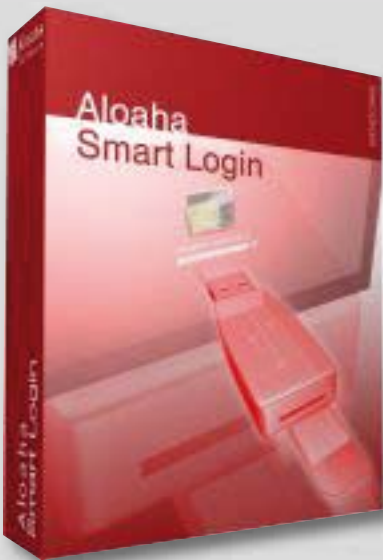




**Aloaha**  
Software

**Aloaha Smart Login – Manual**

# **Aloaha Smart Login Manual**



**Aloaha**  
Software

Wrocklage Intermedia GmbH  
Rudolf-Diesel-Straße 28  
49479 Ibbenbüren

Tel.: 0 54 51 / 9 43 50  
Fax: 0 54 51 / 9 43 5-99

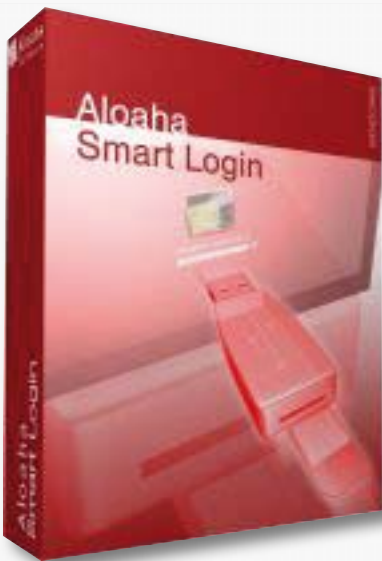


## Contents

<b>1. Aloaha Smart Login</b>	<b>3</b>
<b>2. Installation</b>	<b>4</b>
<b>3. Configuration</b>	<b>5</b>
3.1 Common Settings	6
3.2 Write Certificate	8
3.3 Aloaha Crypt	10
3.4 Smart Login	13
3.5 USB Stick Login	15
3.6 Password Safe	17
<b>4. Usage</b>	<b>19</b>
4.1 Windows Vista and Windows 7	21
4.2 Windows XP and Windows 2000	23
4.3 Set password	24
4.4 Register certificates in the system	25
4.5 Card Assistant	27
4.6 Signature Settings	29
4.7 Digital Signature	33



### 1. Aloaha Smart Login



Aloaha Smart Login is an authentication solution for Windows operating systems. It makes a Windows login with chip cards (smart cards) available under Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 2008, Windows 7 and Windows 2008 R2.

Therefore you will be able to log on to your home or workplace computer with a smart card. Also a log on to websites, for example Outlook Web Access or intranet pages with a chip card is possible.

Additionally, also a Windows login Aloaha Smart CSP, PKCS # 11 and mini driver and integrates the certificates on a smart card fully into the operating system. This way file encryption, email encryption or digital signatures are no longer an issue.

Aloaha Smart Login is based on the supplied Aloaha Smart Card Connector. This software integrates certificates stored on smart cards in the operating system. This way, all Windows applications that can work with certificates, can access the Smart Card. Without the Aloaha Smart Card Connector, the so-called smart card middle-

ware, this is not possible.

You can digitally sign and also encrypt e-mails with Outlook for example. Internet Explorer can use the certificates e.g. to log on to the intranet. Mozilla Firefox and Firebird, Lotus Notes are also able to access the smart card.

It supports nearly 50 different chip cards.

On the following pages you will find all necessary information concerning the operation and configuration.



### 2. Installation

Please download the software Aloaha Smart login from <http://www.aloaha.com/>  
<http://www.aloaha.de/support/asl-installation.php>.

After unpacking and starting the installation follow the instructions in the installation program.

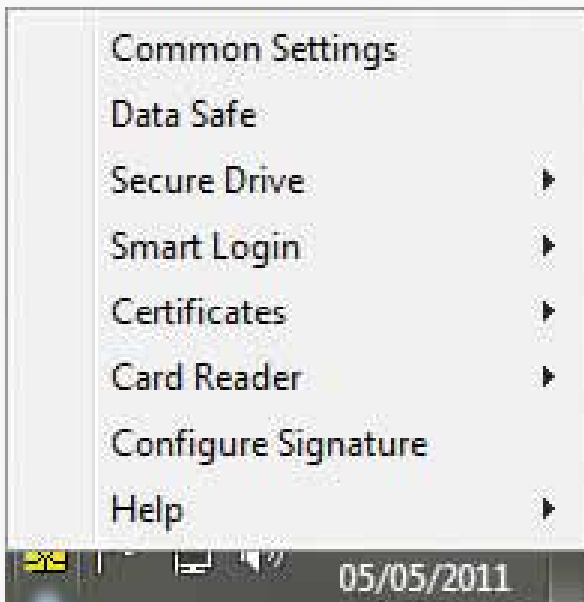


After the completion of the installation there is a small smart card symbol in the Windows taskbar.



### 3. Configuration

If you move the mouse pointer over the icon and click the right mouse button, the following menu appears. This menu is the starting point for all actions and configurations for Aloaha Smart Login. This menu is the starting point for all actions and configurations for Aloaha Smart Login.

