture signature

If this option is selected, a picture is used in the PDF. **By click on the announcement of the topical signature picture you can load own images. This picture must be in the format JPG.**

Enable Text Signature

If the option "Enable Text Signature" is selected, the text entered is seated in the PDF. You have the possibility to paste a placeholder for date and name in the actual cursor position by click on "date" and "name". In the signature process this placeholder is replaced with the actual date and the name of the certificate owner.

Force incremental signature

Aloaha will sign the document incremental. Besides, the signature is attached thus to the document itself any time the original document allows to recover!

4.1.2 Automailer

Aloaha Automailer Config

Mail Server

Address: localhost Port: 25

User: Administrator Alias: Administrator

Password:

WebDAV

Defaults

eMail: me@localhost

Name:

Subject: Your PDF

Folder

Input Folder: C:\Aloaha Files\Test_1\

Output Folder: C:\Aloaha Files\Test_2\

Mailserver:

Here the following data has to be entered for your account:

Address:

Port:

Your **Username**

Your **Aliasname**, if he is not the same with than the username

The **Password** according to the username.

if necessary activate **WebDAV**, if you like to use a WebDAV server (as for example Microsoft Exchange or SharePoint server) for your documents.

Defaults:

eMail - E-mail address of the receiver

Name - Name of the receiver

Subject - Subject to the documents

Folder:

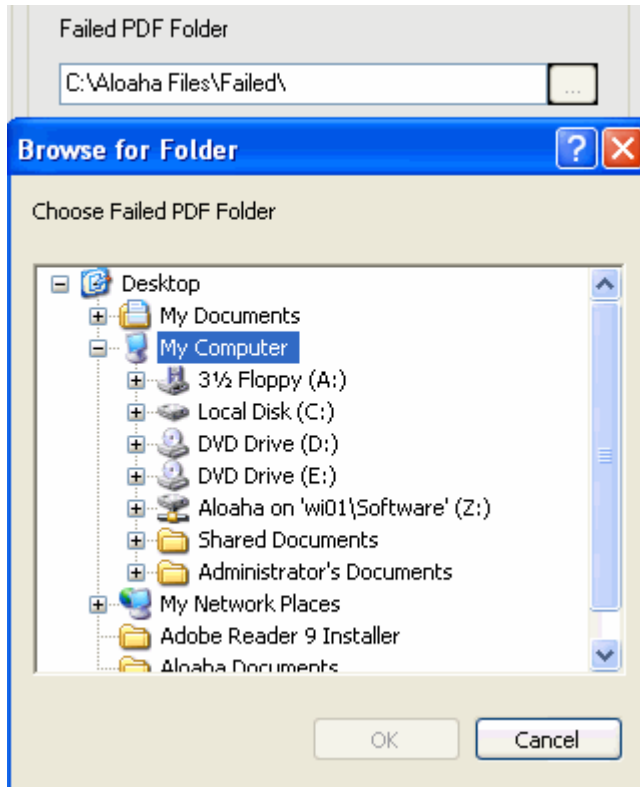
Input Folder - Is the directory from which Aloaha loads the documents to sign them.

Output Folder - Is the directory, were successfull signed files are removed to.

4.1.3 Global Settings

Failed PDF Folder:

Is the directory, where files with failed signature attempts are removed to.

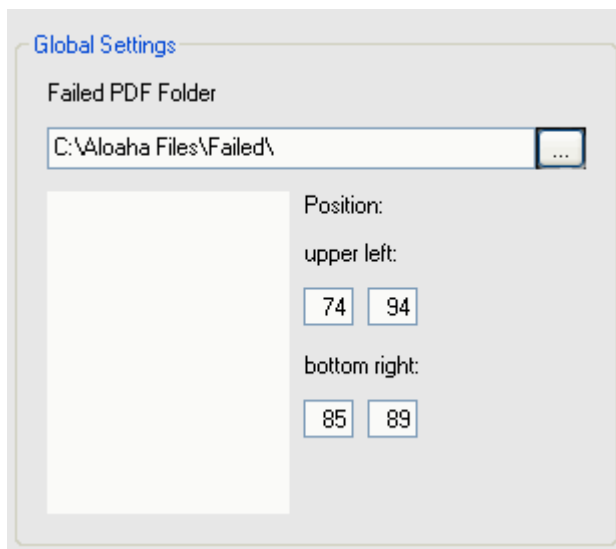


Position of the signature:

