Charismathics Smart Security Interface™

V4.3

Manual

Contents

1. Preface

Congratulations on your purchase of **Charismathics Smart Security Interface (CSSI)**!

Charismathics Smart Security Interface provides modules that you need in order to integrate different smart cards and TPM chips in to your applications, beginning with functions for the administration of the card, up to modules supporting the operating system to use the smart card. The following file structures (profiles) are supported:

- Charismathics corporate profile
- PKCS#15 profile
- Carta Nazionale dei Servizi (CNS) profile

Charismathics Smart Security Interface comprises the following modules:

- the administration tool *Charismathics Smart Security Interface Manager*
- the user tool *Charismathics Smart Security Interface Utility*
- the *Register Tool* for the automatic registration of the certificates
- the CSP
- the PKCS#11-module
- the TSS module for TPM chips (optional)

With the user tool *Charismathics Smart Security Interface Utility* you can change your user PIN and register your smart card. You can manage your keys and certificates of the smart card with the administration tool *Charismathics Smart Security Interface Manager*. You can generate, import or export keys and certificates on a smart card. Furthermore, you can display information about the contents of a smart card, change the PIN of the smart card, unlock the smart card and create new profiles.

Charismathics Smart Security Interface-CSP enables you to enhance applications and services in a Microsoft environment and their use with a smart card.

Charismathics Smart Security Interface-PKCS#11 enables you to use additional applications and services, that use this standard. PKCS#11-Modules are in use e.g. by Netscape and in Novell environments.

Especially you can augment the following applications by smart card applications:

- smart card login to Windows Domains or Novell eDirectory
- SSL- Authentication by smart card (Internet Explorer, Netscape, …)

- email security with cards (PGP, Netscape Messenger, Outlook, Outlook Express, …)
- VPN with smart cards (Microsoft, Cisco, …)

This manual is meant for system administrators and users that are entrusted with these tasks. Application developers, who develop their own applications that access modules of **Charismathics Smart Security Interface**, e.g. PKCS#11, will find additional information in Appendix A.

2. About this Manual

This manual begins with a description how to install **Charismathics Smart Security Interface**.

If you have acquired **Charismathics Smart Security Interface** in the admin edition, you will find a description of the administration tool. It contains: how to manage keys and certificates, changing PINs, unlocking, initializing and personalizing smart cards.

If you have acquired **Charismathics Smart Security Interface** in the user edition, you will find a description of the user tool. It contains: how to change PINs and register your smart card.

Furthermore, you will find more precise information regarding the Register Tool, CSP and PKSC#11 and which applications can be employed with smart cards. A reference part consolidates your knowledge. Application developers can find further information in appendix A how to access modules (e.g. accessing PKCS#11) of **Charismathics Smart Security Interface**, if they intent to develop a proprietary application. Appendix B is a concise description of the certificate attributes, i.e. information about key employment.

However, there is no explanation how to configure environments of Microsoft or other producers. In these cases, please consult the documentation of the corresponding producer.

***NOTE**: To understand this manual you need basic knowledge in IT-security. Especially, you should be familiar with the following notions: certificate, private, public, and secret key, digital signature, PKI, etc. If you want to consolidate your knowledge in IT-security and cryptography, there are informations in the service area of the charismathics homepage: http://www.charismathics.com/*

3. Installation

Before you can install **Charismathics Smart Security Interface** the card reader you purchased must be installed according to the producer's guidelines and be fully operative. The installation of **Charismathics Smart Security Interface** is run from the program CD. Please execute the file SETUP.EXE as a user with administrator rights. Follow the installation instructions.

3.1. Installation Requirements

If not explicitly required otherwise in the following:

Microsoft Windows NT 4.0 with Service Pack 6a
or Windows 2000 with Service Pack 4
or Windows XP with Service Pack 2
or Windows Server 2003
or Windows Vista

Note: *During the installation the CSP Module is registered automatically in the Windows operating system. If there is a Netscape/Firefox version on your computer, there will be the possibility to register the PKCS#11 Module in the Netscape Navigator over the file "InstallNetscapePKCS11.html". With the help of the file "UninstallNetscapePKCS11.html" this procedure can be cancelled each time*.