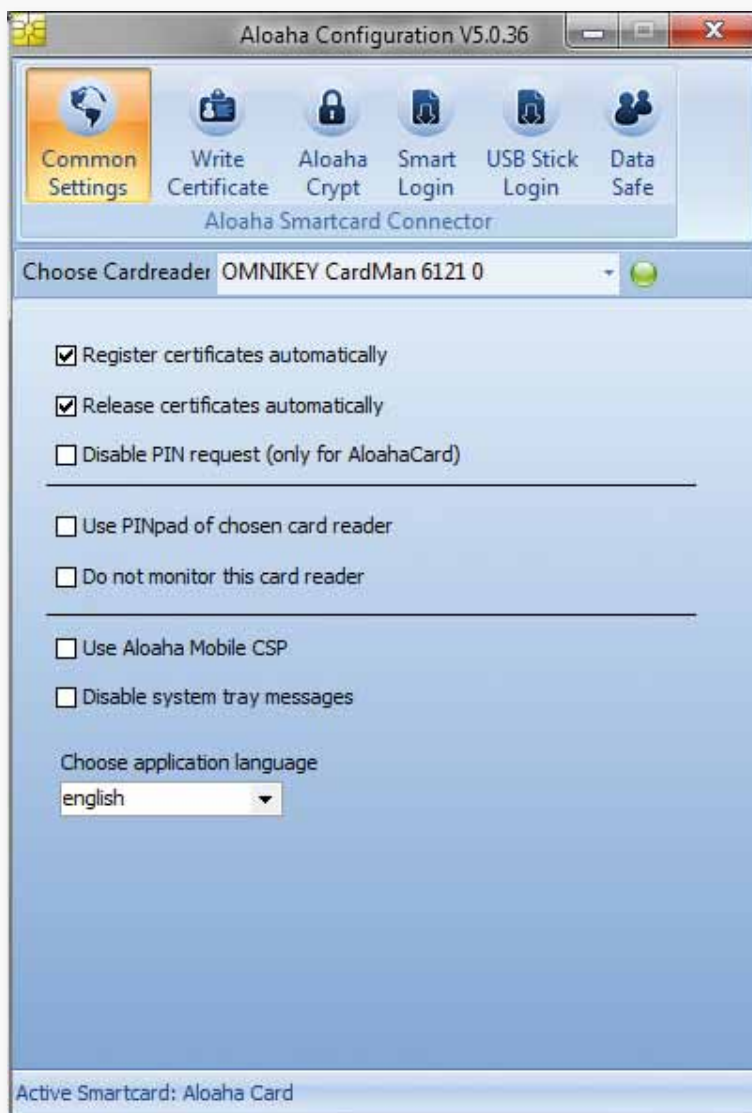


On the following pages each menu item is explained.  
Please select in the left menu, each current menu item entry.



## 3.1 Common Settings

By clicking on the menu item entry you'll get the following window:



in the Aloaha configuration window, click on the individual buttons on top to select the desired setting in the particular area in which you would like to make the changes.

All settings are connected to a chip card certificate. This chip card must be inserted into a chip card reader. The desired chip card reader can be chosen in the selection box under „choose Cardreader“.

In the bottom of the window, the software will show the recognized smart card.



On the page „Common Settings“ you have following configuration possibilities:

### **Register certificates automatically**

If this option is selected, certificates will be automatically registered in the system when inserting a chip card and can then be used directly.

### **Release certificates automatically**

If this option is selected, the certificates will be released, when the chip card is removed from chip card reader. The Programs can no longer find the certificates in the system store.

If this option is not selected, the certificate entries remain in the system. If a program requires a particular certificate, the Aloaha software requests the card with the particular certificate.

### **PIN code request off**

Here you can switch off the query of the smart card PIN. This can be done if the 2-factor authentication is not needed. A login, encryption or decryption process works, without requesting the PIN.

**This is only possible with the Aloaha Card. The safety of the stick is not fully given.**

### **Use the PIN pad of the card reader**

If the selected card reader is a Class 2 or Class 3 reader with PIN pad, you can choose here whether the PIN pad should be used for PIN entry or the computer's keyboard.

### **Do not monitor this card reader**

With several card readers at the computer, it may be reasonable that one particular card reader is not monitored by the Aloaha Software. There is no action (pull/insert again) reported from this card reader.

### **Use Aloaha CSP Mobile**

The underlying Aloaha Crypto Service Provider also exists for mobile end devices. It is possible to use a cell phone as a card reader. The key material is then located on the SIM card (if the mobile operator supports it) or it is stored encrypted in the software of the phone.

### **Disable system menu messages**

The software displays different messages on the lower right monitor screen. These messages can be turned off here.

### **Choose Program language**

Here you select the program language.