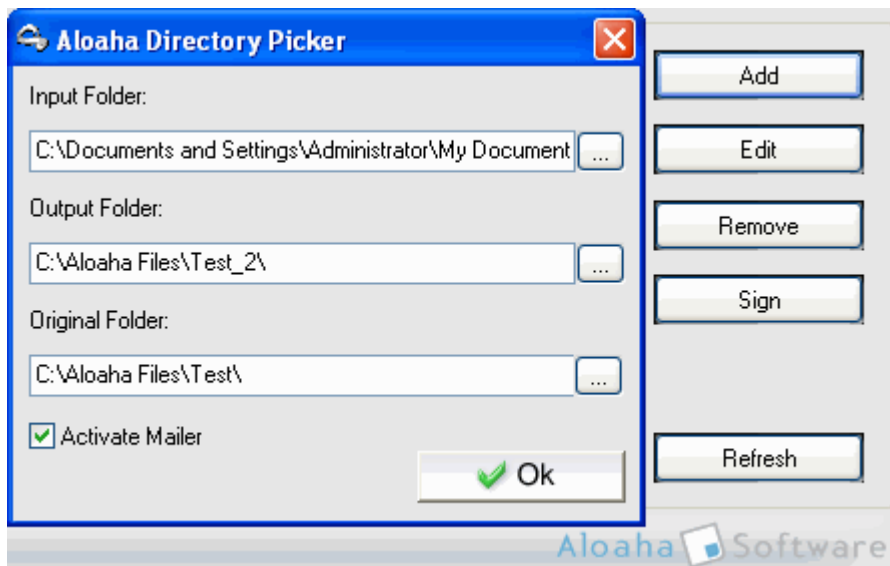
In four fields you give the position of the signature. It is always calculated in % of the page size. The co-ordinate system starts with 0% on the left bottom of the PDF. Under "on top of the left" you configure the left upper corner of the signature field.

Under "below on the right" you set the position of the lower right corner of the signature field. If in all fields 45 is entered, the field appears in the middle of the page.

Alternatively you can determine the position with the mouse. Click with the right mouse button to delete the actual choice. Now you start with the mouse the upper left corner of the position and click with the left mouse button. Then you start the right lower position and click again with the left mouse button.



4.1.4 Directory Picker



Input Folder:

Is the directory from which Aloaha loads the documents to sign them.

Output Folder:

Is the directory, where successful signed files are removed to.

Original Folder:

Hier werden nach erfolgter Signatur Originaldokumente abgelegt.

Add:

Opens the directory Picker to add other folders with documents to be signed.

Edit:

Opens the directory Picker to change if necessary the input folder, output folder or original folder.

Remove:

Deletes the directories laid out by you from the view.

Sign:

Requests you to the input of your PIN to sign upcoming documents.

Refresh:

Reloads the files to be signed from the suitable folders.

Activate Mailer:

If the option "Aktiviere Mailer" is activated, the Automailer configuration opens. Here you can customise or take over the suitable options (see also Automailer).

4.1.5 POP3 Settings

POP3 Settings

Generic

POP3 Frequency (seconds): 60 Max. POP3 Processes: 3

C:\Documents and Settings\Administrator\My Documents\pdf\Administrator\

Server: localhost Port: 110

User: Max Mustermann POP3 Frequency: 300

Password: Max. downloads: 10

Mail recipient: Hans Hansen CC Sender

Drop Folder: C:\Documents and Settings\Admini

Pop3 Frequency (seconds):

POP3 Frequency (seconds) defines in which time window the POP3 module is called.

Max. Pop3 Processes:

Max. POP3 Processes defines how many POP3 processes are launched.

Server:

Defines which Sever is used.

User:

Defines the user

Password:

Defines the assigned password

Mail recipient:

Specifies in who should receive messages

Drop Folder:

Specifies the input directory

Port:

Specifies which port should be used.

Pop3 Frequency:

POP3 Frequency defines how often a POP3 server is allowed to be put in the "connect" mode.

Max. downloads:

Max. downloads defines how many e-mails from will be downloaded.

CC Sender:

If "CC Sender" is activated, every e-mail is also routed to the sender.

5. Digitally Sign

PDF files electronically sign

With the Aloaha PDF Multisignator you can sign PDF files digitally. An electronic signature is supported after the default of the signature law (SigG) of the Federal Republic of Germany.

Legal electronic calculations can be created.

