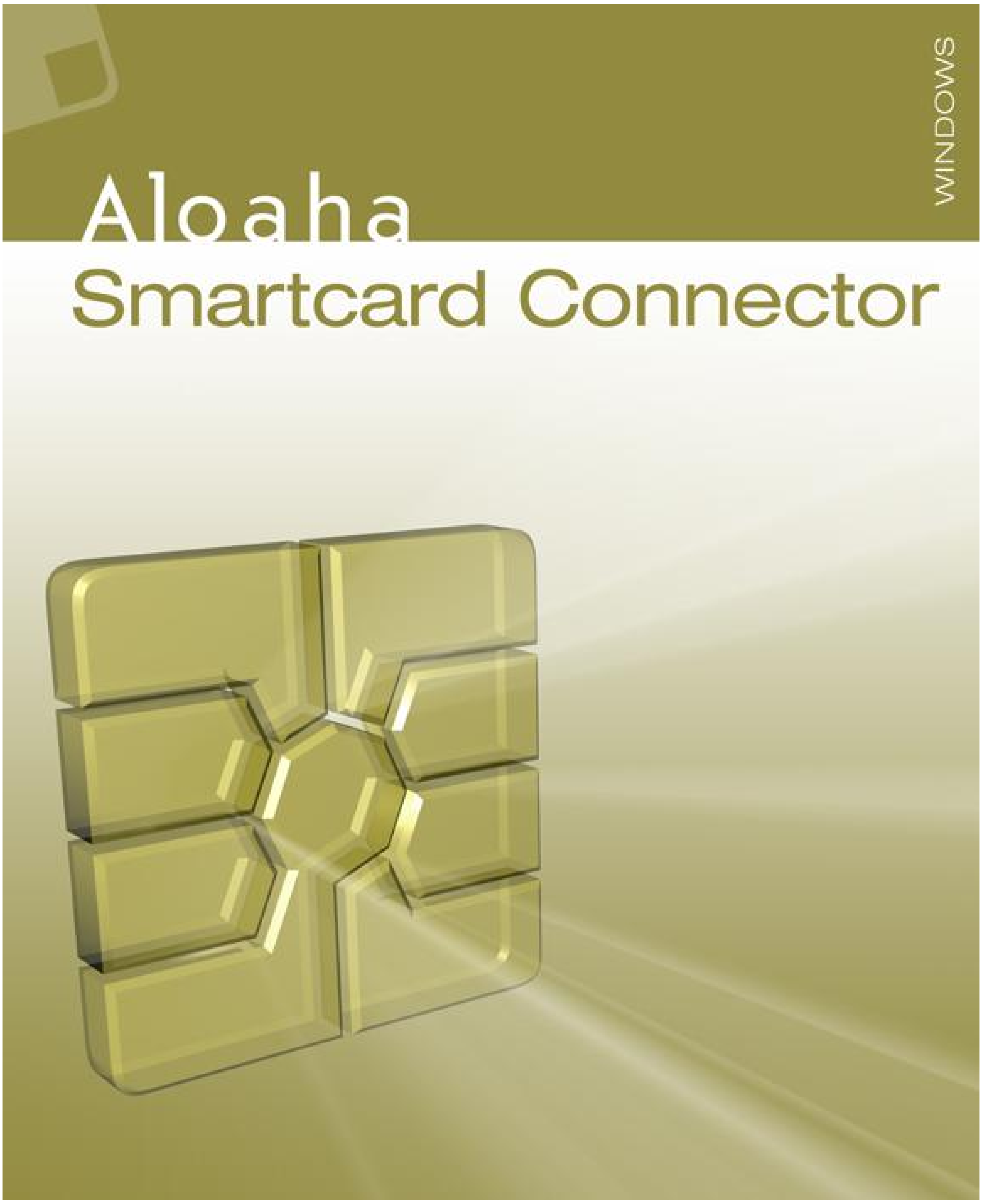


# Aloaha Cardconnector

# Aloaha Cardconnector

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: Februar 2010

# Table of Contents

# 1. Introduction

## Aloaha Smart Card Connector

Aloahas´s Smart Card Connector, including a Microsoft approved CSP (Cryptographic Service Provider) and a PKCS #11, provides native, plug & play security enhancement to Microsoft Windows operating systems and Applications.

The Aloaha Smartcard Middleware supports various Smart Cards such as the German Health Insurance Card, Health Professional Card, Belgium e-ID (Belpic), Swiss GS1, Italian Infocamere, SagemOrga Micardo, CardOS, Sicrypt, Mifare 4k and more...

**Integration of the Aloaha Card Connector is unbelievably simple and quick. The system is operable after a 2-minute installation process.**

- No complicated configurations.
- No special personalization processes.
- No headaches.
- Small Footprint

Once the CSP is installed, the Aloaha supported Smart Cards become integrated into your Windows environment, providing you with a highly secured, mobile, certificate storage solution.

With the certificates stored on your Smart Card, you can easily improve your Windows Security in many ways.

**Here are some examples:**

- Email protection (encrypt and sign)
- Office document protection (encrypt and sign)
- File and directories protection (certificate-based EFS / NTFS encryption)
- Client authenticated communication (SSL/HTTPS)
- Digitally sign electronic forms (PDF, Info Path, Share Point)
- VPN Authentication like OpenVPN
- Windows Logon (Active Directory)

**Aloaha Features:**

- Signed and verified by Microsoft
- Windows 2000 / XP / Vista / 7 compliant
- Windows 2000 / 2003 / 2008 server compliant
- Qualified Signature Cards supported
- PKCS #11 module included
- Plug & Play

**Supported Standards:**

- ISO 7816
- PC/SC
- Secure Pin Pad via PC/SC II
- Mifare
- Microsoft CSP
- Remote CSP for Card Sharing
- PKCS#11
- PKI

**Supported Algorithms:**

- RSA 1024 – 2048
- Elliptic Curves (ECC)
- DES & Triple-DES
- RC2 & RC4
- MD5, SHA-1 & SHA-2

# 2. Installation

To install the Aloaha Cardconnector please download the installation package from http://www.aloaha.com/download/cardconnector.zip

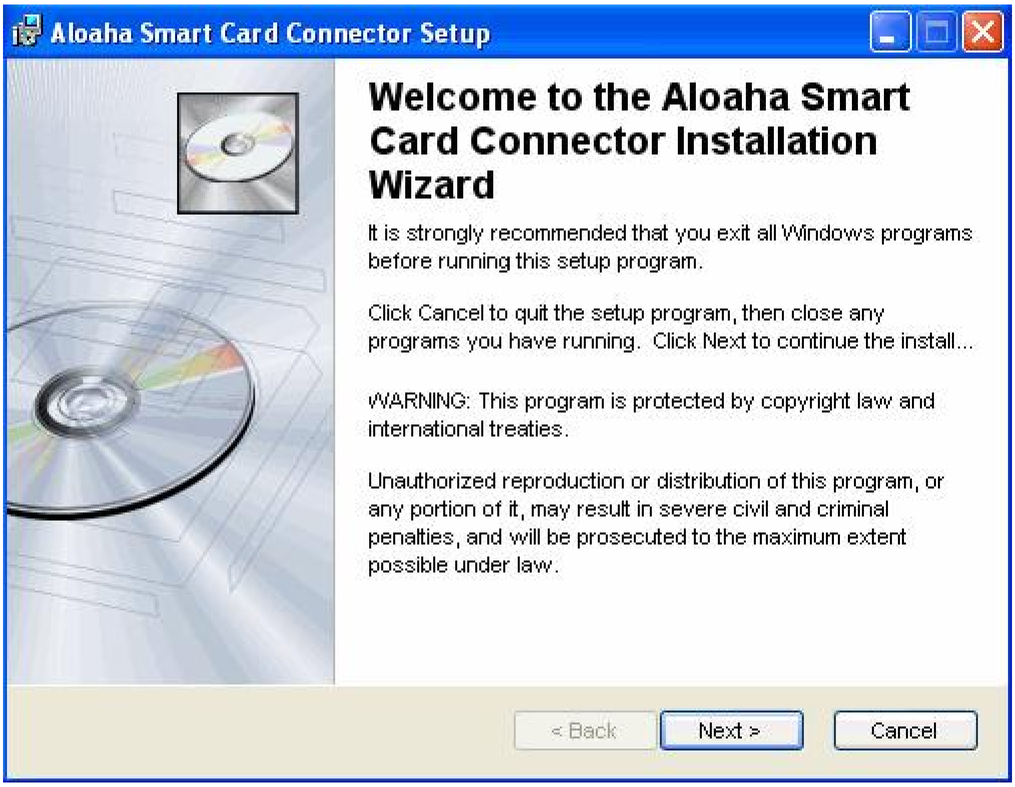
**Installation Requirements:**

- Windows 2000/3/8
- Windows XP (Service Pack 3 suggested but not required)
- Windows Vista
- Windows 7

The installation package contains a file cardconnector.exe. Please start that file with a double click.

Now the Windows Installer will start and will ask for the installation language.
The program language can later be changed in the Windows Registry - **`HKCU\Software\Aloaha\pdf\language`**

After you choose your language the setup will start.



Welcome to the Aloaha Smart Card Connector Installation Wizard

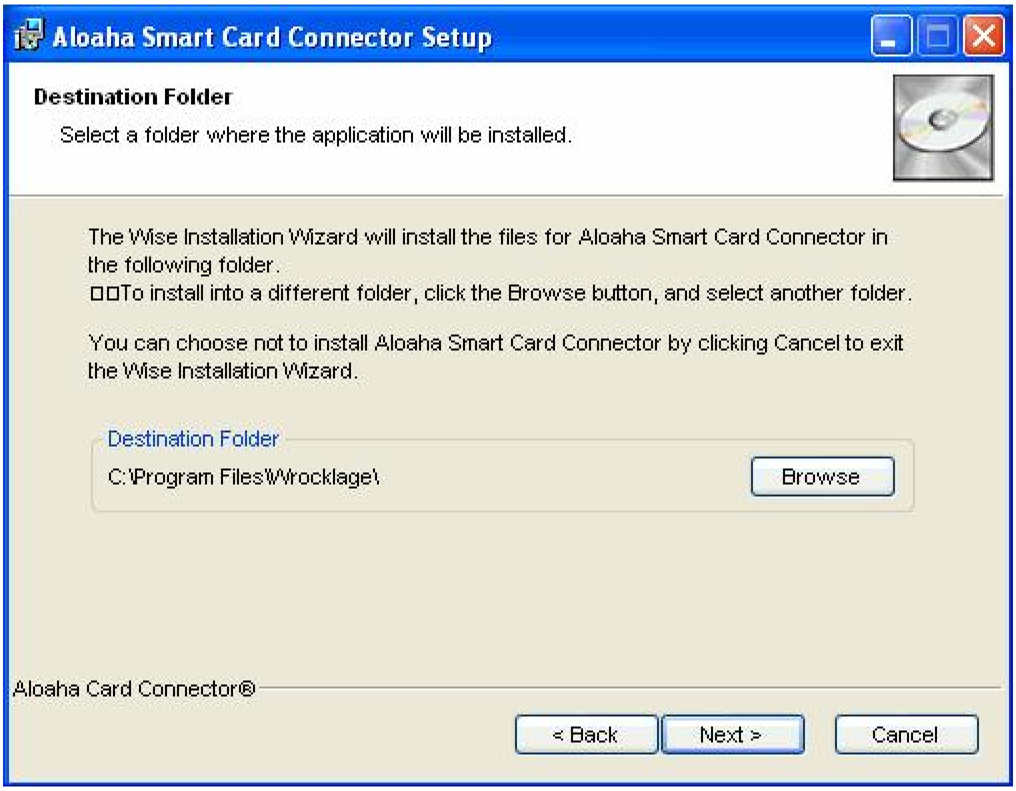
It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the install...

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Setup will ask for the installation directory before it begins to install the product. It is suggested to install all Aloaha products into the same directory.



Aloaha Smart Card Connector Setup

**Destination Folder**

Select a folder where the application will be installed.

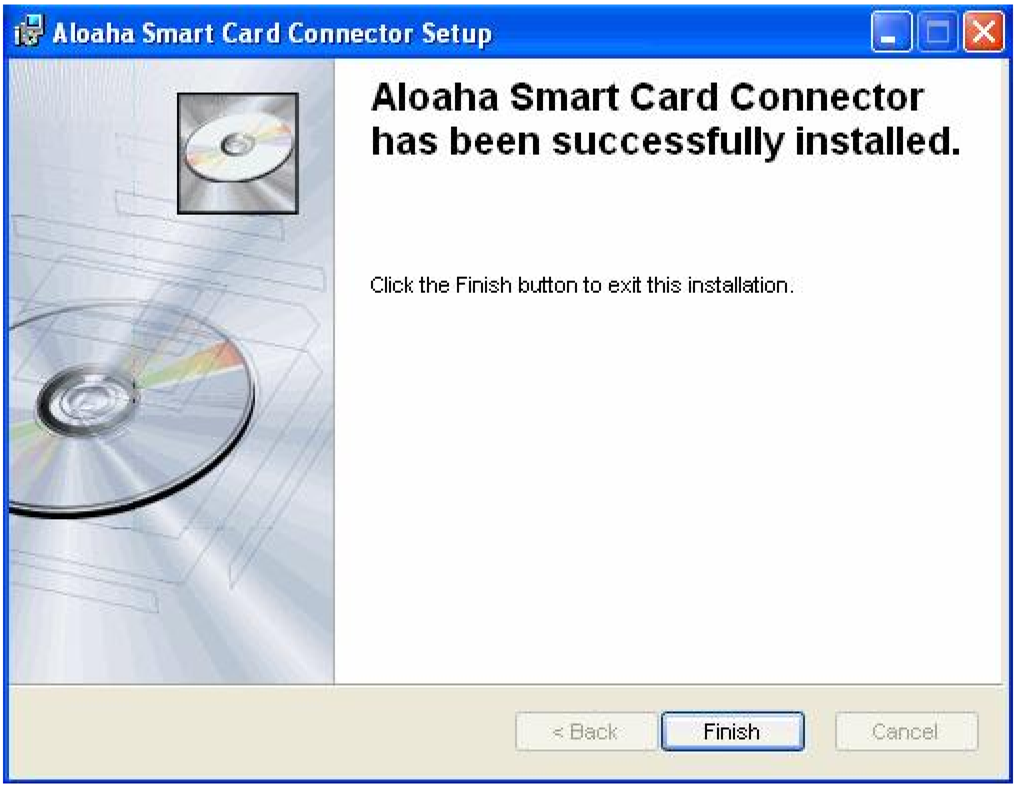
The Wise Installation Wizard will install the files for Aloaha Smart Card Connector in the following folder.
□□To install into a different folder, click the Browse button, and select another folder.

You can choose not to install Aloaha Smart Card Connector by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder

C:\Program Files\Wrocklage\

As soon the setup is ready please click finish.



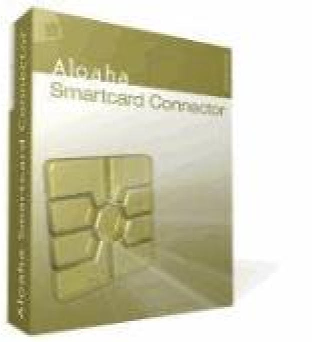
Aloaha Smart Card Connector Setup

**Aloaha Smart Card Connector has been successfully installed.**

Click the Finish button to exit this installation.

You will now see a small Smartcard icon in your system tray.

# 3. Usage

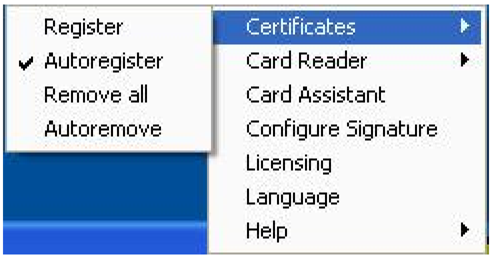


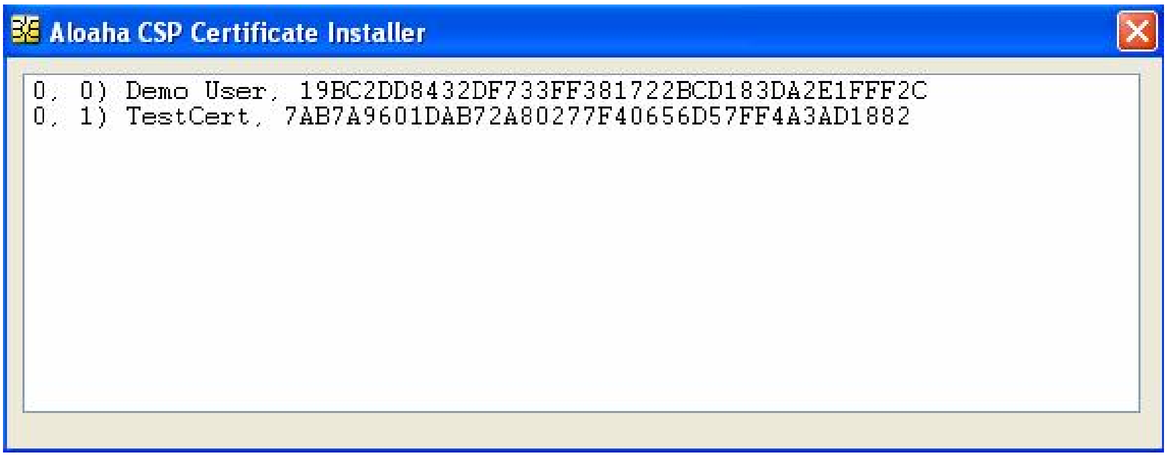
The Aloaha Cardconnector includes a Microsoft approved Cryptographic Service Provider (CSP) and a **PKCS #11** Library (aloaha_pkcs11.dll in system32).

The advantage of a CSP is that it installs the certificates transparent in the Windows certificate store of the currently logged on user. It is also called Current User Store.
When the CSP registers a certificate in the current user store is stores the certificate itself in the store. Instead of the private key it will place a link to the CSP in charge for that private key.