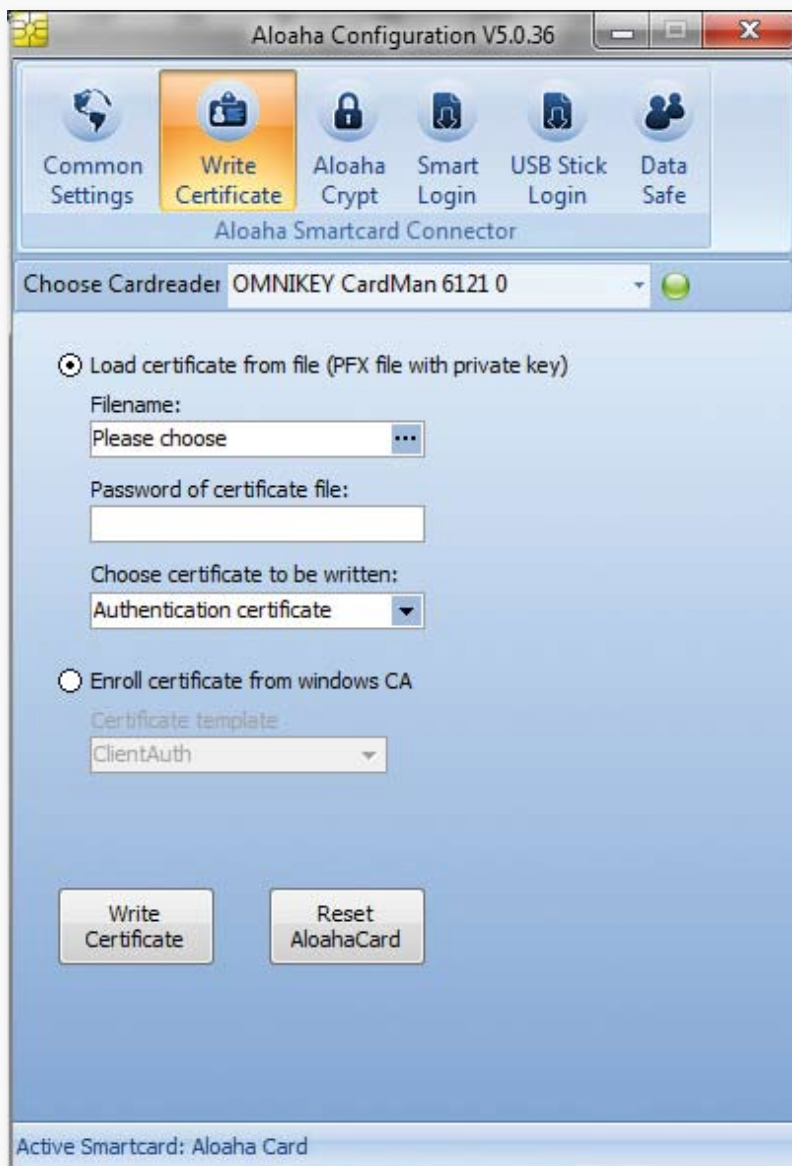


## 3.2 Write Certificate

To use the chip card in the system there must be a certificate existing on the smart card. With the Aloaha configuration, you can write Certificates on the Aloaha Card, Mifare 4k including private key (PFX file) and TCOS 3.0 (without private key. CER file).

### Call the system menu: Certificates -> PFX Writer

By clicking on the menu item entry you'll get following window:





### Certificate from file

Under „File Name“ select the certificate file to be written. Depending on the chip card that has been detected, you can select the following files by clicking on the 3 points at the end of the field:

- **Aloaha Card and Mifare 4k:** .PFX files with private key.
- **TCOS 3.0:** .CER files without private key.

Under „Password of certificate file“ you can enter the password of the certificate file, if available. Under „choose certificate to be written“ you specify which certificate is to be written.

There are the following:

- Authentication certificate
- Signing certificate
- Encryption certificate

### Roll out a certificate from Windows CA

If your computer is a member of an Active Directory domain with an installed Windows CA, you can choose whether a certificate is to be rolled out directly by the CA to the chip card. To do this, select the certificate template that is configured in the CA.

### Write certificate

By clicking this button, the certificate will be written with the above-selected settings. For this purpose a window appears where you need to enter the smart card PIN.

### Reset Aloaha Card

If the chip card that still is in the currently selected smart card reader is a Aloaha Card, this can be set back to the delivery status. **ALL DATA ON THE CARD WILL BE DELETED.**

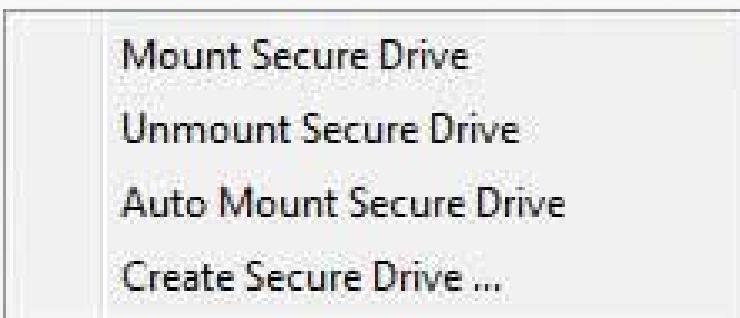


### 3.3 Aloaha Crypt

The software is able to create encrypted disk containers on a single disk. This allows you to encrypt data on hard drives or on removable storage with the smart card.

If such a created drive container is registered with the Aloaha Software, the PIN code enquiry of the smart card shows and if the log in is correct the Secure Drive is used as an additional drive with an additional drive letter in the system.

You access following menu from the system menu item „Secure Drive“:



#### Mount Secure Drive

By clicking on this menu item a Secure Drive is registered. The software automatically checks for the Secure Drive on the drives. At first the removable disk, then the hard drive is searched for Secure Drives. If any are found, the drives will be logged on automatically to the matching registered certificate in the system.

Once a drive has been registered, the menu will change to „unmount Secure Drive“. Please make sure that you log off Secure Drive before unplugging a USB flash drive!