Calculations which are transmitted by fax or e-mail and/or are provided to download from the Internet (e.g., as a PDF document) and no "certified electronic signature" carry, display no calculation for the purposes of the section 14 to paragraph 3 sales tax law.

From Aloaha PDF Multisignator created digital signatures are embedded in the PDF document and can be checked with the Acrobat Reader up from version 6.

Digital Signature

A digital signature for the purposes of the law is „a seal generated with a private signature key to digital data which with the help of an accompanying public key, with a signature key certificate of a certification authority stock is, the owner of the signature key and the unadulterated quality of the data reveals“ (SigG.).

With the development of the digital signature the destination was traced to develop one of the personal signature equivalent signature method with which on electronic way data can be signed.

The main problem by transmission of electronic data is the manipulability. The problem could be eliminated only by electronic signature, because an unnoticed manipulation of data is no more possible.

Requirement is that the electronic signature is connected like a handwritten signature inseparably with the respective document. It can be seen by everybody, but only be changed by the signer itself. The signer can be identified and the signature makes every possible manipulation, like additional pranks or changing text passages, immediately recognizable.

By the certificate check can be proved that the signature was not faked and the certificate owner is real. except his name no personal data is revealed.

Legal regulations

Definitions of different kinds of the digital signature are found in the signature law (SigG) and in the order to the signature law (SigV). In it demands for the electronic signatures are as well displayed as Certification Service Provider (ZDA) were defined.

It is distinguished in **easy**, **advanced** and **certified** digital signatures. Every signature stands for a certain quality level. The higher valued the signature, the more meaning she has for the legal relations, and the greater is her functionality.

Only certified signatures fulfil the demands concerning electronic data just as the handwritten signature demands concerning data in paper form. They are admitted in court as an evidence.

The cryptographic algorithms admitted for certified electronic signatures are approved and published by the federal network agency. under www.bundesnetzagentur.de you find a list of all accredited Certification Service Provider (trust centres). There are also listed the products admitted for a certified electronic signature.

The requirements for a certified signature are given when:

- this can be associated exclusively to the signatory who admits unequivocal identification of the signatory
- with means is created which only the signatory controls
- makes every additional update of the signed data evident
- is based on a certified certificate

A certified certificate can only be issued by an accredited Certification Service Provider. Particularly strict demands concerning the security of the key creation and the organisation of the trust centre are valid. The observance of the legal instructions through the trust centre is in Germany also controlled by the federal network agency.

Public Key procedures

Digital signatures are based on asymmetrical Crypto systems and use a key pair which passes signature key of a private (confidential one) and public (not confidential).

The data which were encoded with one key can be opened again only with the other.

In order to sign the private key is used. The key is on the chip of the card and cannot be read out. The data to be processed are loaded on the chip, are encrypted or decrypted there and transmitted again back to the computer.

To use the private key, the right PIN which guarantees additional security is required. The signature can be only from the card owner, because only he is in possession of card and PIN.

The public key is integrated into a certificate and is available for everyone. This can also be retrieved by directory services via LDAP or HTTP. Of course he can also be dispatched by e-mail. To guarantee that the certificate and therefore the key was not faked, every certificate is signed by the publisher. Therefore checks up to themselves whether the certificate of a trustworthy place was published.

While checking the signature the public key of the receiver is used. The encrypted Hash value of the publisher is decrypted and compared to the Hash value of the document. If both values agree the document was not modified.

While signing a file a Hash value which is comparable with a fingerprint is formed. Two different documents can never have the same Hash value. The Hash value is encrypted under use of a key with a length of at least 1024 bits (depending on the used card) after the procedure RSA .

The encryption of the Hash value takes place on the card with electronic chip processor which can process smaller data volumes. Thus it is made sure that the private key does not leave the card. The encoded Hash value is sent back again to the computer and is seated in the document to be signed. Before the document could be signed the private key must be released by the right PIN (Personal Identification Number).

6. Language.ini

Aloaha Translation/Localisation Engine

Recent Builds of Aloaha localise/translate used strings fully automatic. String Tables are saved as ini files to allow the user to change strings himself or to localise into a new language without having to touch the Aloaha Code.