To see a flash based usage video please follow this link:
[http://www.aloaha.com/movies/register.htm](http://www.aloaha.com/movies/register.htm)

Per default Aloaha registers certificates automatically as soon a Smartcard has been inserted into the card reader. It is also possible to register manual. Just right click on the Aloaha system tray icon and click on Register. A window will be opened which lists all the certificates available in all connected card reader.





```
0, 0) Demo User, 19BC2DD8432DF733FF381722BCD183DA2E1FFF2C
0, 1) TestCert, 7AB7A9601DAB72A80277F40656D57FF4A3AD1882
```

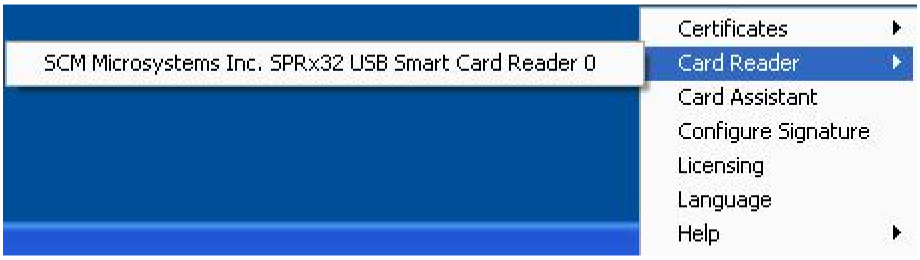
The first number in the list indicates the card reader number. Counting starts at 0. The screenshot above shows the certificates of the cards in the second and third connected reader. There is also a second number after the comma. That number indicates the certificate type.

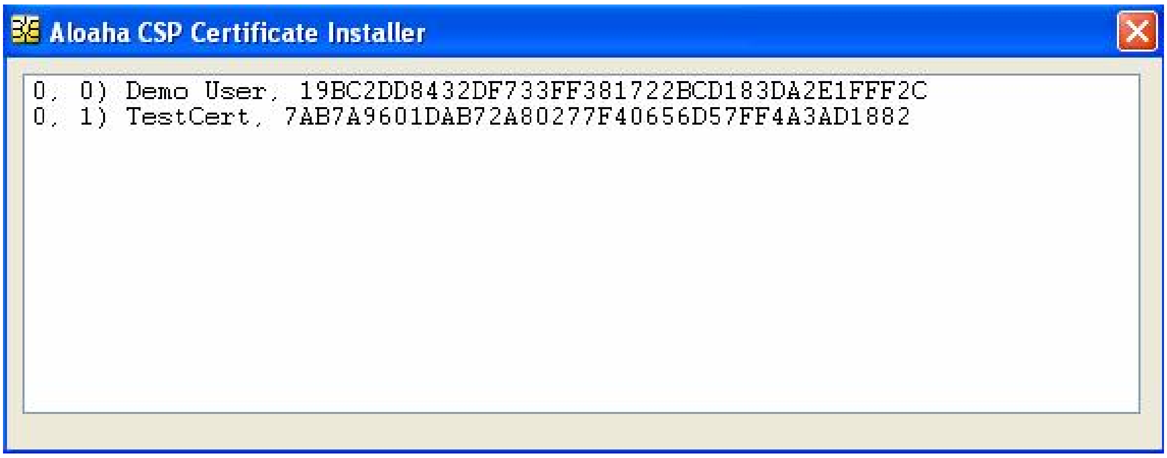
Type 0 = Signature certificate,
Type 1 = Authentication certificate,
Type 2 = Encryption certificate.

If a card holds only one certificate it will be shown as type 1.

To remove all Aloaha registered certificates from the current user store just click **Remove all**. If **Autoremove** is enabled all Aloaha registered certificates will be removed as soon all smartcards are removed from the connected readers.

In some cases there are many card readers connected to a system. To enumerate all certificates in all reader might take some time. In that case you can choose directly the reader itself as shown in the screenshot below. In that case Aloaha will enumerate only the certificates of the card in the chosen reader.





```
0, 0) Demo User, 19BC2DD8432DF733FF381722BCD183DA2E1FFF2C
0, 1) TestCert, 7AB7A9601DAB72A80277F40656D57FF4A3AD1882
```

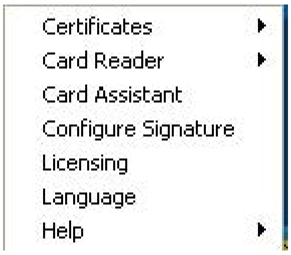
You can now right click on a certificate to display it or just double click to register it in the current user store.

**Manual registration has two advantages:**

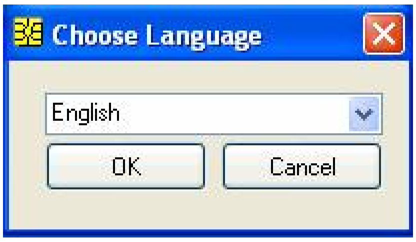
1. If the issuing root certificate is not available on the system Aloaha will try to download it from the Aloaha Website
2. The registered certificate will be automatically configured as the default signing certificate.

## 3.1 Language

Thus you change the Userlanguage regardless of the systemlanguage of the operating system. The userlanguage can be changed about the Windows top menu or the Traymenu.



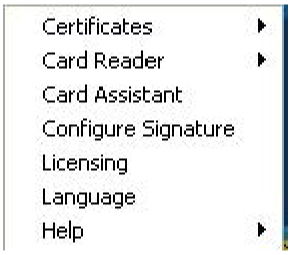
To be available:
English
German
Italian
Dutch



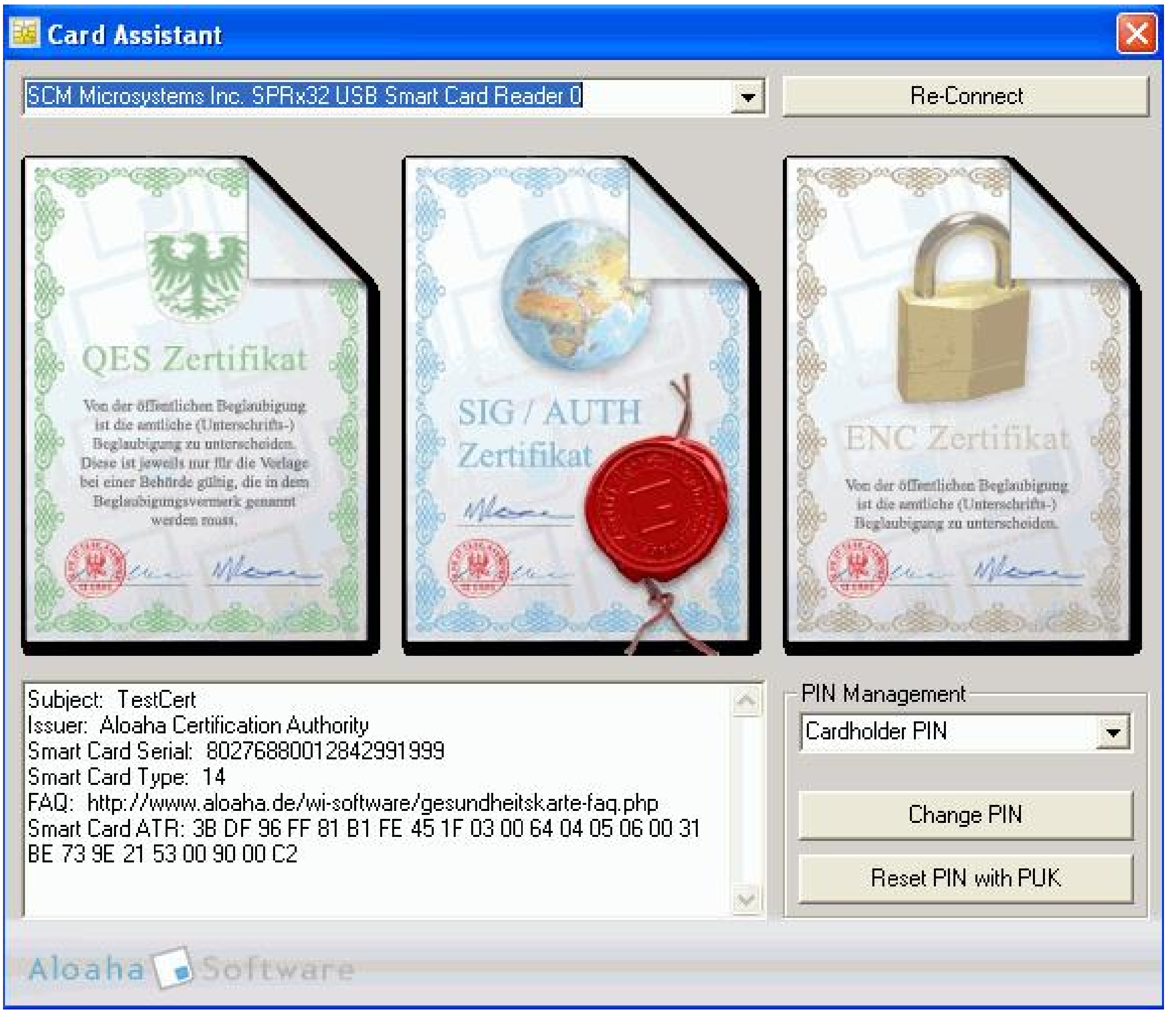
After you have changed the language, you are requested to restart the program.

## 3.2 Card Assistant

The "Aloaha Card Assistant" can be started via the Aloaha Cardconnector System Tray Icon or the Startmenu of Windows.

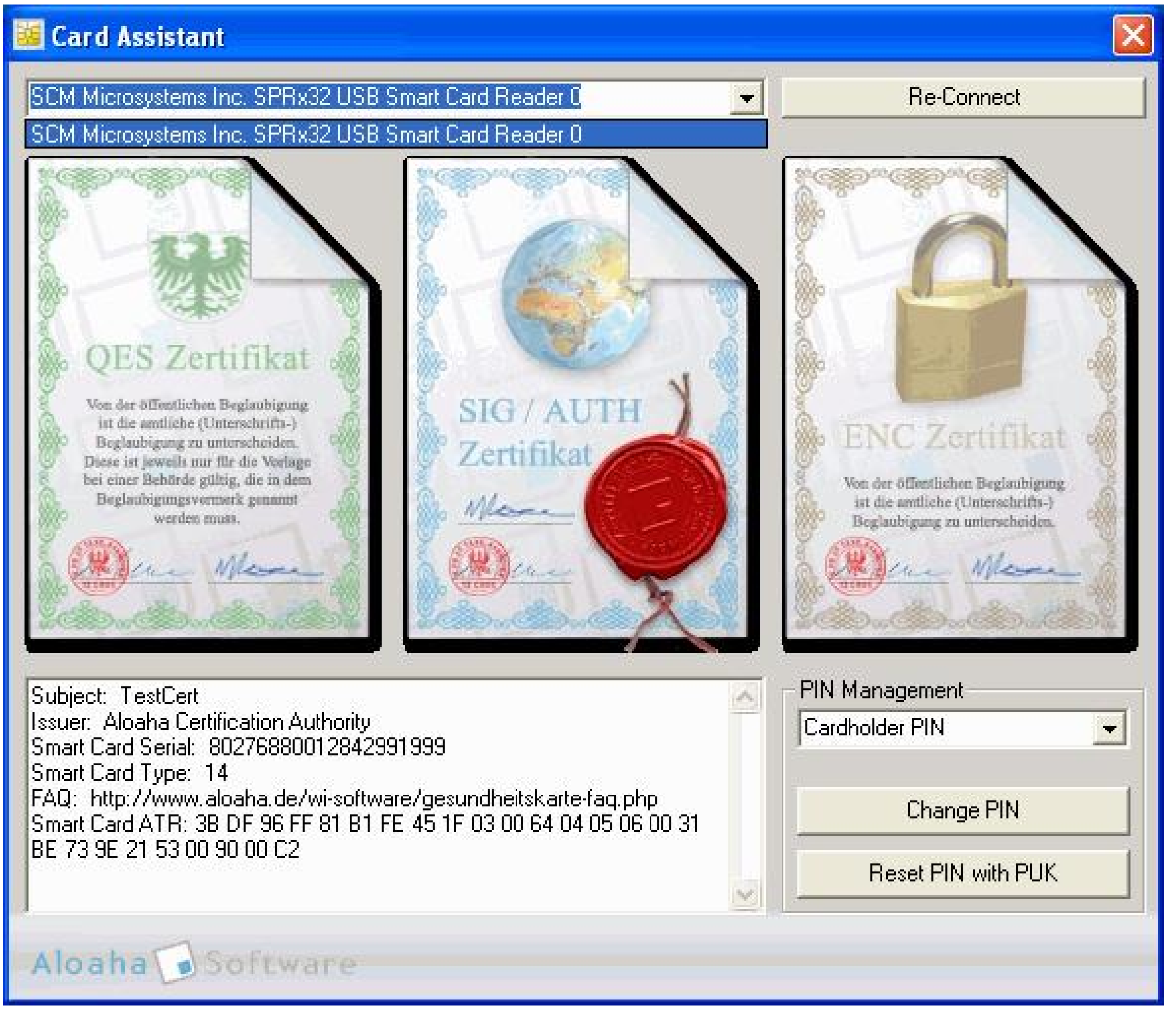


Depending on the type of card used it is able to change the PINs or unblock PINs with the PUK.


Card Assistant
SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0
Re-Connect
QES Zertifikat
Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden. Diese ist jeweils nur für die Vorlage bei einer Behörde gültig, die in dem Beglaubigungsvermerk genannt werden muss.
SIG / AUTH Zertifikat
ENC Zertifikat
Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden.
PIN Management
Cardholder PIN
Change PIN
Reset PIN with PUK
Aloaha Software

Subject: TestCert
Issuer: Aloaha Certification Authority
Smart Card Serial: 80276880012842991999
Smart Card Type: 14
FAQ: http://www.aloaha.de/wi-software/gesundheitskarte-faq.php
Smart Card ATR: 3B DF 96 FF 81 B1 FE 45 1F 03 00 64 04 05 06 00 31
BE 73 9E 21 53 00 90 00 C2

By opening the select menu all available card reader in the system are able to be selected.



Subject: TestCert
Issuer: Aloaha Certification Authority
Smart Card Serial: 80276880012842991999
Smart Card Type: 14
FAQ: http://www.aloaha.de/wi-software/gesundheitskarte-faq.php
Smart Card ATR: 3B DF 96 FF 81 B1 FE 45 1F 03 00 64 04 05 06 00 31 BE 73 9E 21 53 00 90 00 C2

Depending on the card type PINs or PINs with PUK are able to be changed or unlocked.

## 3.3 Digitally sign

### PDF files electronically sign

With the Aloaha CardConnector 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 Saver 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

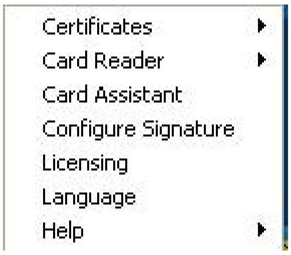
A certified certificate can only be issued by an accredited Certification Service Provider. Particularly strict demands concerning the security of the key creation and the organisation of the trust centre are valid. The observance of the legal instructions through the trust centre is in Germany also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

## Public Key procedures

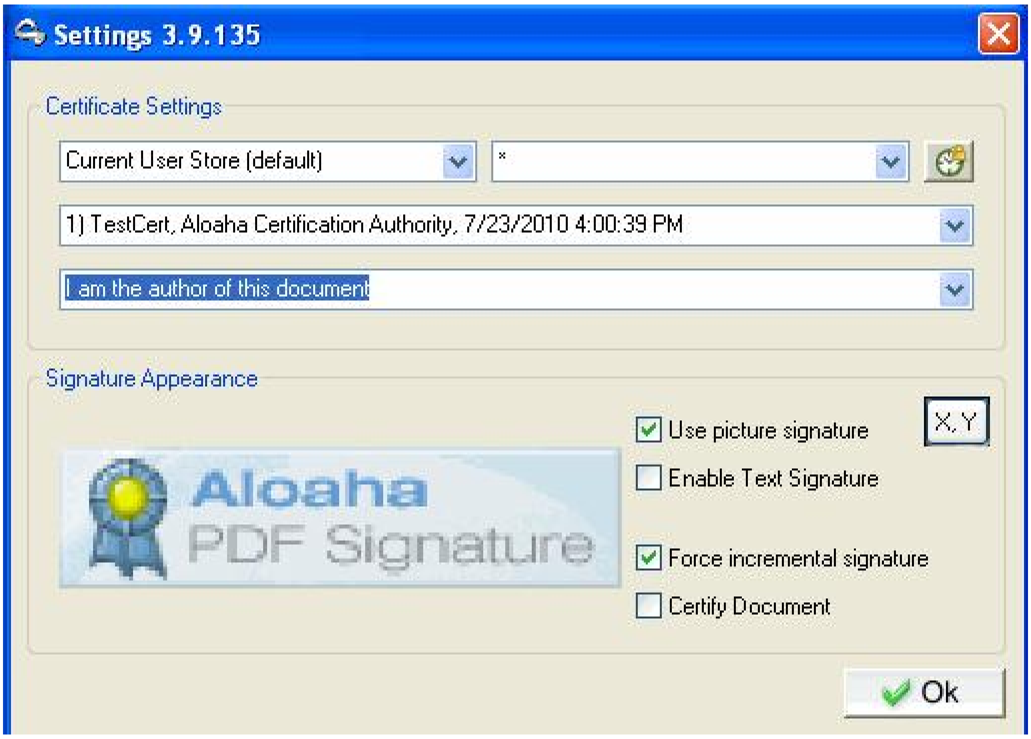
Digital signatures are based on asymmetrical Crypto systems and use a key pair which passes signature key of a private (confidential one) and public (not confidential).
The data which were encoded with one key can be opened again only with the other.
In order to sign the private key is used. The key 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).

### 3.3.1 Configure Signature

With a right click on the Aloaha Cardconnector System Tray Icon you can open die Dialog **Configure Signature**.



Here you can configure which certificate or Smartcard is being used if you sign a document via right click from within the Windows Explorer. It is furthermore possible to define the look and feel of a signature in case you sign a PDF document. To sign PDF documents the Aloaha PDF Signator or the Aloaha PDF Suite needs to be installed as well.