Further the following applications are supported:

- Smart card login to a Windows 2000 or 2003-Domain:
  ADS, Enterprise CA, Windows 2000 or 2003 Server and as Client: Windows 2000 Professional or Windows XP Professional

- SSL- Authentication with smart card using Internet Explorer:
  Microsoft Internet Explorer 5.0, 5.5 or 6.0, High Encryption Pack, SSL V3 with Strong User Authentication

- Outlook with digital signature and encryption via smart card:
  Outlook Express 5.0, 5.5 or 6.0
  Windows Mail
  resp. Outlook 2000, 2003

- Lotus Notes with digital signature and encryption via smart card:
  Lotus Notes 6.5 or higher

- Windows VPN-Login with smart card:
  Windows 2000 Server and as Client: Windows 2000 Professional or
  Windows 2003 Server and as Client: Windows 2000 or XP
- Smart card login to Novell eDirectory:
  Netware 5.1 SP3, eDirectory 8.6.1, Novell Client 4.83 SP1, NMAS EE 2.0 (with the included Universal Smartcard Login Method) with NICI 1.5.7 (Server and Client), NMAS 2.1 (with the included Universal Smartcard Login Method) with NICI 2.4.1 (Server and Client) or higher in each case

- Smart card login to Lotus Notes:
  Lotus Notes 6.5 or higher

- SSL- Authentication with smart card with Netscape:
  Netscape Navigator 4.72 (High Encryption), 4.73, 4.76, 6.x

- Email-Security via smart cards with the Netscape Messenger:
  Netscape Messenger 4.72 (High Encryption), 4.73, 4.76, 7.x
  Thunderbird 1.5

- E-Mail-Security via PGP support (PKCS#11): PGP Personal Desktop 8.1 for Windows

- Compatibility/Smart card administration of the Baltimore-PKI (PKCS#11): Token Manager für Betrusted Unicert V5.2 for Windows

- Compatibility/Smart card administration of the Entrust-PKI (PKCS#11): Security Manager Administration 7.0

.

The products serving as examples do not need any further client requirements; please observe in case of other products the corresponding manuals.

3.2. Supported Smart Cards

Charismathics Smart Security Interface supports the following smart cards/tokens:

- CardOS M4.01
- CardOS M4.01a
- CardOS V4.2

- CardOS 4.2b
- CardOS V4.3
- CardOS V4.3b
- Aladdin eToken
- ACOS EMV A03
- JCOP 20
- JCOP 30
- JCOP 21
- JCOP 31
- JCOP 41
- StarCOS 3.0
- Sm@rtCafe 2.0, 2.1, 3.0
- GemXpresso Pro R3.2
- NetKey PKS/2000/E4
- ActivIdentity Card

and TPM chips:

- Infineon TPM 1.1 & 1.2
- Broadcom TPM 1.1 & 1.2

3.3. Tested Card Readers

Please observe, that your PC/SC smartcard reader has been installed according to the producer's specifications and is operating. **Charismathics Smart Security Interface** has been tested with the following card readers:

- SCM SCR241 PCMCIA
- SCM SCR331 USB
- SCM SCR333
- SCM SCR335 USB
- SCM SCR532 seriell/USB
- Omnikey Cardman 1010 seriell
- Omnikey Cardman 2011 seriell
- Omnikey Cardman 2020 USB
- Omnikey Cardman 3121 USB
- Omnikey Cardman 3620 USB
- ACS38 USB

- ORGA Card Mouse USB
- Fujtsu Siemens Computer Smartcase SCR USB
- Fujtsu Siemens Computer Smartcase SCR USB internal
- Fujtsu Siemens Computer Smartcase KB SCR PRO
- Fujtsu Siemens Computer Smartcase KBPC CX
- Fujtsu Siemens Computer Smartcase Token USB
- SCM SCR 3340 (Express-Card)
- Omnikey Cardmann CM4040 (PC-Card)

Note:

- Only PC/SC-drivers are supported. There is no support for CT-API-drivers.
- If RSA 2048 bit key shall be used, then the smartcard reader must support the extended APDU.