Translation Mechanism

- When Aloaha starts it looks for the language settings in language.ini. If that file does not exist Aloaha will ask
 - o HKCU\Software\Aloaha\language
 - o HKLM\Software\Aloaha\language
 - o The Operating System LanguageID
- Based on the LanguageID Aloaha will ask UserLanguage_<ID>.ini for the string translation. If that file does not contain the correct translation Aloaha will ask Language_<ID>.ini
- The file Language_<ID>.ini will be overwritten by every setup/upgrade. In case a user wants to modify strings it is suggested to use UserLanguage_<ID>.ini

language.ini

Section [Mapping] instructs to map one language to another. For example 410=409 would mean to use english (409) on italian (410) systems

Section [languageID] defines which ini files to use for the current mapping.

Translation Files

First Aloaha will ask UserLanguage_<ID> for the translation. If no translation is found it will ask Language_<ID> for the translation.

If a user wants to change strings it is advised to do the changes in UserLanguage_<ID>.ini since Language_<ID>.ini will be overwritten with every setup/upgrade.

It is also possible to set registry key HKLM\Software\Aloaha\pdf\WriteMissing to 1. In that case Aloaha will log all Translation Problems to MissedLanguage_<ID>.ini. This is very useful to find the strings to be translated for the new language/localisation.

7. Aloaha signature service

Aloaha Signature Service

The Aloaha Multisignator contains a dedicated Windows service to sign PDF files and to create PKCS#7 signatures. Access to the Aloaha Signature Service is given via command line interface (CLI).

The Aloaha Signature Service has been optimized for multisigning signature cards. For the PIN entry a card reader with display (Class III) should be used. It is also possible to use other card readers with PIN Pad if they have a way of signaling (for example with a beep) the start of the PIN Entry Process.

The use of the Aloaha Signature Service is quite easy. You need to use ACS.exe which can be found in the Aloaha installation folder (<program files>\wrocklage)

The command line syntax of ACS is very powerful. In case you do not find a required command, please do not hesitate to contact our support at: info@aloaha.com

More details of the Aloaha Command line Signer (ACS) can be found [here](#).

Info

With the command "info" you can display connected card readers, inserted cards and certificates on those cards. It is suggested to activate the command "info" every time you insert a card which is not known to the system.

Below you see a sample output of the info command:

```
C:\program files\wrocklage>acs -info
ReaderCount:4
0:OMNIKEY CardMan 3821 0
1:OMNIKEY CardMan 5x21 0
2:OMNIKEY CardMan 5x21-CL 0
3:SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0

Reader:0,0,-1,0,-1,-1
Reader:1,0,-1,0,-1,-1
1,0)aloaha_b564d11f02d43f43daf5ecc2a882d65d73276b25
1,1)aloaha_dac91f79cb9d3642e6b1b0a5c5f5f565ac9e7a4e

Reader:2,0,-1,0,-1,-1
Reader:3,0,-1,0,-1,-1
3,0)aloaha_19bc2dd8432df733ff381722bcd183da2e1fff2c
3,1)aloaha_6e02cc5647e15114c3f03093d04ef4626dfd7199
```

The above sample output lists 4 connected card readers. Reader 1 and 3 contain a smartcard with two certificates each.

Open

The Aloaha Signature Service is specialized for multisigning signature cards. Such cards do not require a PIN for every crypto operation. For example it is possible to "open" a card for a number of signatures or for a specific time.

```
C:\program files\wrocklage>acs -open:3,0 -maxtime:10 -maxsignatures:10
0:3,0,1,9,10|SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0,7148
```

The numbers in the answer have the following meaning:

```
0: return value OK
3,0: reader 3, certificate 0
1,9: 1 file signed, 9 signatures left
(1 signature of 00 bytes is required to open the card)
10: 10 minutes left
7148: process ID of signature service
```

Sign PDF

With the command `-oop -x:p` ACS submits a signature job to the Aloaha Service Signer. The option `-o` instructs ACS to wait until the signature has been applied and to save the signed file into the file defined by `-o`.

```
C:\program files\wrocklage>acs -oop -x:p -u:3,0 -sha2 -i:c:\test.pdf
-o:c:\signedpdf.pdf
Signed file: c:\signedpdf.pdf
```

- oop -x:p instructs the service to apply a PDF signature
- sha2 forces are SHA256 Signature
- u:3,0 defines to use reader 3, certificate 0
- i define input file
- o wait and save to output file

Create PKCS#7

```
C:\program files\wrocklage>acs -oop -x:a -u:3,0 -i:c:\test.pdf
-o:c:\signedpdf.p7m
Signed file: c:\signedpdf.p7m
```

```
C:\program files\wrocklage>acs -oop -x:d -u:3,0 -i:c:\test.pdf
-o:c:\signedpdf.p7s
Signed file: c:\signedpdf.p7s
```