Settings 3.9.135

Certificate Settings

Current User Store (default)

*

1) TestCert, Aloaha Certification Authority, 7/23/2010 4:00:39 PM

I am the author of this document

Signature Appearance

☑ Use picture signature

□ Enable Text Signature

☑ Force incremental signature

□ Certify Document

**1. Certificate source**

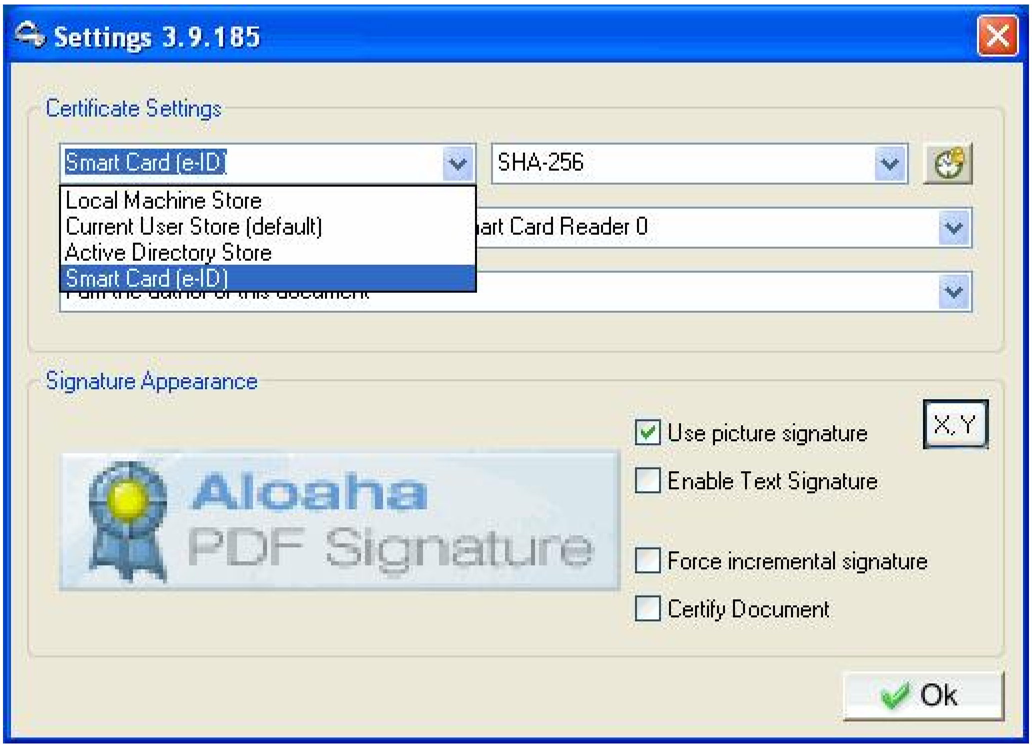
Here you can select between different kinds of certificates which you would like to use for signing of your PDF files.

To be available:

- **Computer certificates**
  All certificates which are associated to the computer are indicated in the certificate list.
- **User certificates (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.


Settings 3.9.185

Certificate Settings

Smart Card (e-ID)

SHA-256

art Card Reader 0

Signature Appearance

☑ Use picture signature

□ Enable Text Signature

□ Force incremental signature

□ Certify Document

## 3. Certificate select

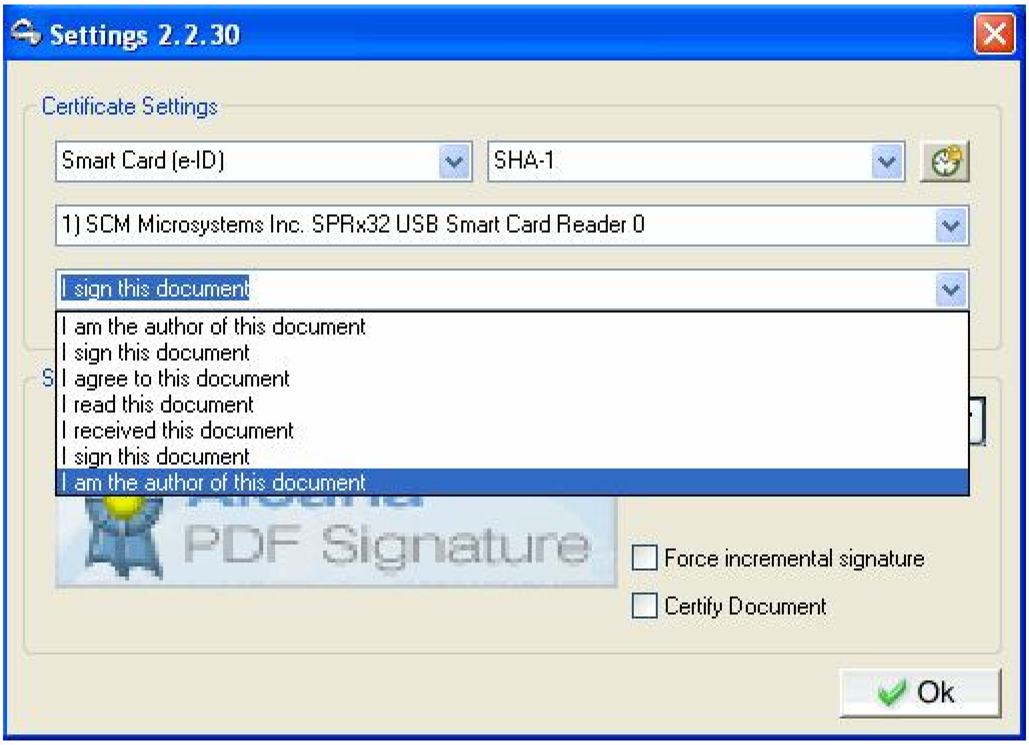
This menu depends on the certificate source. If you select "current user store", you receive a listing of all user's certificates on your PC and can select the suitable certificate.
Select as a certificate the SmartCard (e-ID), a listing of all installed SmartCard readers appears.
The Aloaha Card Connector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

## 4. 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

You can also enter free text.



Settings 2.2.30

Certificate Settings

Smart Card (e-ID)

SHA-1

1) SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0

I sign this document

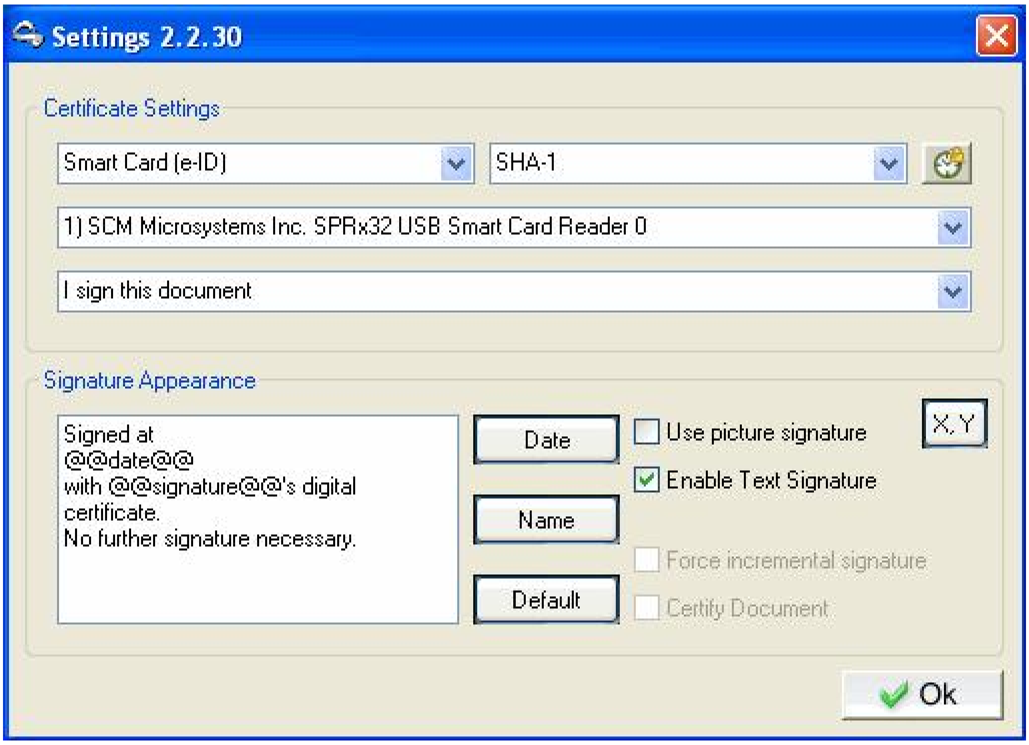
I am the author of this document
I sign this document
I agree to this document
I read this document
I received this document
I sign this document
I am the author of this document

☐ Force incremental signature

☐ Certify Document

## 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.



Settings 2.2.30

Certificate Settings

Smart Card (e-ID)

SHA-1

1) SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0

I sign this document

Signature Appearance

Signed at
@@date@@
with @@signature@@'s digital
certificate.
No further signature necessary.

□ Use picture signature

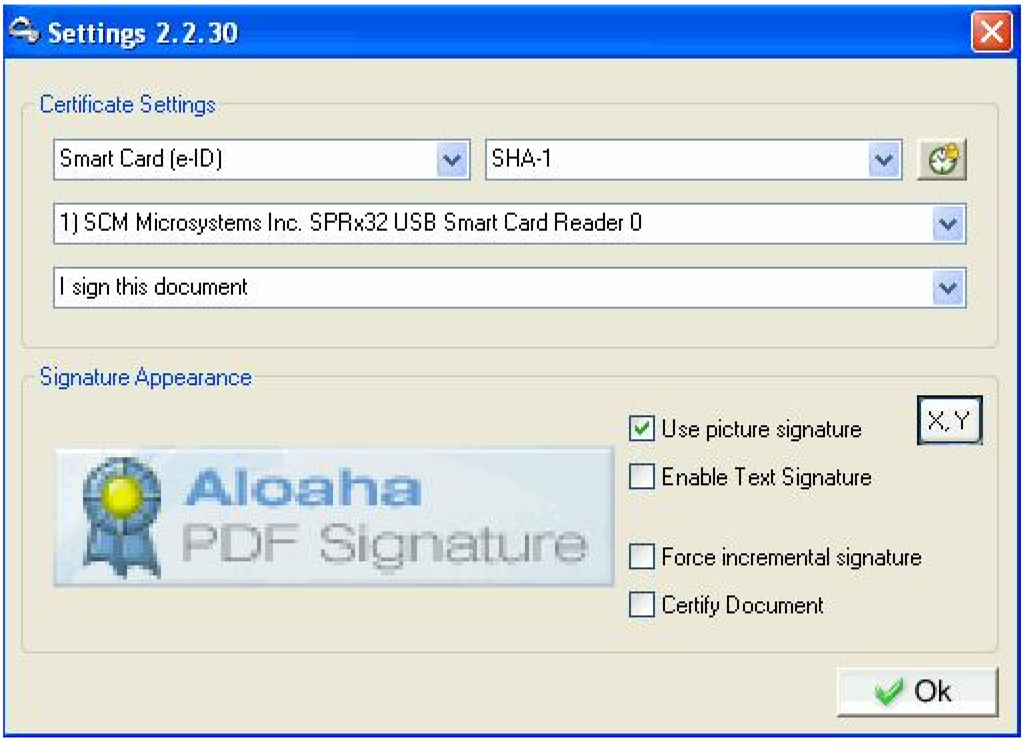
☑ Enable Text Signature

□ Force incremental signature

□ Certify Document

## Picture signature

You have also the possibility to sign the document with a picture signature.
You find further details in "signature settings"



Settings 2.2.30

Certificate Settings

Smart Card (e-ID)

SHA-1

1) SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0

I sign this document

Signature Appearance

☑ Use picture signature

X,Y

□ Enable Text Signature

□ Force incremental signature

□ Certify Document

Ok

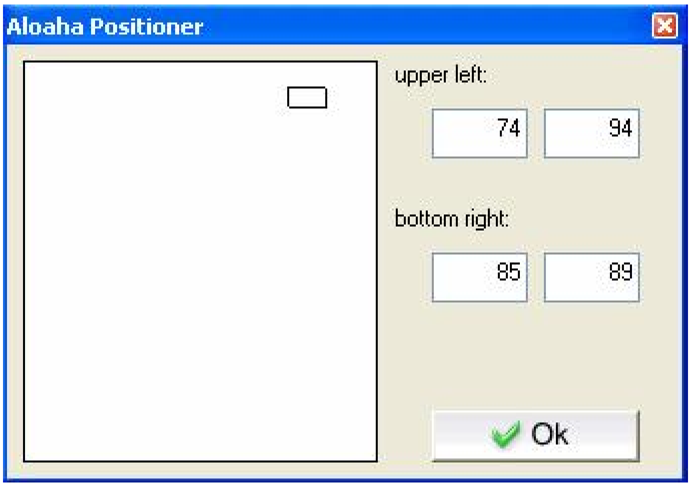
## 5. Settings for the time stamp

If you click on the watch icon another window opens:
You find further details to the settings of the time stamp under "time stamp"

## 6. 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.



Aloaha Positioner

upper left: 74 94

bottom right: 85 89

To change the signature image just click on the image itself. A file picker will pop up so that the user can choose a new 24 Bit jpg image.

It is also possible to time stamp the digital signature. To configure the time stamping server please click on the clock icon in the upper right corner of the dialog. In evaluation mode Aloaha will display only https addresses. The server https://tsa.aloaha.com is a free time stamping server of Aloaha. If http://AloahaTimestamper is choose Aloaha will use the local system time to time stamp the signature.

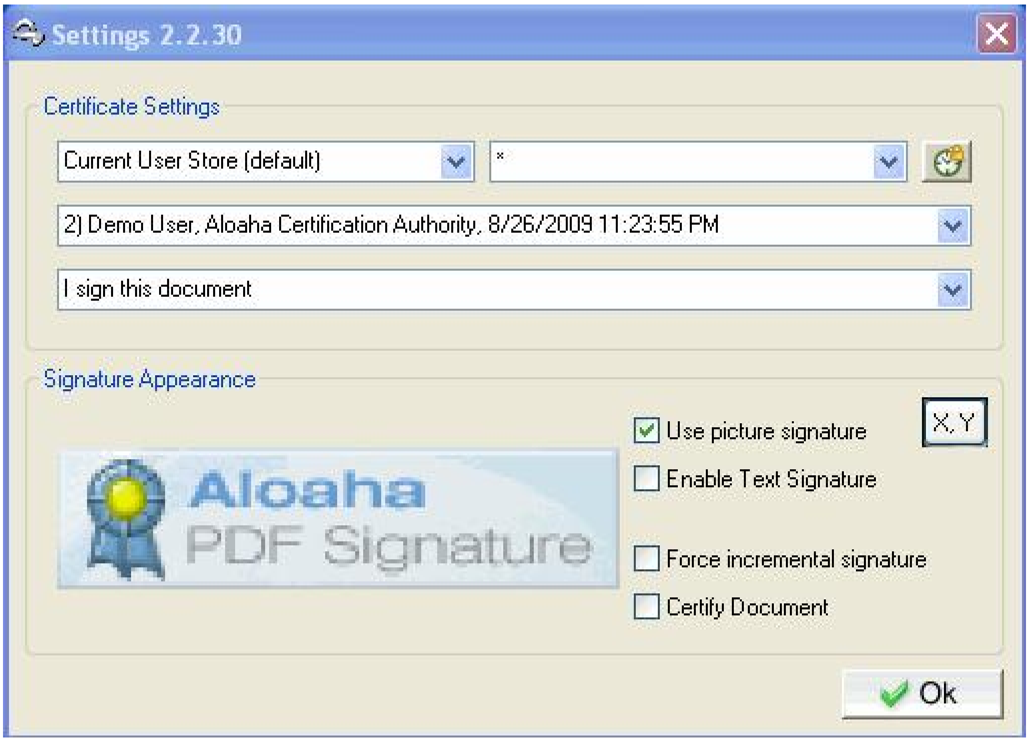
Please note that there are many time stamping authorities around which are not RFC 3161 compliant. That is the reason why Aloaha does not allow the user to add an authority to the authority list himself. If a user wants to have his authority added he needs to send a request to aloaha@wrocklage.de

### 3.3.2 Signature settings

If you click in the menu bar with the right mouse button on the icon, you will reach the signature settings.

In the certificate settings the kind of the certificate a document should be signed with can be selected.
The document to be signed can be selected in the explorer with click on the right mouse button.
If you would like to sign a PDF document it is possible to select between different signatures.

To be able to sign PDF documents, it is necessary that the Aloaha PDF Signator or the PDF Suite is installed.



Settings 2.2.30

Certificate Settings

Current User Store (default)

*

2) Demo User, Aloaha Certification Authority, 8/26/2009 11:23:55 PM

I sign this document

Signature Appearance

☑ Use picture signature

□ Enable Text Signature

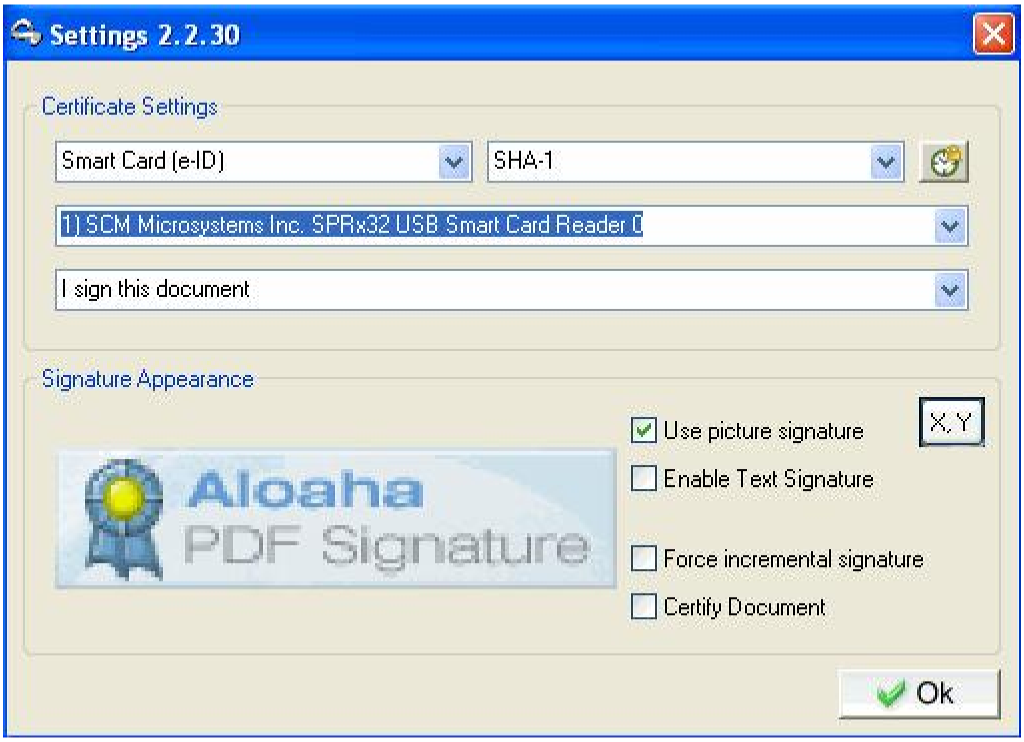
□ Force incremental signature

□ Certify Document

Instead of in the system located certificate a Card reading device can be selected if necessary also as a signature data source.