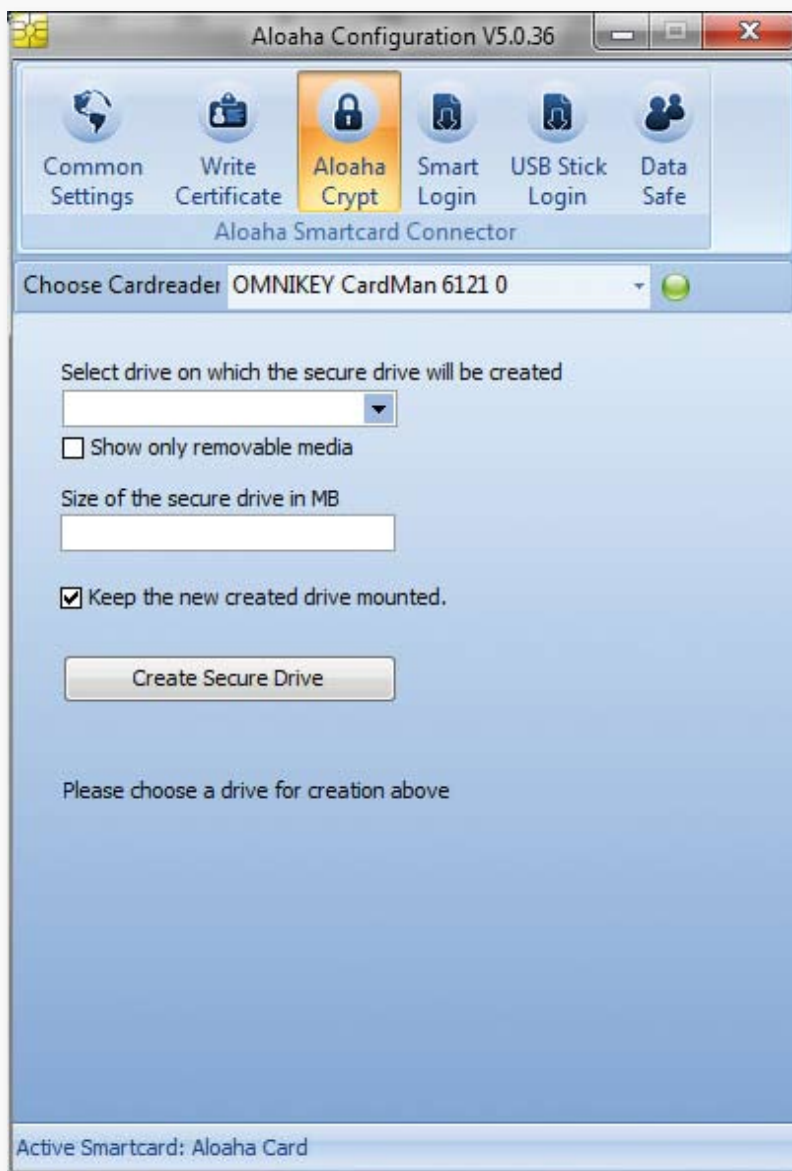
#### Auto Mount Secure Drive

If this option is checked, then the Secure Drive from the USB stick is mounted automatically.



### Create Secure Drive ...

By clicking on the menu item entry you'll get following window:





### **Select drive on which the Secure Drive will be created**

Select the storage location on which the encrypted disk container is to be saved, the carrier drive. If the option „Show only removable disk“ is selected, the selection list only shows removable media including USB sticks and other memory cards. If the option is not selected, then hard drives also appear.

The carrier drive is ALWAYS created in the subdirectory: /aloaha/. This behavior can not be changed.

### **Size of the Secure Drive in MB**

Here you specify the size the Secure Drive should get. Please note that many USB sticks are formatted with the FAT file system at the factory. The maximum size for the Secure Drive is then 2000 MB. With NTFS-formatted disks larger drives are possible.

### **Keep the new created drive mounted**

Use this option to control whether the drive mount on after creation. Then you'll find the Secure Drive as an additional drive with your specified size in the Windows Explorer.

### **Create Secure Drive**

By clicking on this button the Secure Drive is created. You are asked for the chip card PIN and is this entered correctly the creation starts. Please note that the production depending on the selected size like on USB sticks can take a very long time. The compilation will be displayed by the status messages on the lower right screen.



### 3.4 Smart Login

Here you write the Windows credentials to the smart card. If a Aloaha Card or Mifare 4k card is used, the credentials are stored directly on the smart card. With chip cards, which are read-only, the credentials are stored encrypted with the card on the hard disk of the computer.

#### Calling up the System Menu: Smart Login -> Chip Card

By clicking on the menu item entry you'll get following window:



Aloaha Configuration V5.0.36

Common Settings Write Certificate Aloaha Crypt **Smart Login** USB Stick Login Data Safe

Aloaha Smartcard Connector

Choose Cardreader OMNIKEY CardMan 6121 0

### Write Windows Logon credentials to smartcard

Windows username (Domain\user):

Windows password:

Retype Windows password:

Active Smartcard: Aloaha Card



### **Store Windows credentials on smart cards**

Enter in the „Windows User“ the login name that you use for normal registration. On a computer that is member of a Windows domain, you must use the format <Domain>/<user>. By using a computer that is not in a Windows domain, simply type the user name without a preceding domain.

In the „Windows Password“, type your current Windows password. For security, enter the password in the additional field again.

To save the data on the smart card, click on this button.