- oop -x:a: create attached PKCS#7 signature
- oop -x:d: create detached PKCS#7 signature
- u:3,0: use card reader 3, certificate 0
- i: inputfile
- o:outputfile

Reader status

The command `reader status` can be used to check how many signatures or time is left.

```
C:\program files\wrocklage>acs -readerstatus:3
0:3,0,2,8,9|SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0,7148

0: OK
3,0: Reader 3, Certificate 0 open
2: two signatures applied
8: 8 signatures left
9: 9 minutes left
7148: process ID of signature service
```

Close

The `close` command is being used to close an open reader/card

```
C:\program files\wrocklage>acs -close:3,0
0:OK
```

8. Aloaha Commandline Signator

You will find information to the Aloaha Commandline Signator here:

Aloaha Commandline Signator EN

9. CryptoAPI

The Cryptographic Application Programming Interface (also known variously as Crypto API, Microsoft Cryptography API, or simply CAPI) is an application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt or sign the data.

Crypto API supports both public-key and symmetric key cryptography. It includes functionality for encrypting and decrypting data and for authentication using digital certificates..

Crypto API works hand in hand with the Aloaha CSP installed on the machine. CSPs are the modules that do the actual work of encoding and decoding data by performing the cryptographic functions. They are also responsible for the communication between Smartcards and the Windows Operating System

10. Technical Informations

Type of the signature

PDF Signature (Adobe standard)
Certify PDF Document (Adobe standard)
EML Signature (signing of PDF attachments of mail files)
PKCS#7 detached signature
PKCS#7 enveloped signature
Timestamping (RFC 3161)
S-MIME V3 (signed e-mail)

Aloaha Commandline Signer (ACS) included

Batch signature

Software certificates
Qualified Smartcard supported
Multiple smartcards can be used for higher performance

Archiving

Signed PDF Files can be easily archived by your existing archive

Management

Configuration using a comfortable Windows User Interface

Signature Checks

Central automated checking of signatures
Certificate Revocation List (CRL) checks.
Online Certificate Status Protocol (OSCP) checks
Result can be archived

Compatibility

Easy integration in existing infrastructure because of the hotfolder architecture

Integration

SMTP (e-mail System)
WebDAV
Hotfolder (Files are read from a special folder of the harddisk)
POP3 downloader

Secure Pin Caching

System requirements

Windows 2000/3/8, Windows XP SP3, Windows Vista.
No software from third party vendors required
Uses the infrastructure of every smartcard vendor (e.g. CA, certificates, CRL, OSCP Responder, Smartcards, cardreader ets.)

Currently supported smartcards (as of March 2008):

SECCOS Cards (as Sparkassen Card), TCOS 3 (TeleSec), D-Trust, German Health Professional Card (HBA), German Health Insurance Card (eGK), Belpic E-ID, a-sign premium (Austrian Bürgerkarte), TC Trustcenter QSIGN, GS1 Switzerland, SiCrypt based cards and Italian Infocamere and Actalis Card.

If you have further questions or you do not find your smart card in the list of supported cards please do not hesitate to contact us! We are continuously adding support for new smartcards to our system.

Standards Compliance

Aloaha helps organizations to comply with rules and regulations pertaining to the use of Digital Signature and electronic transactions like:

- EU Directive for Electronic Signatures
- Sarbanes-Oxley Act (SOX)
- Uniform Electronic Transactions Act (UETA)
- US Electronic Signatures in Global and National Commerce Act (E-Sign)
- Government Paperwork Elimination Act (GPEA)
- Health Insurance Portability and Accountability Act (HIPAA)

11. FAQ Multisignator

How can I define to which email address Aloaha delivers the signed document?

There are two possibilities:

1. You can use the Aloaha embedded commands such as emailto. Aloaha will read commands from the document itself. The command emailto defines the recipient(s)
2. You can create subdirectories in your configured inputfolder. If the name of the subdirectory is an email address Aloaha will use that as emailto. Please restart the Multisignator after creating new subdirectories.

A combination of 1 and 2 is possible. For example you can use the subdirectory functionality to define an email to which is always used. Additional recipients are then defined via 1 (embedded commands)

Is it possible to sign emails?

With the Aloaha Multisignator it is possible to sign PDF documents embedded in an email. If you drop .eml files in one of the configured input folders Aloaha will digitally sign all PDF documents embedded in that eml file.