This can be helpful by use of several signature cards. The card reader is in the basic settings as a data source already defined.

In this case Aloaha uses the signature of the card in the configured reader.
The advantage consists in the fact that the user must not configure the signature settings with use of other cards once more.



Settings 2.2.30

Certificate Settings

Smart Card (e-ID)

SHA-1

1) SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0

I sign this document

Signature Appearance

☑ Use picture signature

□ Enable Text Signature

□ Force incremental signature

□ Certify Document

To change the Sigantur, click on the graphics. Afterwards you can change the picture.

**Use picture signature**
If this field is activated, a picture is seated in the PDF as it is shown in the preview of this dialog. You can load an own image file by click on the actual signature picture from your harddisc. This picture must be in 24 bit JPG format.

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

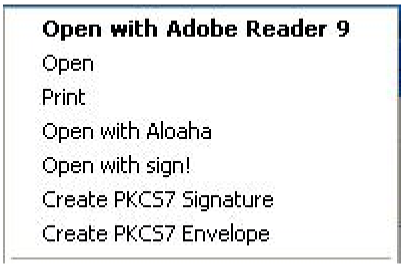
**Force incremental signature**
Aloaha will sign the document incremental. Besides the signature is attached to the document itself that any time the original document allows to recover!

With this programme it is possible to provide the signature with a time stamp. To configure the time stamp click on the watch icon.
https://tsa.aloaha.com is an independent time stamp server which is provided by Aloaha.
If you have selected http://AloahaTimestamper, the program uses the local system time to stock the signature with a time stamp.

**Note**: Many time stamp authorisations are not RFC 3161 compatible, hence Aloaha gives no competence to the user to assign other authorisations.
For other authorisations write an email to aloaha@wrocklage.de

# 3.4 Create PKCS #7 Signature

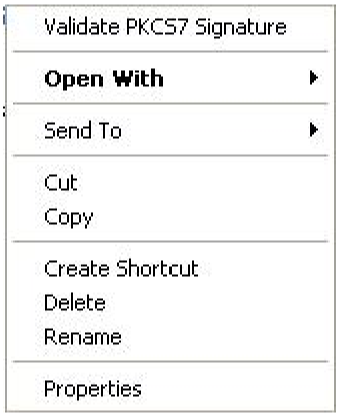
The Aloaha Cardconnector integrates itself neatly into the Windows Explorer.



If the user clicks with the right mouse button on a file the Windows Explorer Context Menu opens. The Aloaha Shell Extension allows the user to create a PKCS #7 Signature and a PKCS #7 Envelope. Aloaha will use the certificate configured via the Signature Settings Dialog.

In case the Aloaha PDF Signator or the Aloaha PDF Suite is installed and licensed on the same machine a third entry Create PDF Signature will be available. Clicking on that item will create an embedded PDF Signature.

## PKCS #7 Validation



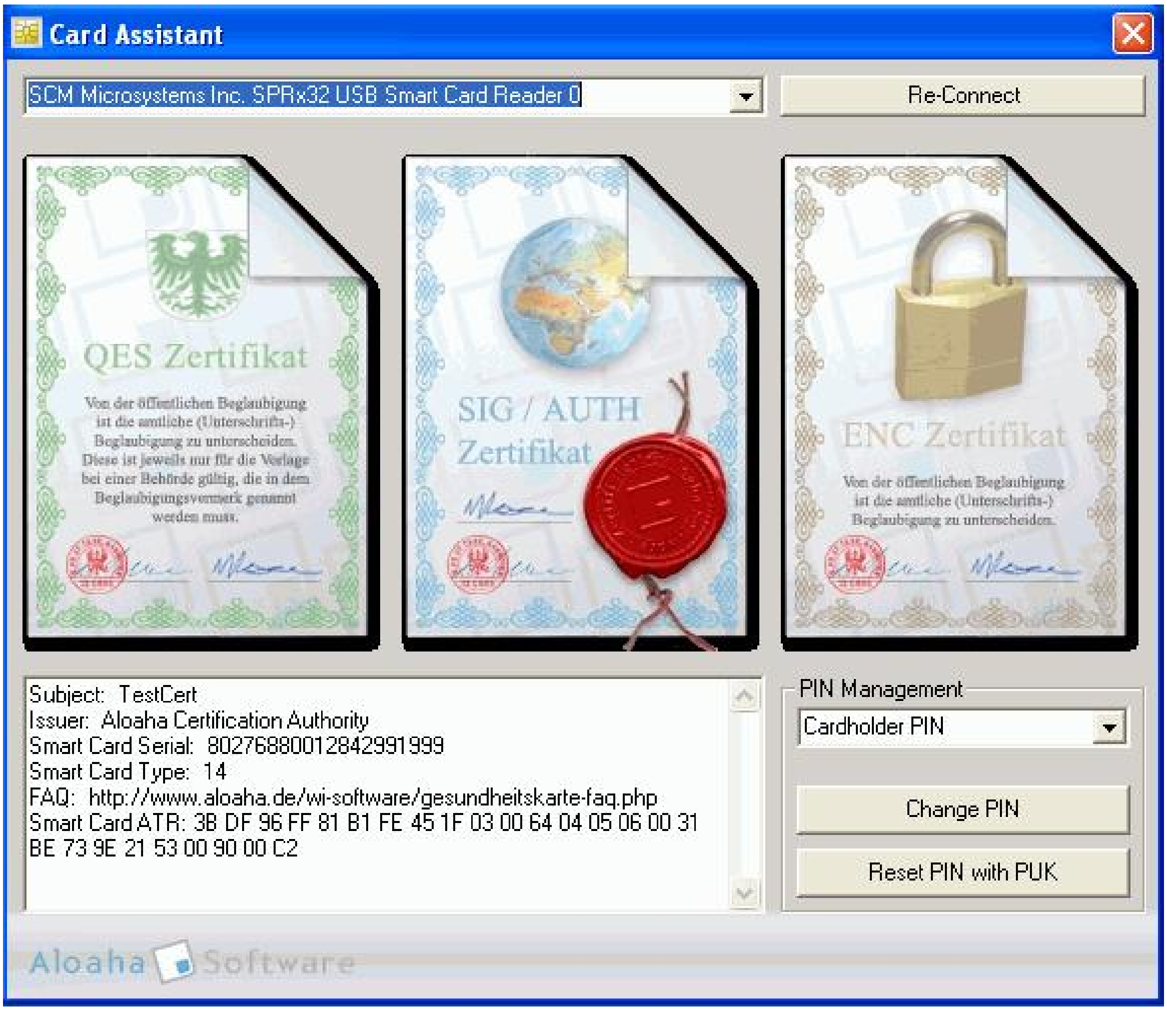
The Aloaha Shell Extension is also able to validate PKCS #7 signatures. Just right click on one of them and chose **Validate PKCS7 Signature**. In case the signature is valid Aloaha will display the certificate. If the signature is an enveloped signature Aloaha will also extract the original file and place it in the same folder.

**Signature Validation is a freeware feature of Aloaha.**

## 3.5 PIN Administration

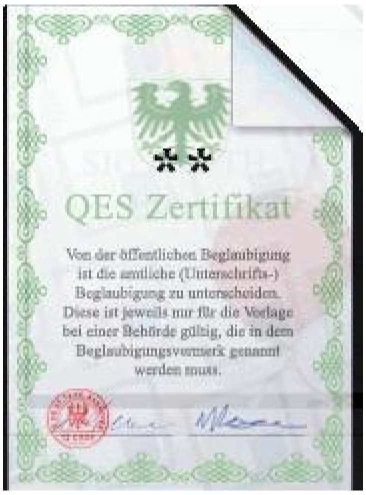
About the select menu **Card Assistant** you can administer following PIN's:

Signature pin
Card pin
PIN Home


Card Assistant
SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0
Re-Connect
QES Zertifikat
Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden. Diese ist jeweils nur für die Vorlage bei einer Behörde gültig, die in dem Beglaubigungsvermerk genannt werden muss.
SIG / AUTH Zertifikat
ENC Zertifikat
Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden.
PIN Management
Cardholder PIN
Change PIN
Reset PIN with PUK
Aloaha Software

Subject: TestCert
Issuer: Aloaha Certification Authority
Smart Card Serial: 80276880012842991999
Smart Card Type: 14
FAQ: http://www.aloaha.de/wi-software/gesundheitskarte-faq.php
Smart Card ATR: 3B DF 96 FF 81 B1 FE 45 1F 03 00 64 04 05 06 00 31 BE 73 9E 21 53 00 90 00 C2

After you clicked on the button Change PIN, the following picture appears:

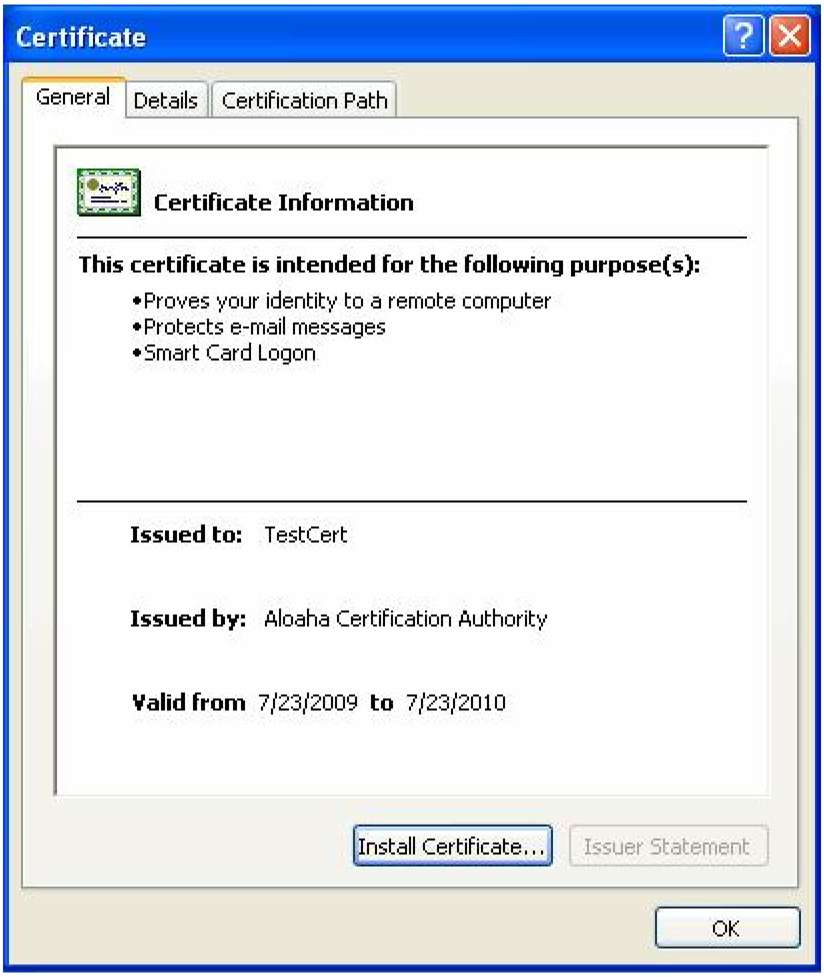

**
QES Zertifikat
Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden. Diese ist jeweils nur für die Vorlage bei einer Behörde gültig, die in dem Beglaubigungsvermerk genannt werden muss.

First you enter the old PIN over the Card reading device. Confirm the input with the green button.
Afterwards you enter the new PIN. You are asked to confirm this by repeated input.
Afterwards the process is concluded.

## 3.6 Certificate

### General certificate informations

To receive information about the certificates, call the Card Assistant.
Click on one of the certificates contained in the Card Assistant and you receive the information about the chosen certificate.
Here it is indicated, how long the certificate is still valid, whether it has run off if necessary who has issued the certificate and which name the certificate bears.



Certificate Information

This certificate is intended for the following purpose(s):

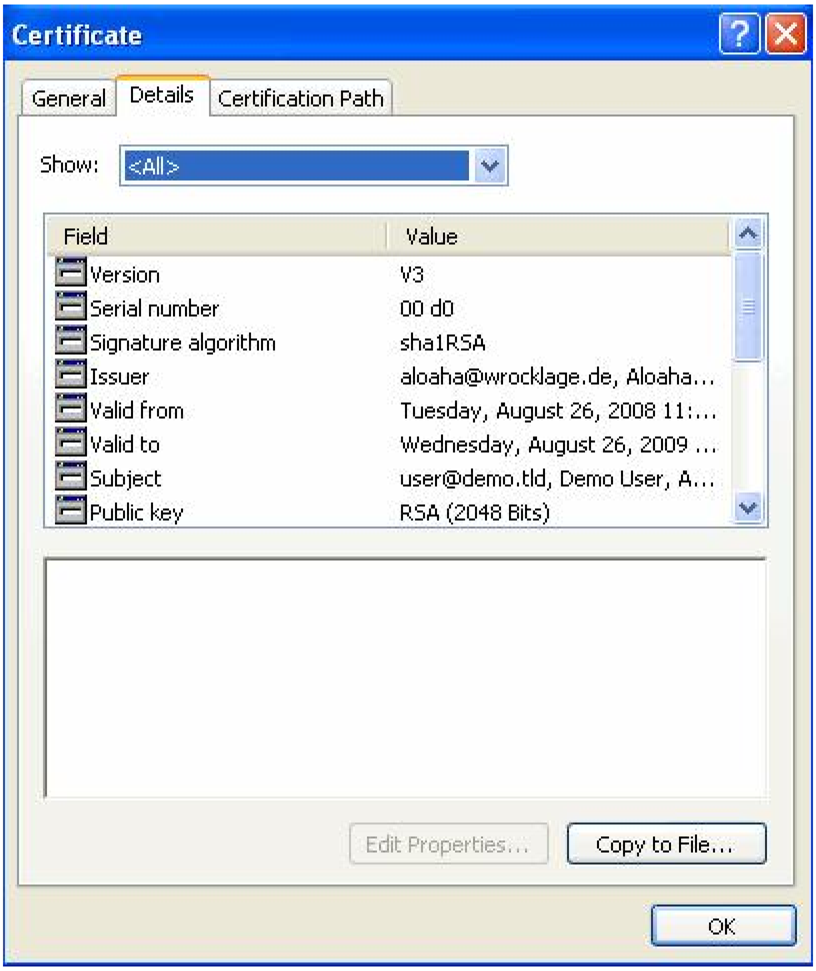
- Proves your identity to a remote computer
- Protects e-mail messages
- Smart Card Logon

Issued to: TestCert

Issued by: Aloaha Certification Authority

Valid from 7/23/2009 to 7/23/2010

In the flag "Details" you find further information to the respective certificate, for example:
Version
Serial number
Signature algorithm
Exhibitor
valid from
valid to
Applicant
public key

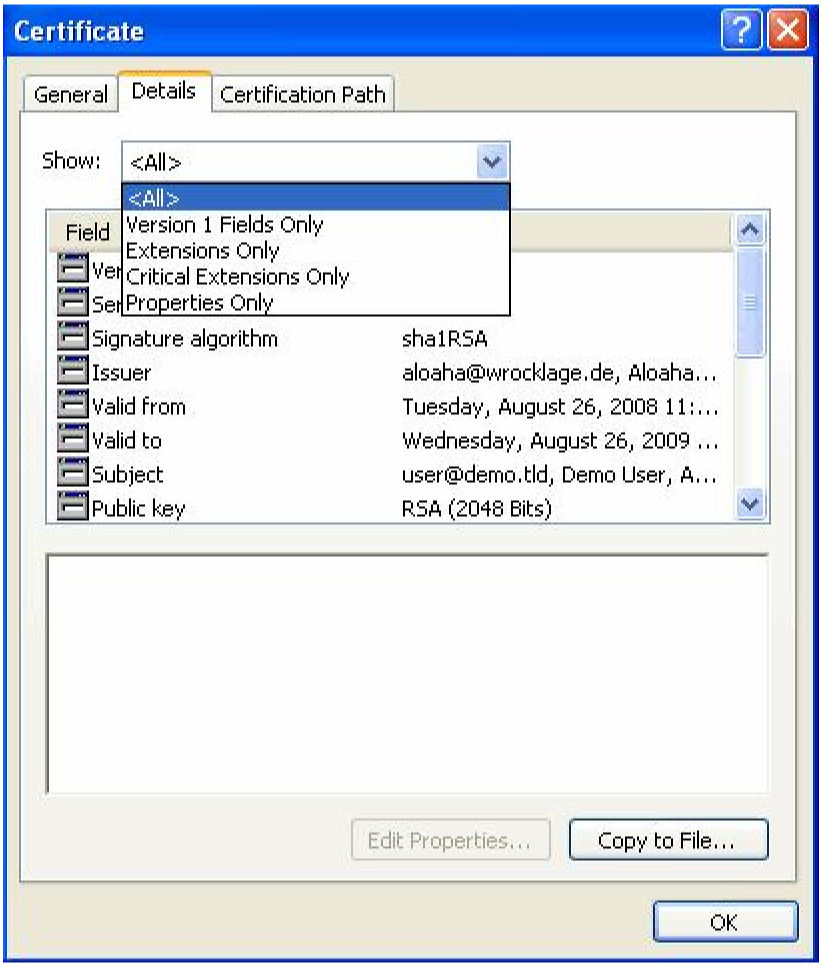


Show: <All>

| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 00 d0 |
| Signature algorithm | sha1RSA |
| Issuer | aloaha@wrocklage.de, Aloaha... |
| Valid from | Tuesday, August 26, 2008 11:... |
| Valid to | Wednesday, August 26, 2009 ... |
| Subject | user@demo.tld, Demo User, A... |
| Public key | RSA (2048 Bits) |