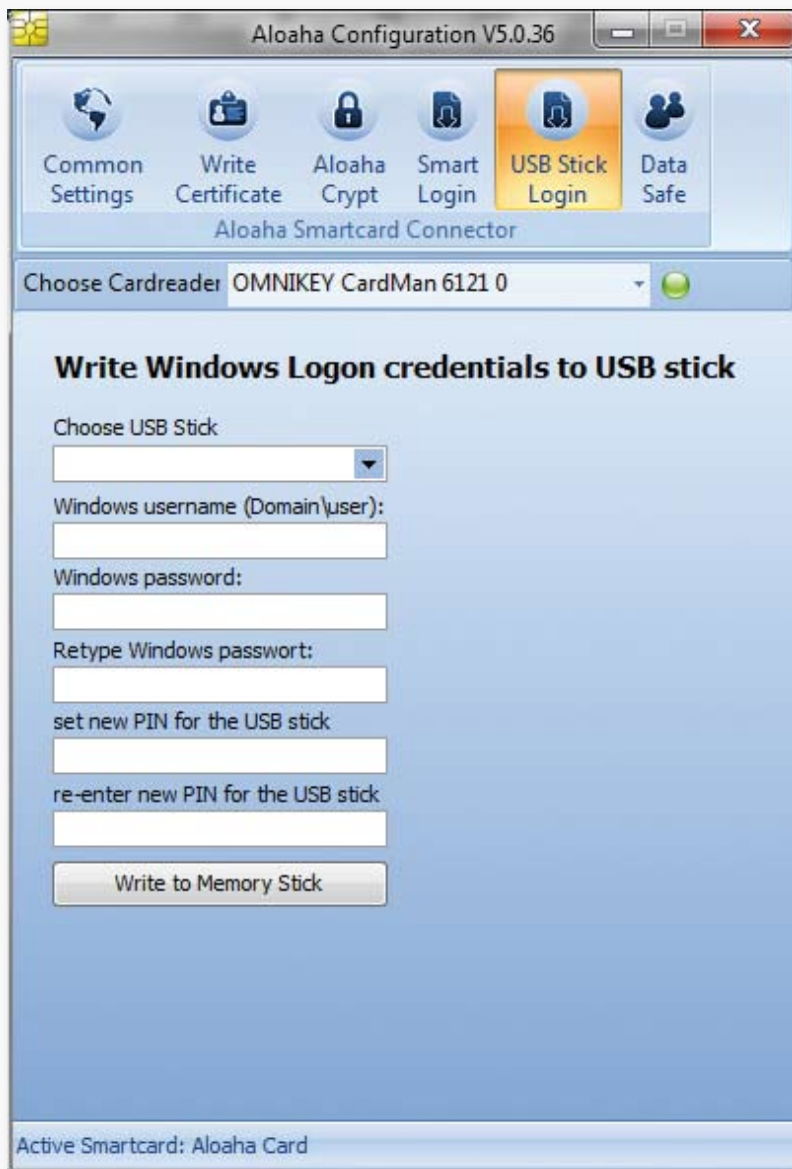


## 3.5 USB stick login

With the software it is possible to use a standard USB memory stick for Windows login. These credentials are encrypted using different features and secured with a PIN.

### Calling up the System Menu: Smart Login -> USB stick

By clicking on the menu item entry you'll get following window:



The screenshot shows the 'Aloaha Configuration V5.0.36' window. At the top, there is a menu bar with icons for 'Common Settings', 'Write Certificate', 'Aloaha Crypt', 'Smart Login', 'USB Stick Login' (highlighted in yellow), and 'Data Safe'. Below the menu bar, there is a dropdown menu for 'Choose Cardreader' set to 'OMNIKEY CardMan 6121 0'. The main area is titled 'Write Windows Logon credentials to USB stick' and contains the following fields and buttons:

- Choose USB Stick:
- Windows username (Domain\user):
- Windows password:
- Retype Windows password:
- set new PIN for the USB stick:
- re-enter new PIN for the USB stick:
- Write to Memory Stick:

At the bottom left, it says 'Active Smartcard: Aloaha Card'.



### **Store Windows login information on USB Stick**

In the selection field „Select USB Stick“ choose your USB stick that should be used for storing the login information.

Then enter in the „Windows username“ the login name that you use for the normal application. On a computer that is located in a Windows domain, you must use the format <Domain>/<user>. On a computer that is not in a domain, simply enter the user name without a preceding domain.

In the field „Windows Password“, type your current Windows password. For security, enter the password in the additional field again.

In the field „set new PIN for the USB Stick“ enter an arbitrary numeric PIN. This PIN will be requested later in the use of the stick. For security, enter the PIN in the additional field again.

### **Save data to USB stick**

To save the data on the USB stick, click on this button.

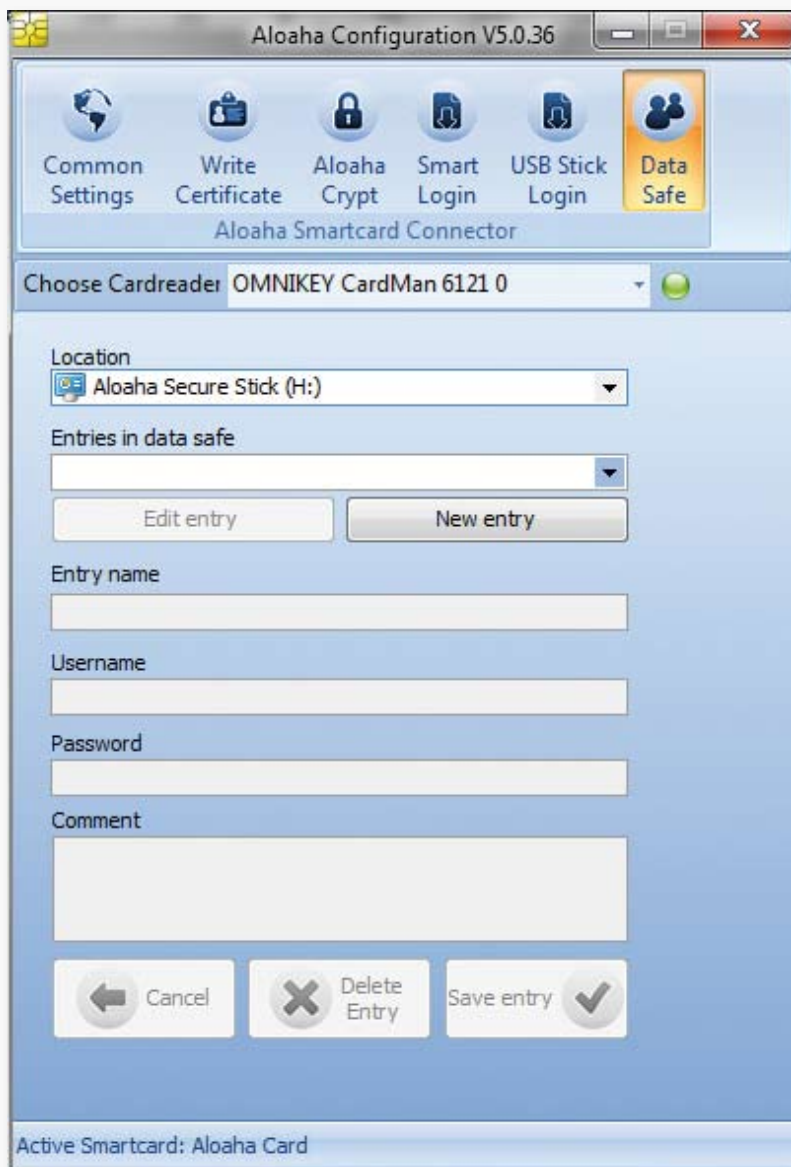


### 3.6 Password Safe

The software offers the possibility of saving credentials from websites or other important data encrypted to the smart card.