It is also possible to use the inbuilt POP3 downloader to download emails from an external POP3 mailbox and drop them into the dropfolder.

Can Aloaha send out eml files by SMTP?

Yes, if mailing is enabled Aloaha will automatically send out the email via the configured SMTP Server.

In case the input directory has the form of an email address Aloaha will automatically rewrite the recipient address so that the recipient address matches the folder name.

Should the email delivery via SMTP fail Aloaha will submit the email to the local IIS directory. In case even this fails the eml.file will be saved in the define failed diretory.

Can I load different profiles?

Yes, per default Aloaha saves the settings in the file MultiSignator.ini. Per commandline you can open any other configuration file.

For example: AloahaMultiSignator.exe; AlternativeSettings.ini

Can I configure different certificates per dropfolder?

Yes, after you configured your folder just right click on them and choose settings such as POP3, Signature, etc.

How do I configure the POP3 downloader?

The POP3 downloader will be configured per hotfolder. That means you need to right click on the configured hotfolder and choose POP3 to configure the POP3 downloader for that folder.

I do not understand the options of the POP3 downloader dialog.

POP3Frequency (seconds) defines how often the POP3 Module will be called.

Max. POP3 Processes will define how many POP3 Processes will be launched.

POP3Frequency defines how frequent a POP3 Server is allowed to be contacted.

Max Downloads defines how many emails will be downloaded from the mailbox.

Mail Recipient defines the target address. To this recipient the documents will be mailed.

If CC Sender is activated every email will be cc'ed to the original sender.

I configured the POP3 downloader but no emails will be downloaded.

To save performance Aloaha will call the POP3 Module ONLY if all drop folder are empty.

How can I make sure that no emails will be lost in case I have problems with my network connectivity?

Per default Aloaha delivers the email per SMTP. Should that fail due to network problems Aloaha will try to submit the mails to the local IIS pickup directory. As soon the network is back the IIS will deliver the mails. For this reason it is suggested (but not required) to operate Aloaha on a machine with a correctly configured IIS SMTP Server.

How can I find out why Aloaha cannot download mails from my mailbox?

Aloaha will write the last problem to the file Multisignator.ini.

Is it possible to upload the signed documents to a web based document library?

Yes, just configure the URL of the library as targetfolder. Aloaha will automatically upload the signed documents.

Is it possible to sign documents directly at the command prompt?

Yes, but you would need the Aloaha Commandline Signer (CLS). Please have a look at <http://www.aloaha.com/software-development/aloaha-commandline-signer-cls.php>

Does it give a log file respectively how can I sign large files (200-800 MB)?

PDF files are loaded and standardised technically into the store while signing. Such large files fail.

There is a Registry key which disables the properties:

```
HKLM\Software\Aloaha\pdf\minSignature = 1
```

If you set this key it should work.

Should you have further questions please do not hesitate to contact us

Index

- A -

- Activate Mailer 20
- Add 20
- Aloaha Commandline Signer (Englisch) 27
- Aloaha signature service 25
- Aloaha Translation/Localisation Engine 24
- Appearance of the signature 12

- C -

- CC Sender 21
- Certificate select 12
- Certificate source 12
- Configuration 10
- CryptoAPI 27

- D -

- Defaults 18
- Digital Signature 12, 22
- Digitally Sign 22
- Directory Picker 20
- Drop Folder 21

- E -

- Edit 20

- F -

- Failed PDF Folder 19
- FAQ Multisignator 30
- Folder 18

- I -

- Input Folder 20
- Installation 7, 8
- Introduction 4

- K -

- Kind of the certificate 12

- L -

- Language.ini 24
- Legal regulations 22

- M -

- Mail recipient 21
- Mailserver 18
- Max. downloads 21
- Max. Pop3 Processes 21

- O -

- Original Folder 20
- Output Folder 20

- P -

- Password 21
- Pop3 Frequency 21
- Pop3 Frequency (seconds) 21
- POP3 Settings 21
- Port 21
- Position of the signature 19
- Preparation 5
- Public Key procedures 22
- Purpose of the signature 12

- R -

- Refresh 20
- Remove 20

- S -

- Server 21
- Settings 11
- Sign 20
- System requirements 7

- T -

- Technical Informations 28
- Time stamp settings 12
- Translation Files 24
- Translation Mechanism 24

- U -

- Usage 5
- User 21