You can allow to indicate following information to the respective certificate:

All
Version 1 Fields only
Extensions only
Critical Extensions only
Properties only

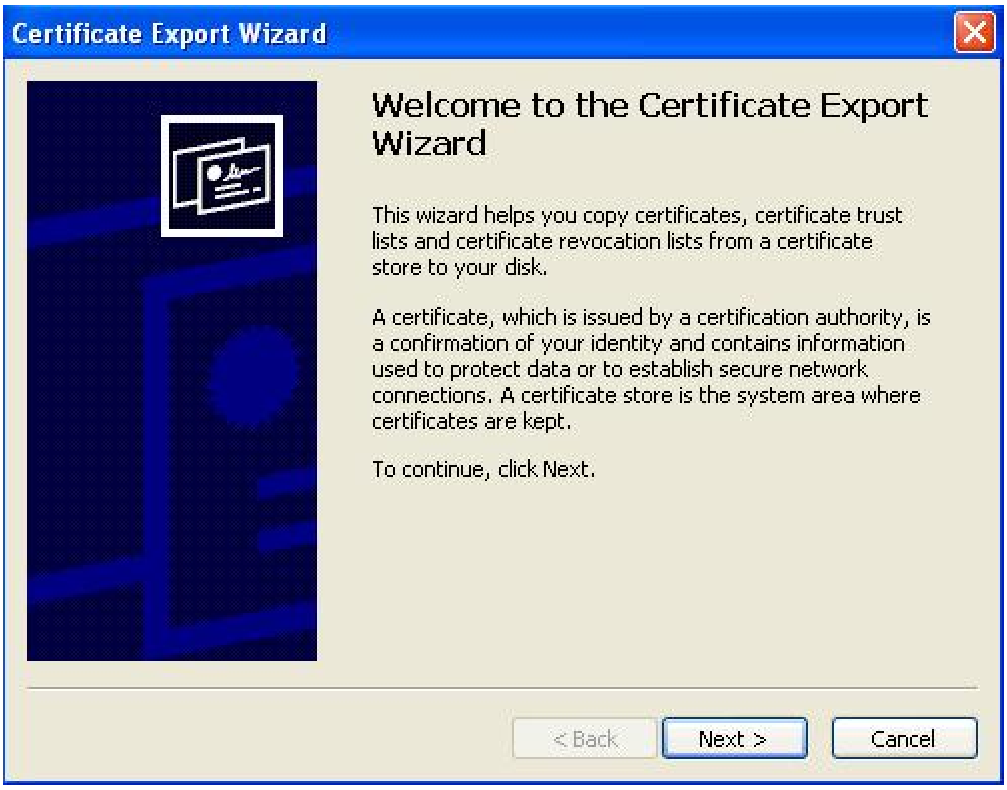


Show: <All>

- <All>
- Version 1 Fields Only
- Extensions Only
- Critical Extensions Only
- Properties Only

| Field | |
|---|---|
| Ver | |
| Ser | |
| Signature algorithm | sha1RSA |
| Issuer | aloaha@wrocklage.de, Aloaha... |
| Valid from | Tuesday, August 26, 2008 11:... |
| Valid to | Wednesday, August 26, 2009 ... |
| Subject | user@demo.tld, Demo User, A... |
| Public key | RSA (2048 Bits) |

You reach the certificate export wizard if you select in the before shown picture "copy to file".



Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

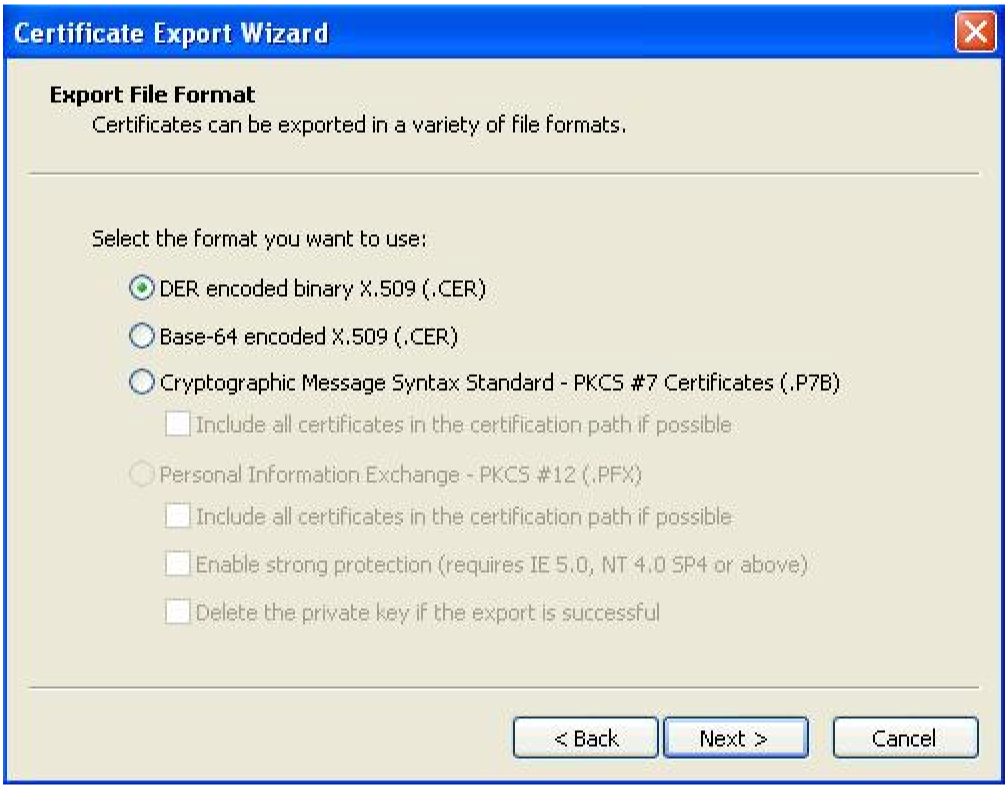
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

After you confirmed with "Next", a window opens and the export file format can be selected.

Three possible export formats stand at possession.

**DER encoded binary X.509 (.CER)**
**Base-64 encoded X.509 (.CER)**
**Cryptographic Message Syntax Standard- PKCS #7-Certificates (.P7B)**



Certificate Export Wizard

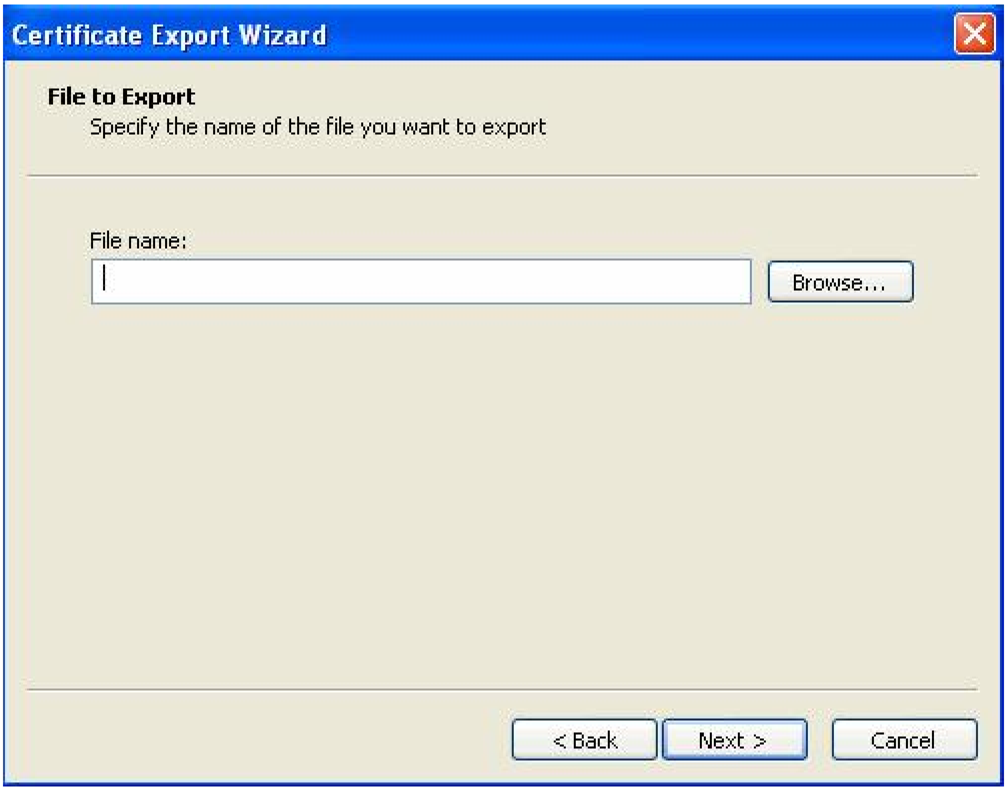
**Export File Format**
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
  - □ Delete the private key if the export is successful

After you have selected the file format, confirm with "Next" and reach to the following flag.

Here you have to give a name to the file and save in a directory of your choice.



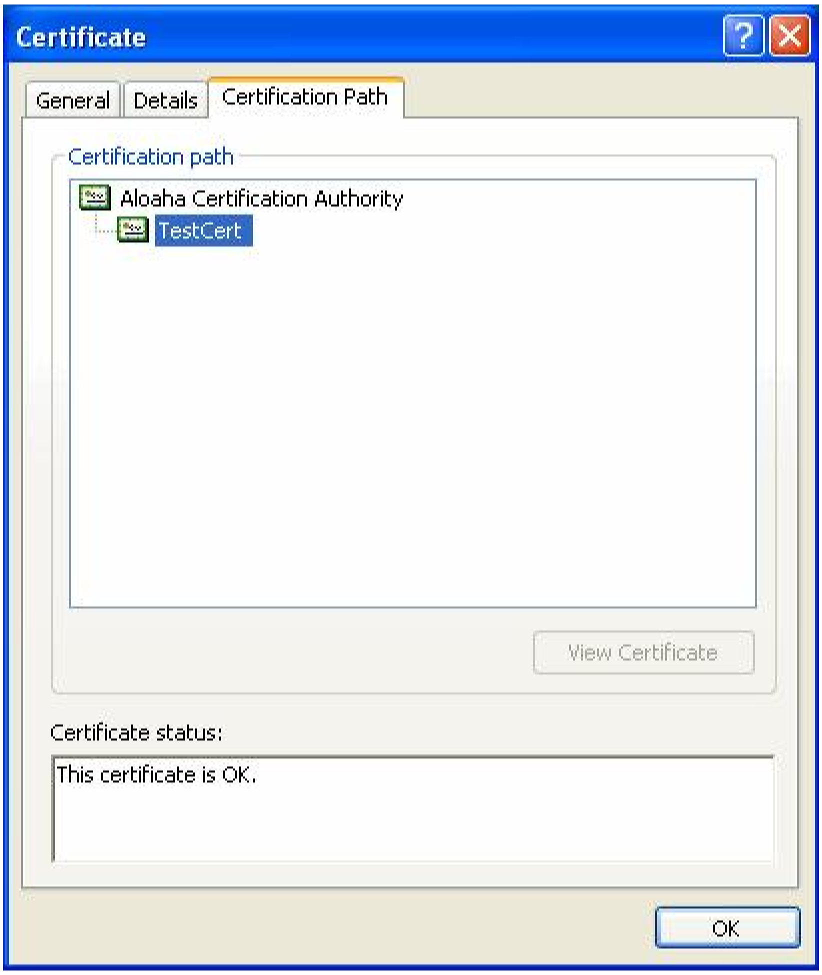
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

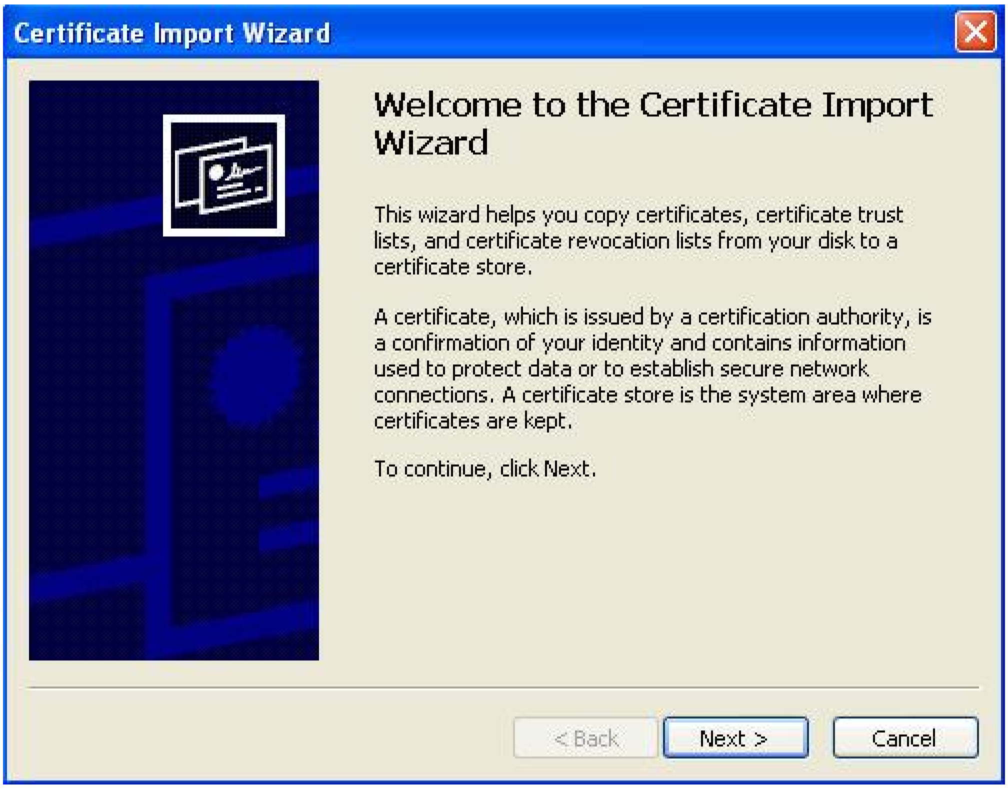
The certification path specifies who is originator of the document.



Certificate status:

This certificate is OK.

You reach the certificate import wizard if you click in the flag "General" install certificate. With "Next" you continue the process.



Certificate Import Wizard

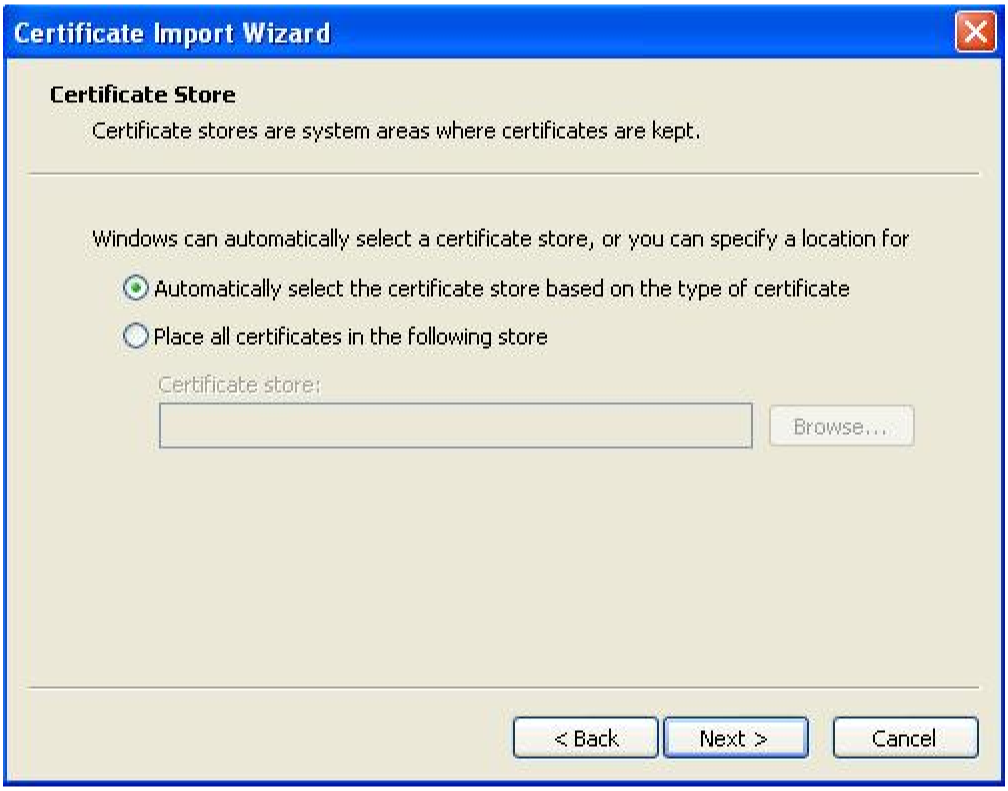
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Here you select the certificate store either based on the certificate type automatically or you fix the memory store where certificates should be saved.