Call up the system menu: Password Safe or double-click on the yellow chip card icon in the system menu bar

By clicking on the menu item entry you'll get following window:



The screenshot shows the 'Aloaha Configuration V5.0.36' window. At the top, there is a menu bar with icons for 'Common Settings', 'Write Certificate', 'Aloaha Crypt', 'Smart Login', 'USB Stick Login', and 'Data Safe'. Below the menu bar, there is a section for 'Aloaha Smartcard Connector' with a dropdown menu for 'Choose Cardreader' set to 'OMNIKEY CardMan 6121 0'. The main area contains several input fields: 'Location' (set to 'Aloaha Secure Stick (H:)'), 'Entries in data safe' (a dropdown menu), 'Entry name', 'Username', 'Password', and 'Comment'. At the bottom, there are three buttons: 'Cancel', 'Delete Entry', and 'Save entry'. A status bar at the very bottom indicates 'Active Smartcard: Aloaha Card'.



### **Location**

Choose the memory location for the password safe. This can be any place in the system on a network drive or be on USB sticks and other portable devices.

### **Entries in data safe**

This box contains the entries of the currently selected memory location. By initial pop-up you'll be asked for the PIN of the smart card and with correct input, all entries are listed.

### **Entry name**

Use this field to assign a name for the entry. It can be a web address, a bank PIN or other for example. This keyword appears in the entries list when all entries are listed. Example: <http://www.onlinebanking.bankxy.de>

### **Username**

Enter the user name or other entries. Example: Konto123

### **Password**

Here enter the password or other entries. Example: pass123

### **Comment**

Enter a comment or other useful data. Example: TAN 1: 123456, TAN 2: 789 012

### **New Entry**

This button creates a new entry in the selected memory location. If there is no data safe yet then a new data safe is created.

### **Cancel**

Closes a currently open entry without saving it.

### **Delete Entry**

Deletes the currently selected entry.

### **Save entry**

Saves the currently selected entry including the made changes.

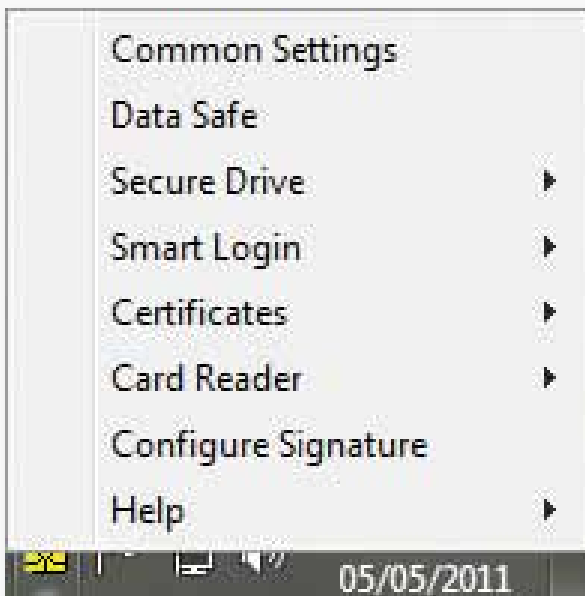


### 4. Usage

The software Aloaha Smart Login operates in basically in secret. If a program is accessing certificates or makes other actions, status messages appear on the right bottom of the screen:



The access to the settings or if a certificate is to be registered, is via the menu. This will open with a right click on the smart card icon, which is in the lower right corner.





### **Password Safe ...**

Use this to go directly to the configuration and to view and manage the entries in the password safe.

**See: Configuration -> Password Safe (page 17)**

### **Secure Drive**

Settings and configuration of Secure Drive.

**See: Configuration -> Smart Login (page 13)**

### **Certificates**

Click here for the registration and the settings of Certificates.

**See: Usage - Register Certificates in the system (page 25)**

### **Card Reader**

Click here for the registration and the settings of Certificates.

**See: Usage - Register Certificates in the system (page 25)**

### **Card Assistant**

Learn how to set card and modify and activate PIN's.

**see: Usage - Card Assistant (page 27)**

### **Configure signature**

Here are the settings for the digital signature made

**see: Usage - Digital Signature (page 33)**



### 4.1 Windows Vista and Windows 7

Aloaha Smart Login adds an additional registration button to the login screen on Windows Vista and Windows 7.





## Aloaha Smart Login – Manual

With a click on the login button the Authentication path Aloaha Smart Login is selected.



At this point, you enter your Windows user name and the matching PIN to your smart card to log on to the system.

This is necessary because up to 63 user data fit on the Aloaha Card.

However, you can leave both fields blank. The software will find the correct user related to various features. Either there is only one user stored, or it uses the last user name.



### 4.2 Windows XP and Windows 2000

Under Windows XP, the Aloaha Smart Login is installed similar. Here, however, the whole login screen from the Aloaha Smart Login is adapted.



But the login screen behaves exactly as described previously.