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

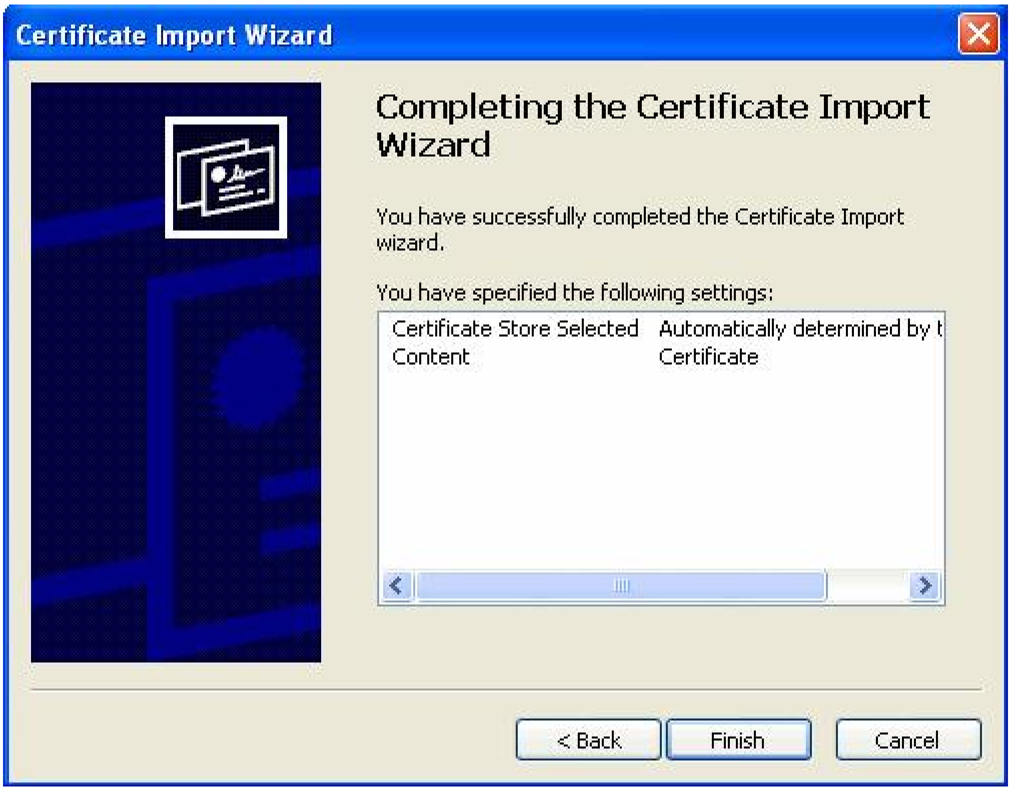
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

In this case the automatic certificate memory is selected. You see the settings covered to the certificate. Conclude the process with "Finish".



Certificate Import Wizard

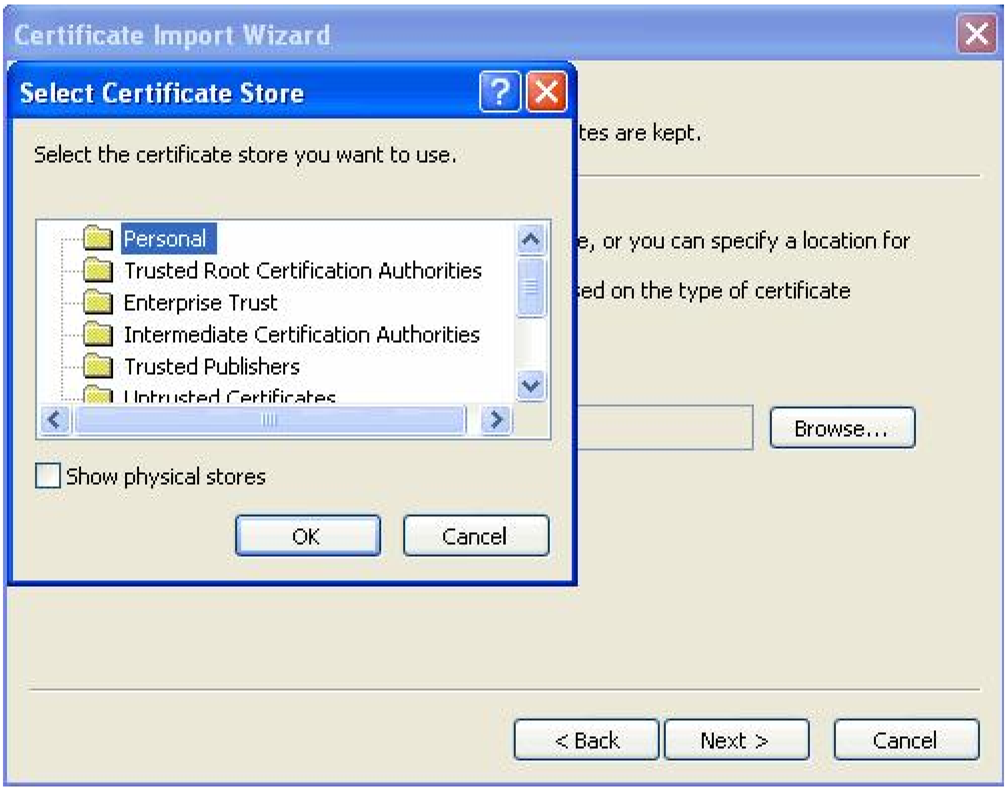
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected | Automatically determined by t |
| Content | Certificate |

You have not only the possibility to save certificates automatically by the wizard. If you decide to select the certificate store independently, activate the suitable field and select the memory store even from the list appearing then. Afterwards you confirm the choice with OK.



Certificate Import Wizard
Select Certificate Store
tes are kept.
e, or you can specify a location for
ed on the type of certificate
Browse...
< Back
Next >
Cancel

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

## 3.7 CSP / CardReader

### Supported Cardreader

Aloaha supports the following card readers of the security class 2 and 3. They were confirmed according to the German signature law and may be seated to the production of certified electronic signatures.

Chipkartenleser OmniKey Cardman 3621Trust

Chipkartenleser Omnikey CardMan® 3821 USB

Chipkartenleser SCM CHIPDRIVE® pinpad pro

CHERRY® Smart Terminal ST-2000UC-R

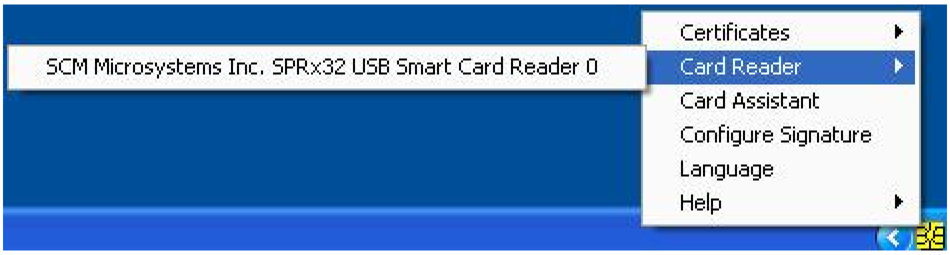
CHERRY® Tastatur G83-6744 LUADE-2 USB DE

Reiner SCT cyberjack

Reiner SCT cyberJack® e-com

all PC/SC correspondent reader

If you click in the menu bar with the right mouse button on the icon, you will reach the settings of the cardreader.
Should several cardreader devices be available, all of them are indicated and you can select the required one.



As soon as a card was put in a reader, the programme automatically registers all certificates located on the card. Nevertheless, the certificates can be also registered manually. Instead of autoregisters you click instead on register.

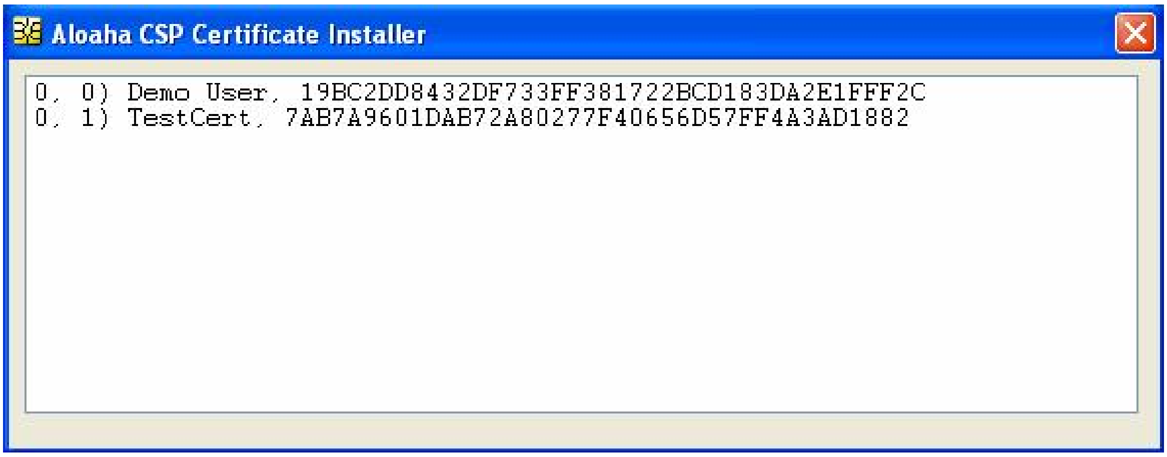
The first number indicates the number of the cardreader devices. The following Screenshot shows the certificates of the card (s) in connected card readers.
The number after the comma indicates the certificate type.

Typ 0 = Signature certificate,
Typ 1 = Authentification certificate,
Typ 2 = Encryption certificate.

If a card contains only one certificate, this is indicated as type 1.

To delete all registered certificates, click on remove all". If autoremoving is activated, all registered certificates are deleted, as soon as all cards from the map reading devices were deleted.

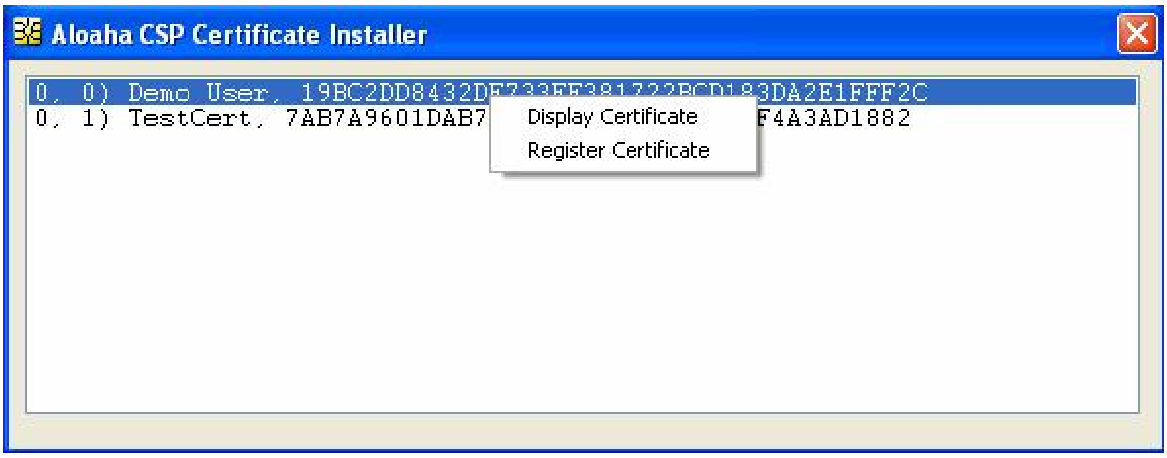
## Cardreader



```
0, 0) Demo User, 19BC2DD8432DF733FF381722BCD183DA2E1FFF2C
0, 1) TestCert, 7AB7A9601DAB72A80277F40656D57FF4A3AD1882
```

In some cases are several cardreader devices connencted to a system. It takes time to enumerate the certificates of all readers. In this case you can select the cardreader device directly. Then Aloaha reads out only the certificates of the card in the selected reader.

Now you can click the certificate to indicate it or to register it by double click in the default directory.



```
0, 0) Demo User, 19BC2DD8432DF733FF381722BCD183DA2E1FFF2C
0, 1) TestCert, 7AB7A9601DAB7
```

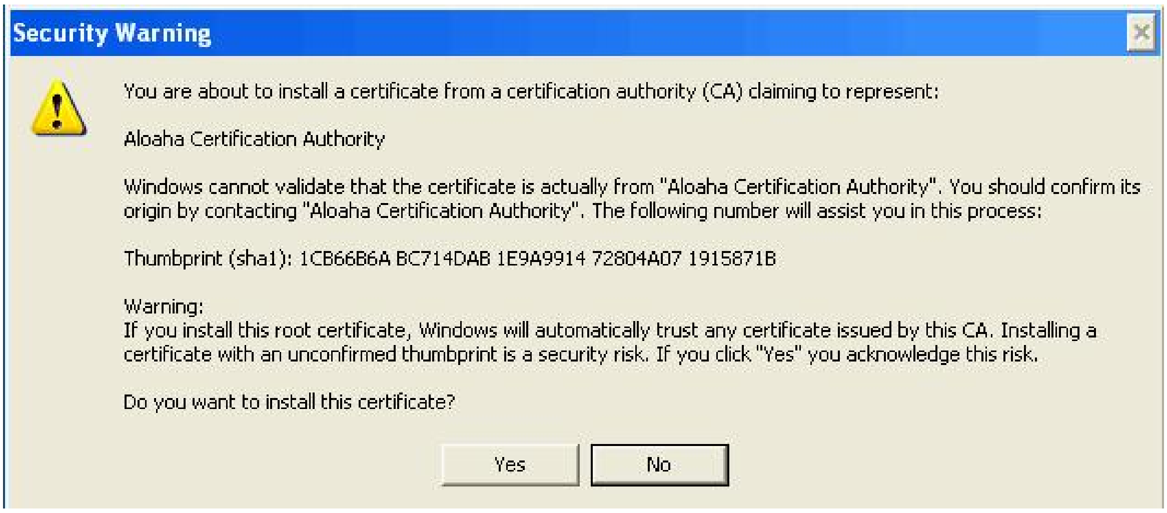
**Advantages of manual registration:**

1. If the output certificate is not available in the system, Aloaha will try to download it from the Aloaha website.
2. The entered certificate is automatically configured as a standard certificate.

### Security warning with certificate indicate / register

If you register a certificate you will receive the following security warning. Peruse the contents and decide whether you would like to register / install the certificate or not.

This dialog appears ONLY the **FIRST** Time if a new Root certificate is built in!



You are about to install a certificate from a certification authority (CA) claiming to represent:

Aloaha Certification Authority

Windows cannot validate that the certificate is actually from "Aloaha Certification Authority". You should confirm its origin by contacting "Aloaha Certification Authority". The following number will assist you in this process:

Thumbprint (sha1): 1CB66B6A BC714DAB 1E9A9914 72804A07 1915871B

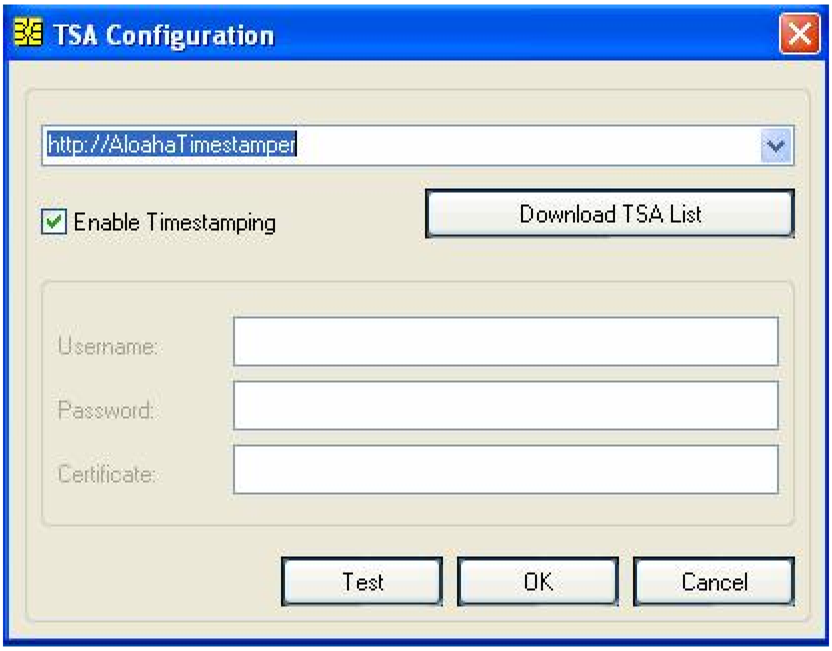
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

## 3.8 Timestamper

### Timestamp settings

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



TSA Configuration

http://AloahaTimestamper

☑ Enable Timestamping

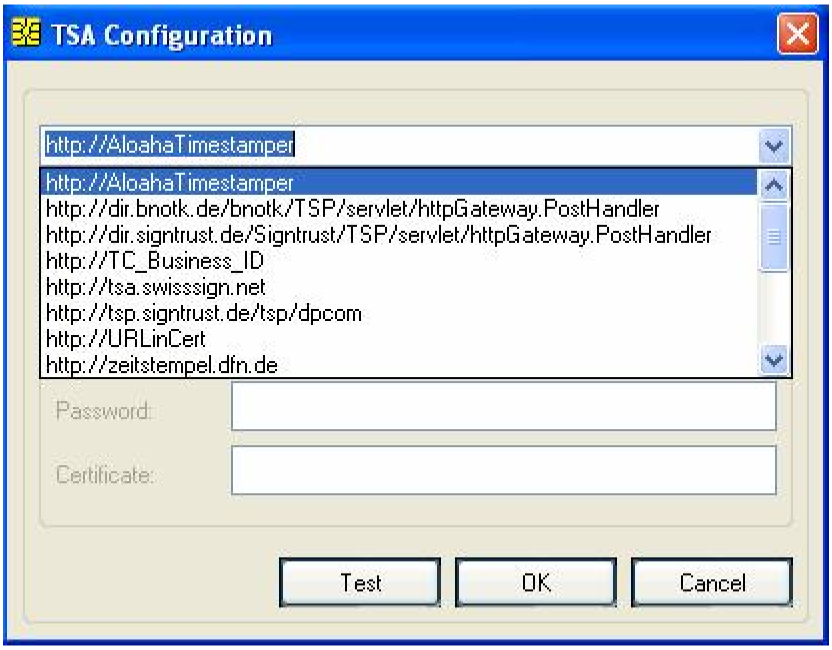
Username:

Password:

Certificate:

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://AloahaTimestamper, the TimeStamp server is used. On this occasion, the local system time is taken as a basis for the time stamp. In user data you configure your access data to the respective time stamp service.



http://AloahaTimestamper

http://AloahaTimestamper
http://dir.bnotk.de/bnotk/TSP/servlet/httpGateway.PostHandler
http://dir.signtrust.de/Signtrust/TSP/servlet/httpGateway.PostHandler
http://TC_Business_ID
http://tsa.swisssign.net
http://tsp.signtrust.de/tsp/dpcom
http://URLinCert
http://zeitstempel.dfn.de

# 4. Application Support

The Aloaha Cardconnector provides with its Cryptographic Service Provider (CSP) a link between the Smartcard itself and the Windows Cryptographic System. Like that it is possible that Windows Applications can make use of the Smartcard Certificates as if they are software certificates. In other words. Thanks to Aloaha the Windows Applications do not even know that the certificates and private keys are hosted on a Smartcard.