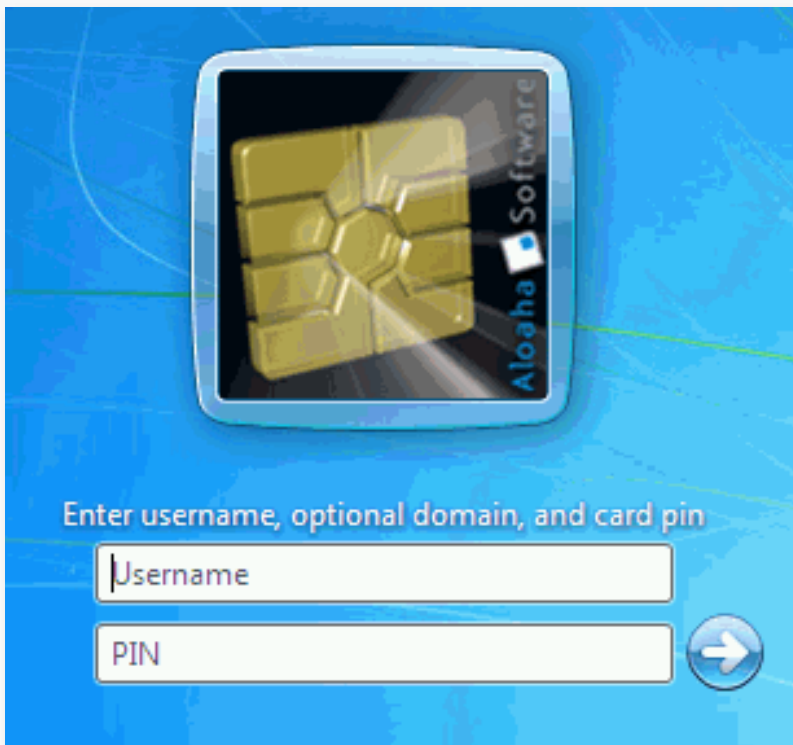
If the „log on with user name and password“ option is chosen, you can also log in with the traditional user name and password. This option can be disabled so that you can always log on only by a chip card.



### 4.3 Set Password

User data and passwords can be set in various ways. Once, the user data is set in the configuration. **The call in the system menu: Smart Login -> smart card.**

Another possibility is to directly set user the data in the home screen.



Type your user name in the username Window. If you use a computer in an Active Directory domain, enter the user name in the format \. To save an encrypted password, enter „SETPASS: „ followed by the password in the second field (PIN).

#### **Example: SETPASS: letmein**

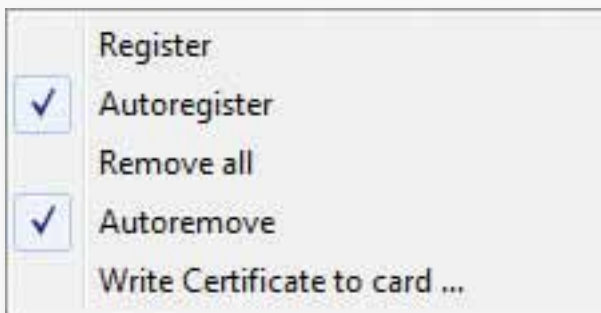
The software encrypts the password with the certificate of the smart card and stores it locally. If the Aloaha Card is taken, the data is also encrypted and stored on the card.

In Windows XP, this function is identical.



### 4.4 Register Certificates in the system

To register Certificates in the system, select the menu item certificates in the system menu. You will see a sub menu where you'll find the following items:



#### Register Certificates automatically when you insert a card

If this option is selected, the certificates on the smart card automatically register in the system with useable applications when you insert a smart card.

#### Remove all with Aloaha registered certificates

By clicking on this menu item all registered certificates with Aloaha are removed from the system. These can no longer be used by applications.

#### Release Certificates on removal of a card automatically

If this option is selected, the registrations are automatically canceled in the system when a card is removed.

#### ! Note!

If the certificates are not removed from the system applications can still list these certificates. If these are used, the software requests the Aloaha Smart Card, on which the certificates are to be found.

#### Write Certificate on smart card ...

It will open the appropriate page of the configuration.

**See: Configuration -> Write Certificate**



### Register Zetifikat in the system

The following window appears:



It lists all certificates on all the system connected card readers. The entries include the number of the card reader on which the certificate is located (1 point). The 2nd Figure indicates the type of certificate, with type 0 = signature certificate, type 1 = authentication certificate, type 2 = encryption certificate. If a Card only contains one certificate, it will be displayed as type 1. This is followed by the name (CN) in the certificate and the fingerprint of the certificate as a hexadecimal string.

In some cases there are several card readers associated with one system. Enumerate the certificates of all readers, takes time. In this case, you can use the card reader (as shown) directly. Aloaha then only reads the certificates of the selected card reader.

By double clicking on the relevant certificate it is registered in the system. Right-click on the relevant certificate, a context menu is displayed, where you also can view the entire certificate.

### The registration in this manual has the following advantages:

- If the root certificate is not available in the system, Aloaha will try to download it from the Internet.
- The selected certificate is automatically set as the default certificate for the Aloaha applications.



### 4.5 Card Assistant

The Aloaha Card Assistant is accessed from the system menu and it allows you to manage PINs and unlock various cards from Nullpin or Transportpin status.

By opening the selection menu for the card reader, you can select the available card reader in the system. After clicking on Re-Connect the information from the connected card can be read.





## PIN management

By using the drop down menu „PIN management“, you can select, change or reset the signing PIN, card PIN and PIN home. The name of the PIN's, unfortunately, differ from card manufacturer to card manufacturer. For the names we have chosen the most common terms.

After clicking on „Change PIN“ one of these two windows appear:

If the chosen card reader has a PIN Pad:



If the chosen card reader has no PIN pad:



Please follow the instructions on the screen and enter the old pin and 2 x is a freely chosen new PIN and enter it from the keypad of the card reader or from the keyboard of your computer.



### 4.6 Signature Settings

By clicking on „Configure signature“ in the System Menu the dialog opens for setting the signature.



#### Certificate source

Here you can choose between different types of certificates that you want to use to sign your PDF files.

The choices are:

- Local Machine Store
  - All certificates are shown in the list that are assigned to the computer.
- Current User Store (default)
  - All certificates are shown in the list that are associated with the current user.
- Active Directory Store
  - All certificates are shown in the list that are in Active Directory.
- Smart Card (e-ID)
  - All certificates connected to the card reader are shown in the list.

#### Type of certificate

Here you can filter the list of displayed certificates with certificate-specific attributes.

If the certificate source „Smart Card“ is selected, you can choose between SHA-1 and SHA-256 as a signature algorithm. SHA-256 is safer and more valid, but not all chip cards can operate this algorithm.



### Select Certificate

This menu depends on the certificate source. If you select „Current User Store“, you get a list of all user certificates on your PC in this field and you can select the appropriate certificate.

Select the the smart card (e-ID) as certificate, all current smart card readers installed on your computer will be listed. The Aloaha Card Connector automatically detects the inserted smart card in the card reader and can read the certificates of supported cards.

### The purpose of the signature

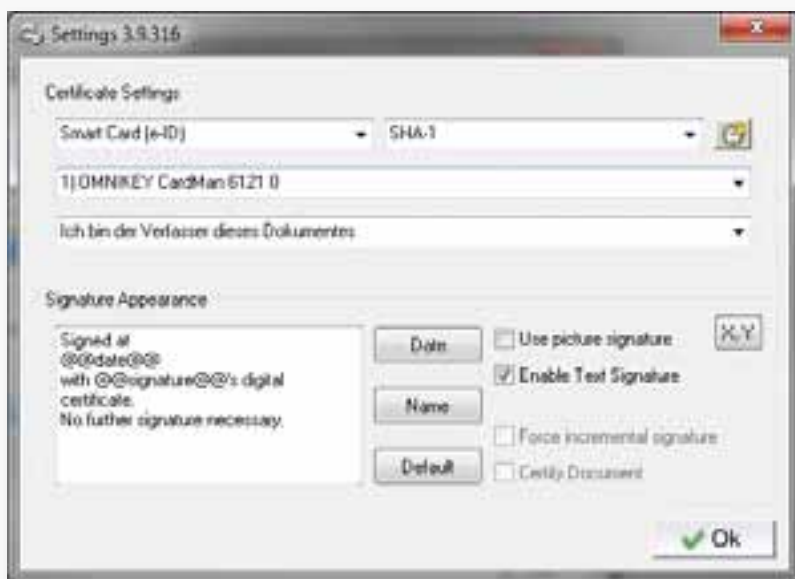
The following options are available:

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

You can also enter free text.

### Text signature

If the option „use signature text“ is selected, the entered text in the box that appears is inserted into the PDF. You have the option by clicking on „Date“ and „name“ to insert a placeholder for the date and name at the current cursor position. During the signature process the placeholders are replaced with the current date and the name of the certificate.





### Caption

You still have the option of signing the document with a caption. If this box checked, an image is used in the PDF, as it shows the preview in this dialog box. By clicking on the display of the current signature image, you can upload your own image file from your hard disk. This image must be in the 24-bit JPG format, and is then set as an image in the PDF.



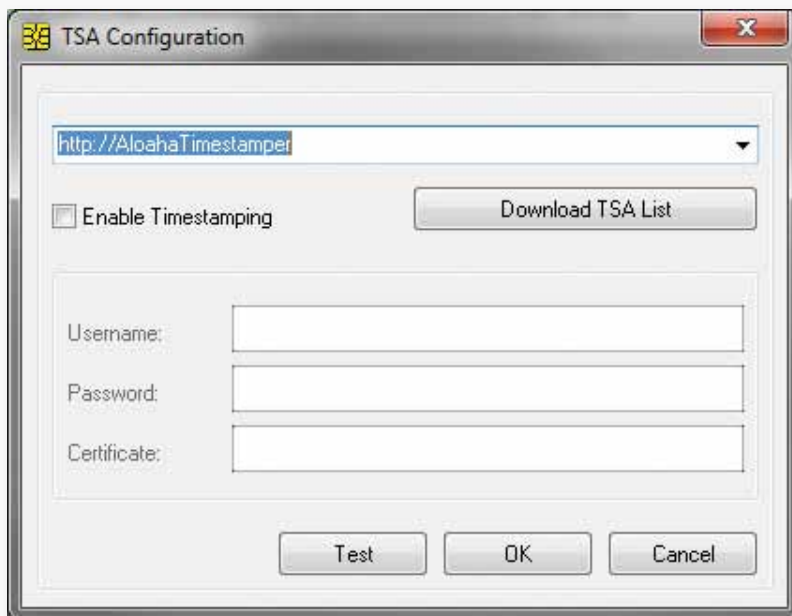
### Incremental signature requires

Aloaha will sign the document incrementally. The signature is attached to the document in a way that you can always revert to the original document.



### Settings for the time stamp

If you click on the clock icon on the top right in the signature configuration menu the window below is shown for the time stamp settings:



Here you can adjust the settings for the built-RFC 3161 compatible time stamp client. In the upper box you can select an available time stamp server. If the list is empty, you can load a list of possible time stamp server by clicking on the button „Load TSA list of servers“ from the Aloaha Web Site. If you select <http://AloahaTimestamper>, the timestamp server is used. The local system time is taken as the basis for the time stamp. Under User data you can configure your access to the respective time stamp.

Many time-stamp authorities are not RFC 3161 compatible, so Aloaha does not allow users to edit the entries themselves. For further entries, you may write to [aloaha@wrocklage.de](mailto:aloaha@wrocklage.de)



### 4.7 Digital Signature

The Aloaha Software integrates with the installation in the Windows Explorer. You can call up a file context menu with a right-click in the Explorer:



The Aloaha Shell extension allows the user to create a PKCS#7 signature and a PKCS # 7 signature envelope. Aloaha uses the Signature settings which are configured in the settings dialog.

In the event that the Aloaha PDF Signator or Aloaha PDF Suite are installed and licensed on the same computer, a third entry for the creation of a PDF signature is available. With a right-click on a PDF file and select this menu item, the PDF is digitally signed. Later the Signatures can be checked in the Adobe Reader or by any program that can handle PDF signatures properly.