Most of open source applications do not make use of the Windows Cryptographic System but of the PKCS #11 standard. For those applications Aloaha installs its PKCS #11 Library in the Windows system32 directory. The name of the Aloaha Library is aloaha_pkcs11.dll.

**Please visit**
**http://www.aloaha.com/wi-software-en/csp-usage.php**
**to find some flash based videos!**

## 4.1 MS Crypto API

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. The are also responsible for the communication between Smartcards and the Windows Operating System

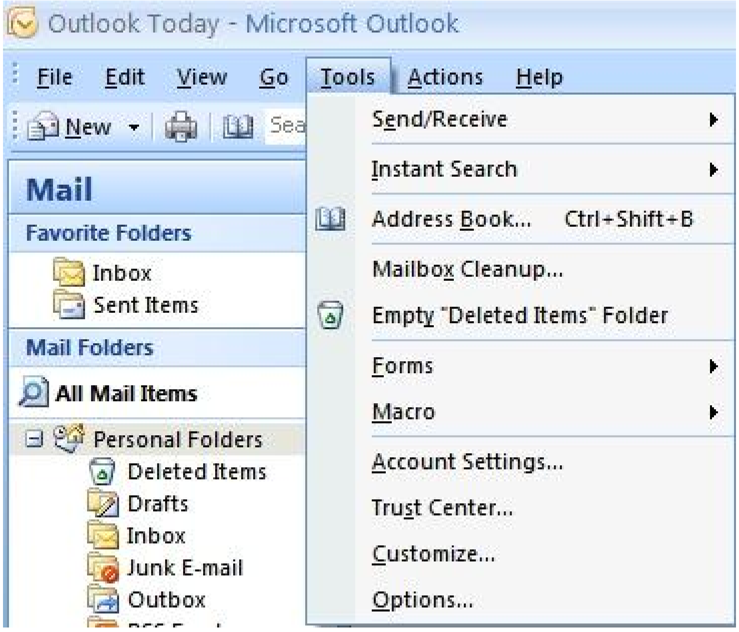
## 4.1.1 Outlook

### Configure Signature Settings in Microsoft Outlook

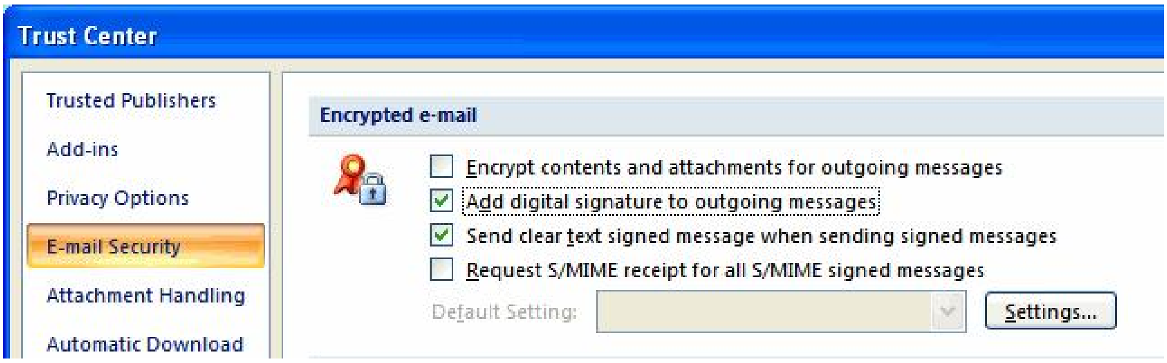
In Microsoft Outlook it is pretty easy to configure the signature and encryption certificate.

Some usage videos can be found on: http://www.aloaha.com/movies/outlook.htm

Open the Tools Menu and choose Options as shown in the screenshot below.
***Start>All Programs>Microsoft Office>Outlook>Tools>Trust Center>E-Mail-Security***



In the Options Dialog you enable **Add digital signature to outgoing message** in case you want Outlook to sign every message by default. It you just want to pre-configure the signature settings just leave that option disabled. To choose the certificates and algorithm used please click on the **Settings** button.



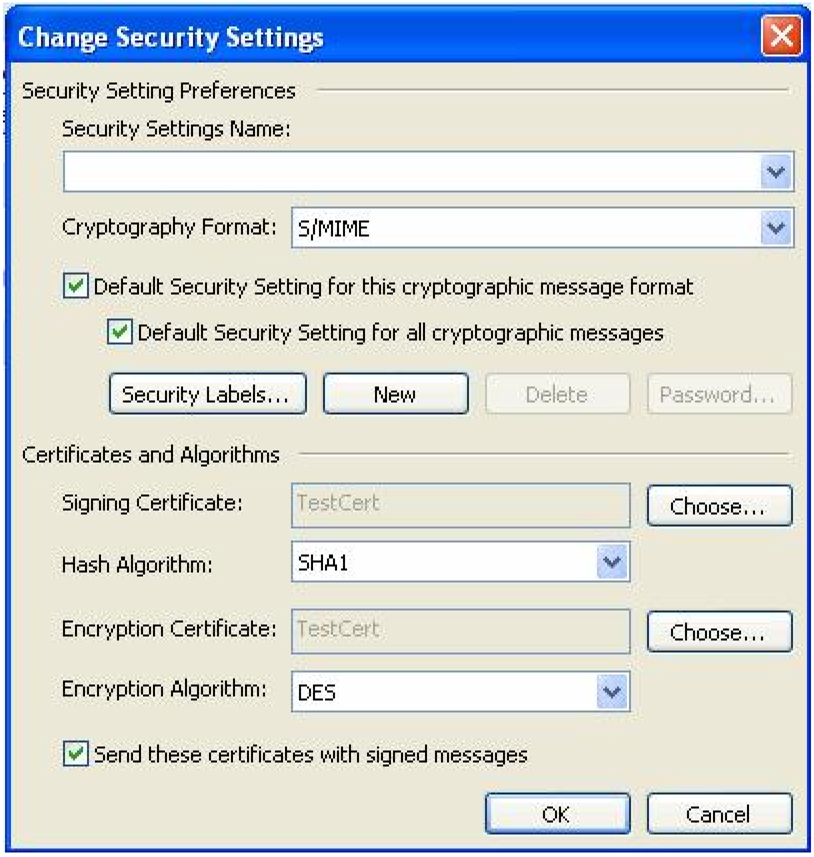
Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
☑ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Here you can just choose the Signing Certificate and the Encryption Certificate. Please make sure that you had registered your certificates before! In case your certificate does not show it means that a required attribute is missing in your certificate or your certificate is invalid/expired.

**Some email clients require that the configured email address matches the email address in the certificate! In that case you will not get the option to choose your card certificate.**


Change Security Settings

Security Setting Preferences

Security Settings Name:

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: TestCert

Hash Algorithm: SHA1

Encryption Certificate: TestCert

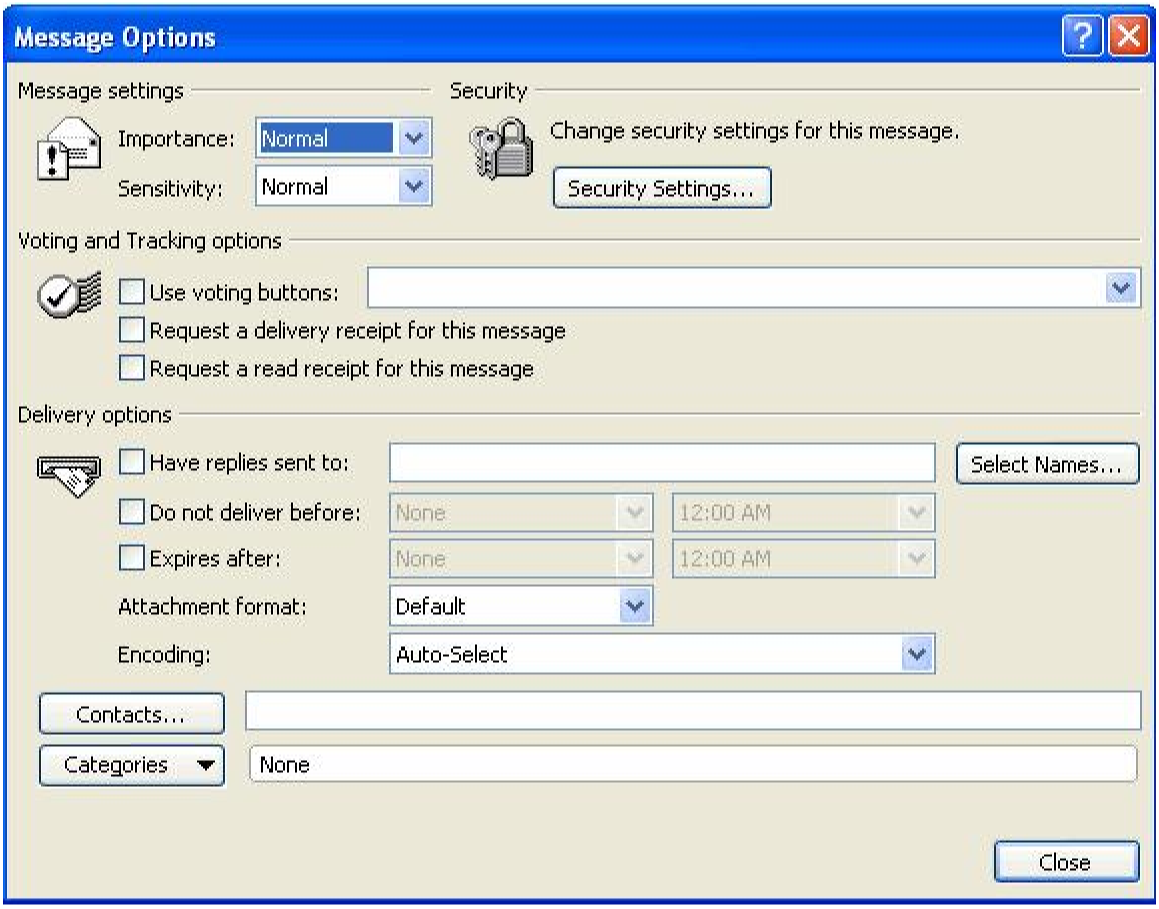
Encryption Algorithm: DES

☑ Send these certificates with signed messages

With OK you confirm your settings.

## Send a digitally signed email

To send a digitally signed message just go on **Options**.
***Start>All Programs>Microsoft Office>Outlook>Tools>Trust Center>E-Mail-Security>Settings***
A new Dialog will pop up in which you press the button **Security Settings**. You can also use the signature icon in the toolbar of outlook.



Message Options

Message settings

Importance: Normal

Sensitivity: Normal

Security

Change security settings for this message.

Voting and Tracking options

□ Use voting buttons:

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

□ Have replies sent to:

□ Do not deliver before: None 12:00 AM

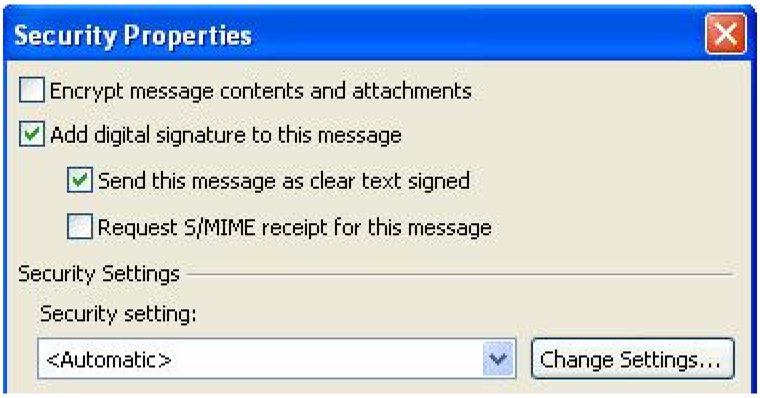
□ Expires after: None 12:00 AM

Attachment format: Default

Encoding: Auto-Select

Categories: None

Now you need to enable **Add digital signature to this message** and press the **Change Settings** Button.



Security Properties

□ Encrypt message contents and attachments

☑ Add digital signature to this message

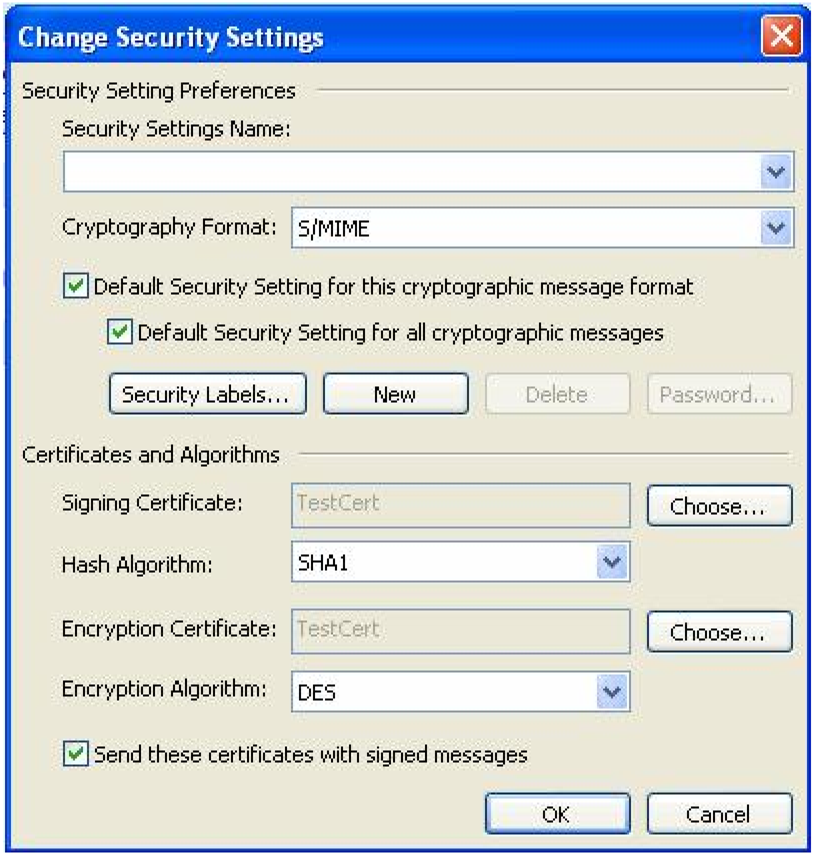
☑ Send this message as clear text signed

□ Request S/MIME receipt for this message

Security Settings

Security setting: <Automatic>

Now a well known dialog pops up. You choose your certificates and confirm with **OK**.



Change Security Settings

Security Setting Preferences

Security Settings Name:

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: TestCert

Hash Algorithm: SHA1

Encryption Certificate: TestCert

Encryption Algorithm: DES

☑ Send these certificates with signed messages

## 4.2 PKCS #11

In cryptography, PKCS#11 is one of the family of standards called Public-Key Cryptography Standards (PKCS), published by RSA Laboratories. It defines a platform-independent API to cryptographic tokens, such as Hardware Security Modules and smart cards. (The PKCS#11 standard names the API "Cryptoki", but "PKCS#11" is often used to refer to the API as well as the standard that defines it.)

Since there isn't a real standard for cryptographic tokens, this API has been developed to be an abstraction layer for the generic cryptographic token. The PKCS#11 API defines most commonly used cryptographic object types (RSA keys, X.509 Certificates, DES/Triple DES keys, etc.) and all the functions needed to use, create/generate, modify and delete those objects.

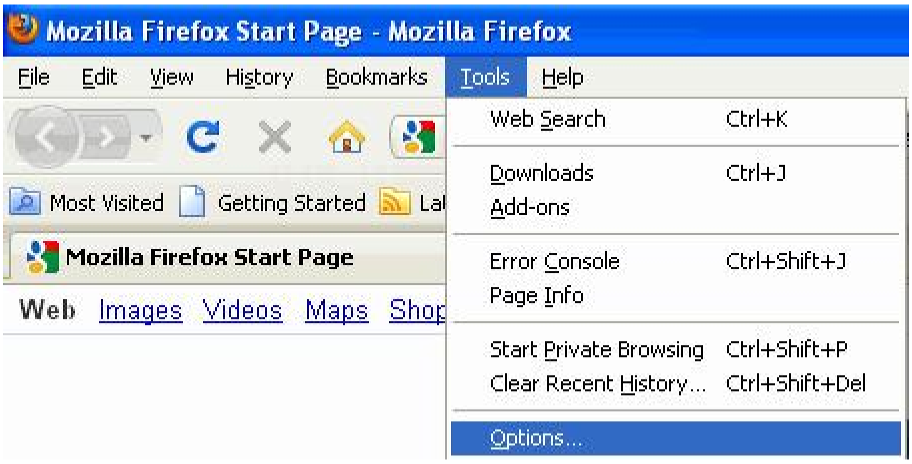
PKCS#11 is largely adopted to access smart cards. Cross-platform software that needs to use smart cards uses PKCS#11, such as Mozilla Firefox and OpenSSL (using an extension). Software written for Microsoft Windows may use the platform specific MS-CAPI API instead.

### 4.2.1 Firefox settings

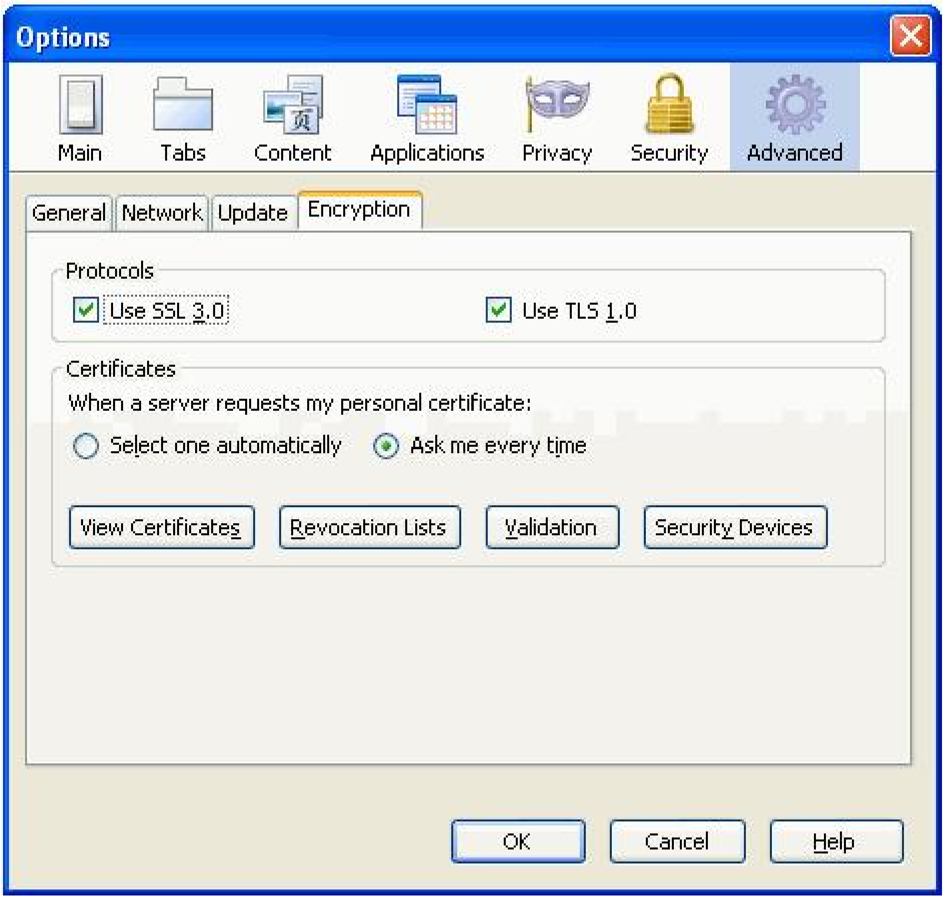
Firefox does not use the Microsoft Crypto API but PKCS #11 Libraries. Below you find the steps on how to register the Aloaha PKCS #11 in Firefox.

There is also an online usage video available on aloaha.com.
The full URL is: http://www.aloaha.com/movies/firefox.htm

To register Aloaha modules in Firefox you click on the top menu of Windows:
***Start>All Programs>Mozilla Firefox>Tools>Options>*****Advanced>Security Devices**


Mozilla Firefox Start Page - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Error Console Ctrl+Shift+J
Page Info
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Options...
Most Visited
Getting Started
Lat
Mozilla Firefox Start Page
Web
Images
Videos
Maps
Shop

Now choose **Advanced** and press **Security Devices**.



Protocols

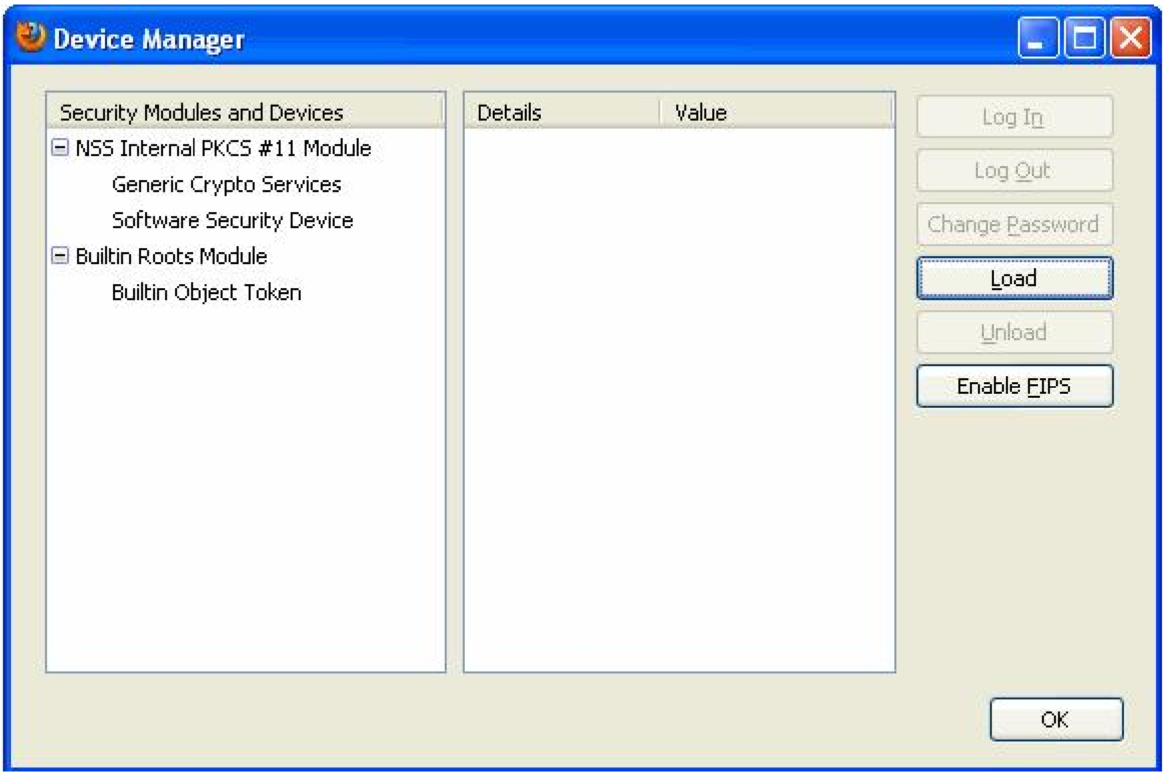
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

Here you have to press the button **Load** to define the path to the Aloaha PKCS #11 Module

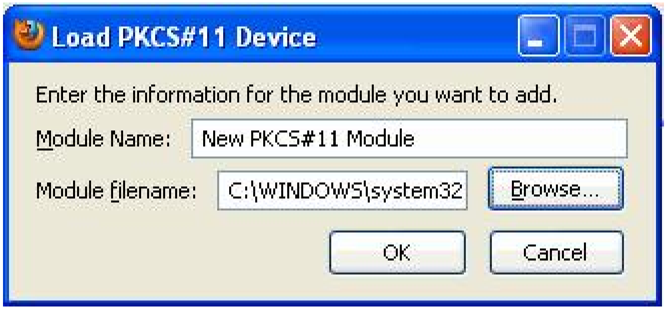


Device Manager

| Security Modules and Devices |
|---|
| ⊟ NSS Internal PKCS #11 Module |
| Generic Crypto Services |
| Software Security Device |
| ⊟ Builtin Roots Module |
| Builtin Object Token |

| Details | Value |
|---|---|

In **Module Name** you can give the Aloaha any Name you wish. In **Module filename** you have to enter the path to the Aloaha Library. It is located in the **`Windows\System32`** directory and is named **`aloaha_pkcs11.dll`**



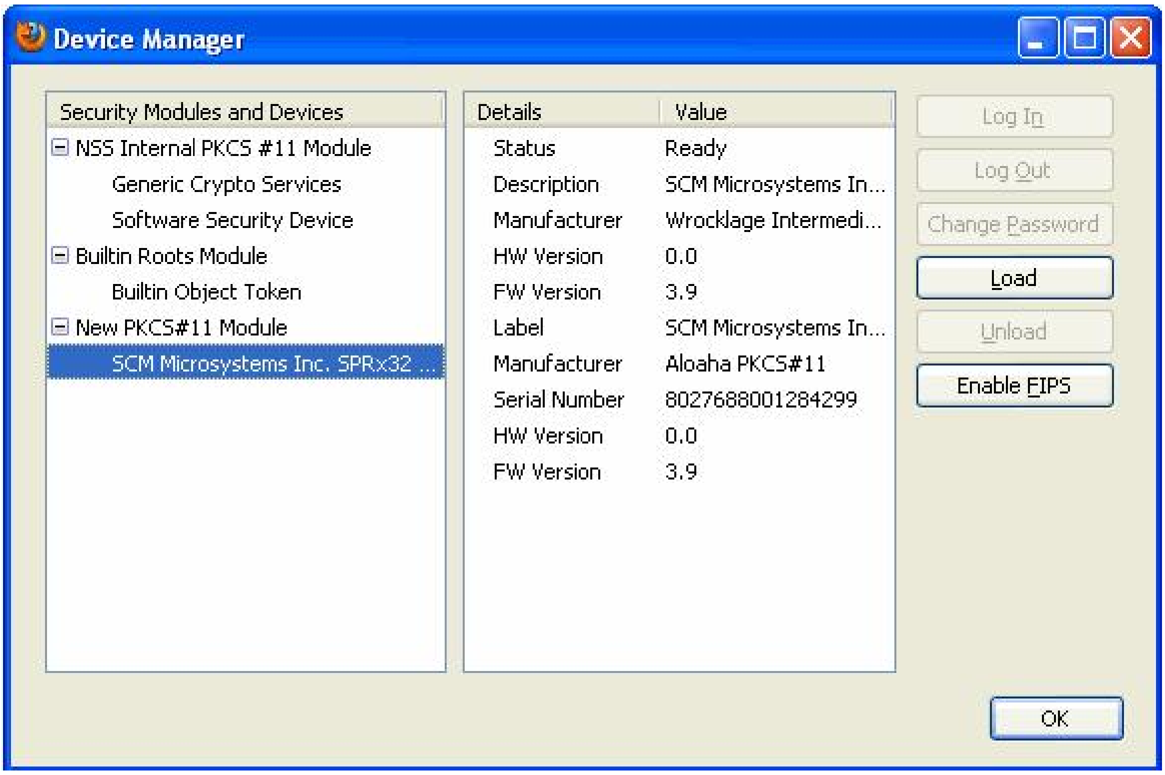
Load PKCS#11 Device

Enter the information for the module you want to add.

Module Name: New PKCS#11 Module

Module filename: C:\WINDOWS\system32

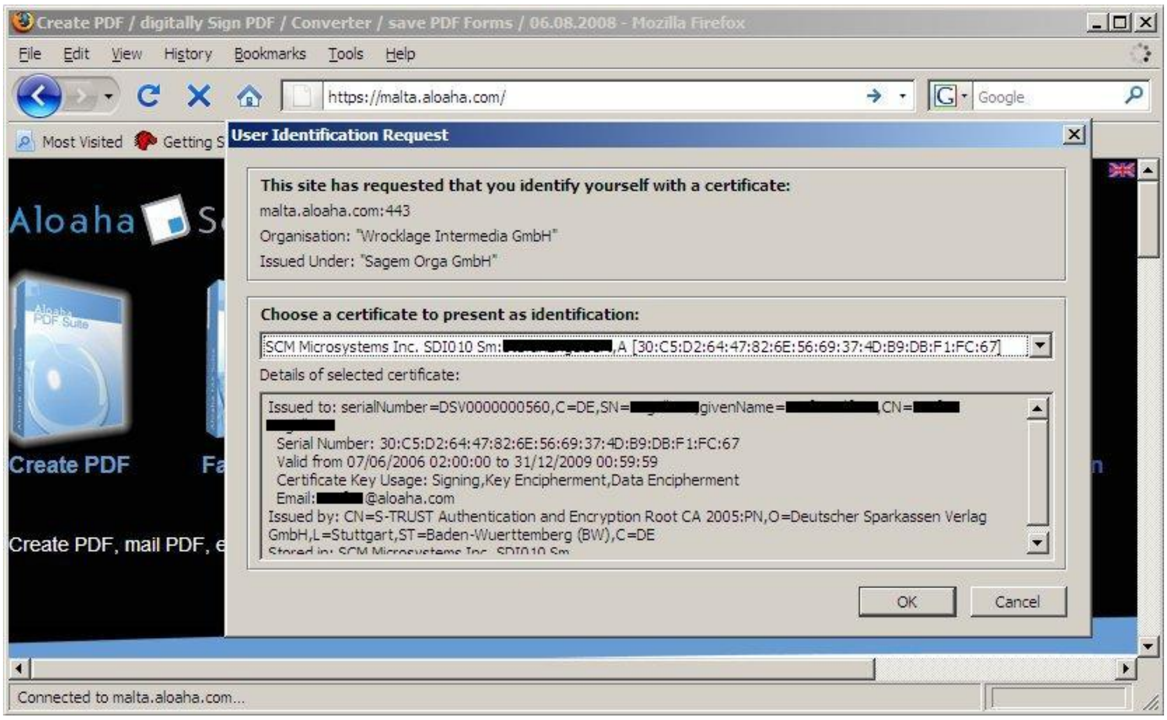
After you confirmed with OK you will see the Device Manager Dialog with the Aloaha PKCS #11 registered.



Security Modules and Devices
- ⊟ NSS Internal PKCS #11 Module
  - Generic Crypto Services
  - Software Security Device
- ⊟ Builtin Roots Module
  - Builtin Object Token
- ⊟ New PKCS#11 Module
  - SCM Microsystems Inc. SPRx32 ...

| Details | Value |
|---|---|
| Status | Ready |
| Description | SCM Microsystems In... |
| Manufacturer | Wrocklage Intermedi... |
| HW Version | 0.0 |
| FW Version | 3.9 |
| Label | SCM Microsystems In... |
| Manufacturer | Aloaha PKCS#11 |
| Serial Number | 8027688001284299 |
| HW Version | 0.0 |
| FW Version | 3.9 |

If you now visit a https which requests a certificate you will the the dialog below. If you do not get that dialog please make sure that your certificate is valid, not expired and contains the right attributes.


Create PDF / digitally Sign PDF / Converter / save PDF Forms / 06.08.2008 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://malta.aloaha.com/
Google
Most Visited
Getting S
Aloaha
Create PDF
Create PDF, mail PDF, e
User Identification Request
OK
Cancel
Connected to malta.aloaha.com...

**This site has requested that you identify yourself with a certificate:**

malta.aloaha.com:443

Organisation: "Wrocklage Intermedia GmbH"

Issued Under: "Sagem Orga GmbH"

**Choose a certificate to present as identification:**

SCM Microsystems Inc. SDI010 Sm:[redacted],A [30:C5:D2:64:47:82:6E:56:69:37:4D:B9:DB:F1:FC:67]

Details of selected certificate:

Issued to: serialNumber=DSV0000000560,C=DE,SN=[redacted]givenName=[redacted],CN=[redacted]
Serial Number: 30:C5:D2:64:47:82:6E:56:69:37:4D:B9:DB:F1:FC:67
Valid from 07/06/2006 02:00:00 to 31/12/2009 00:59:59
Certificate Key Usage: Signing,Key Encipherment,Data Encipherment
Email:[redacted]@aloaha.com
Issued by: CN=S-TRUST Authentication and Encryption Root CA 2005:PN,O=Deutscher Sparkassen Verlag GmbH,L=Stuttgart,ST=Baden-Wuerttemberg (BW),C=DE
Stored in: SCM Microsystems Inc. SDI010 Sm

# 4.3 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 exists 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.

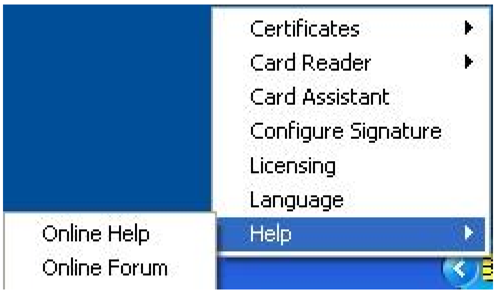
It is also possible to set registry key **`HKLM\Software\Aloaha\pdf\WriteMissing`** to 1. In that case Aloaha will log all Translation Problems to **`MissedLanguage_<ID>.ini`**. This is very usefull to find the strings to be translated for the new language/localisation.

# 5. Help

Thus you reach the online help and the online forum in the Internet: http://www.aloaha.com/support/aloaha-smartcard-connector.php

The online help or the online forum can be launched about Windows start menu or the quick start menu.

Select afterwards the accordingly required menu item.



# 6. FAQ

**FAQ (look also http://www.aloaha.com/support)**

### What is the Aloaha Cardconnector?

The Aloaha Cardconnector provides windows applications access to a variety of smart cards. For example German Health Professional Card (HBA), German Health Insurance Card (eGK), Belgium e-ID (Belpic), Italian Infocamere and Actalis cards, Swiss GS1, and lots of more cards. More supported cards can be found on this website under Support -> Smart Cards

### My card is not supported. What can I do?

Just contact our support. It is always a pleasure to support new cards!

### Which applications are supported?

All applications which access smart cards via CSP (Crypto Service Provider)
or PKCS #11 module are supported by Aloaha. For example Outlook, Internet Explorer, Lotus Notes, Thunderbird, Firefox, Winword, Adobe and more.

### Should I activate the autoremove option in Aloaha?

It depends if you would like to keep the references to a private key in your local certificate store even if you remove the card. If lots of different cards and/or reader are used on one system it is suggested to activate autoremove to increase performance.

### Why do I have the option Configure Signature?

Here you can configure the default certificate or reader used when signing something with the Aloaha PDF Tools or if you right click on a file and choose create XXX Signature/Envelope

### Is it possible to use Aloaha to decrypt a certificate encrypted PDF?

Yes, that is possible. Unlike other CPS Aloaha works also in Adobe 7 and 8.

### Is it possible to use Aloaha to encrypt the NTFS Filesystem?

NTFS Encryption is supported by Aloaha. But it should be noted that the certificates used require special certificate and enhanced certificate attributes.

### Is it possible to disable the shell extension?

Yes, you need to unregister the file AloahaCtxMenu.dll. To do so please go into the aloaha subdirectory of the common program files. There you call regsvr32 /u AloahaCtxMenu.dll.

Now the explorer needs to be restarted. The easiest way is to relogin to the machine.

### Is it possible to hide the blue popup screens?

Yes, you need to create a registry key HKLM\Software\Aloaha\DisableBanner with value 1.

### How can I hide the yellow system tray icon?

You need to create a simple VBS script to show or hide the icon:

```
dim csp

set csp = createobject("AloahaCertInstaller.certserv")

call csp.remove_tray
msgbox "wait"
call csp.add_tray

set csp = nothing
```

### Is it possible to instruct Aloaha to ignore a specific card reader?

Yes, you need to edit the file ReaderIni.ini.

The entry IgnoreReader will instruct Aloaha to ignore that card reader!

```
[SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0]
IgnoreReader=1
```

### Is it possible to avoid the PIN entry?

It is not possible to deactivate the PIN protection of a smartcard. But Aloaha supports the usage of contactless (RFID/Mifare) PIN Token!

**Please do not hesitate to contact us under `aloaha@wrocklage.de`**

# Index