3.4. Unattended Installation

Instead of calling setup.exe, the installation can be started in the unattended mode by calling the corresponding msi file:

```
msiexec /i product.msi /qn
```

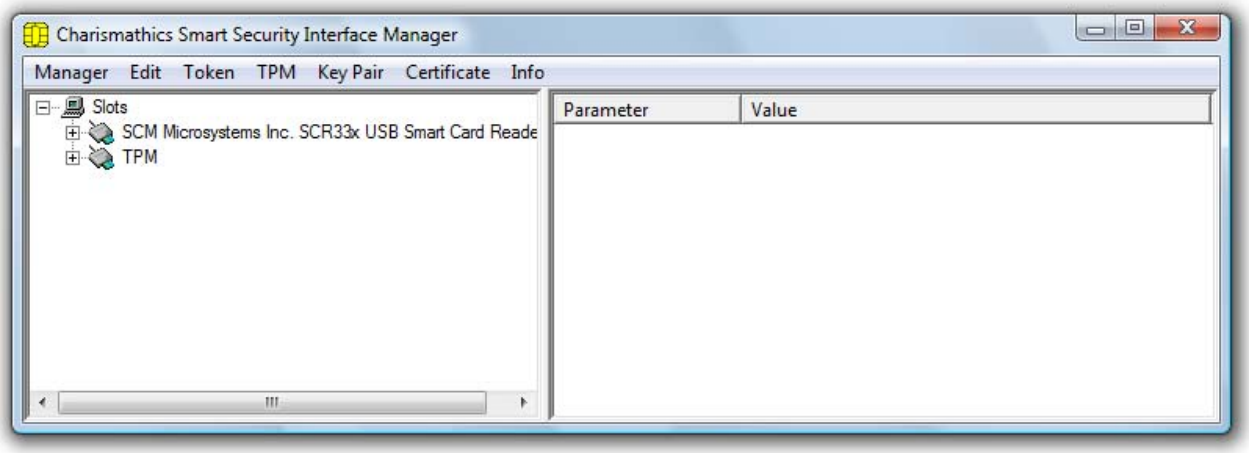
in the setup, where the product name is for example “CSSI 4.3 - admin edition.msi”.

4. Administration Tool: Charismathics Smart Security Interface Manager

If you acquired **Charismathics Smart Security Interface** in the Admin edition, this tool offers the following functions: changing your PINs, unlocking smart cards, generating profiles, keys and certificates and so on. These functions are now described.

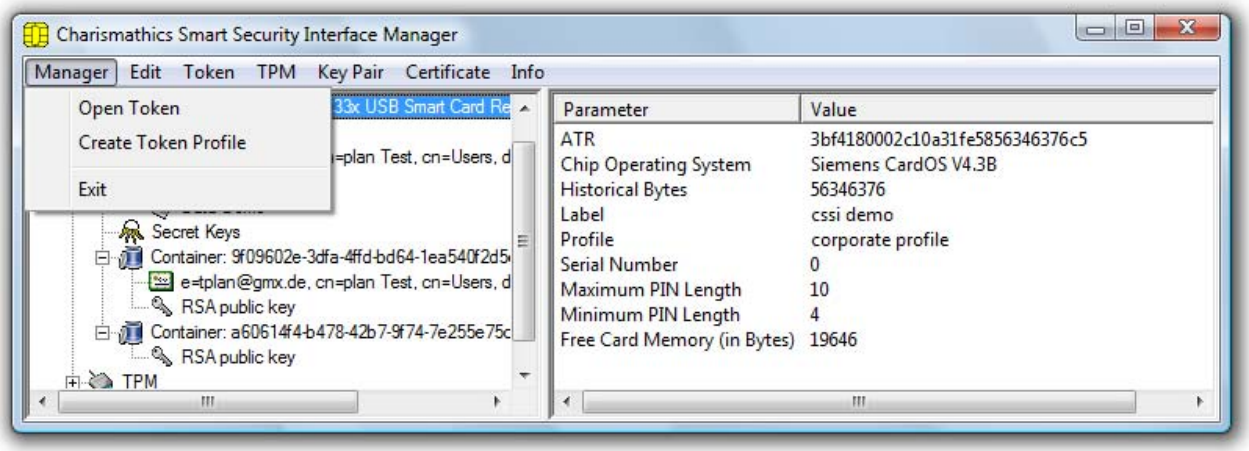
4.1. User Interface

After opening the administration tool of **Charismathics Smart Security Interface** you will see the following interface. The "TPM" Menu item is only visible if the optional TSS module has been installed and TPM hardware is present



The left panel displays the list of smart card readers which are connected to the system. Once a smart card has been inserted, the hierarchy is extended. Selecting an item in the hierarchy view displays its properties in the right hand panel. The properties are displayed in tabular form with, parameter and its associated value.

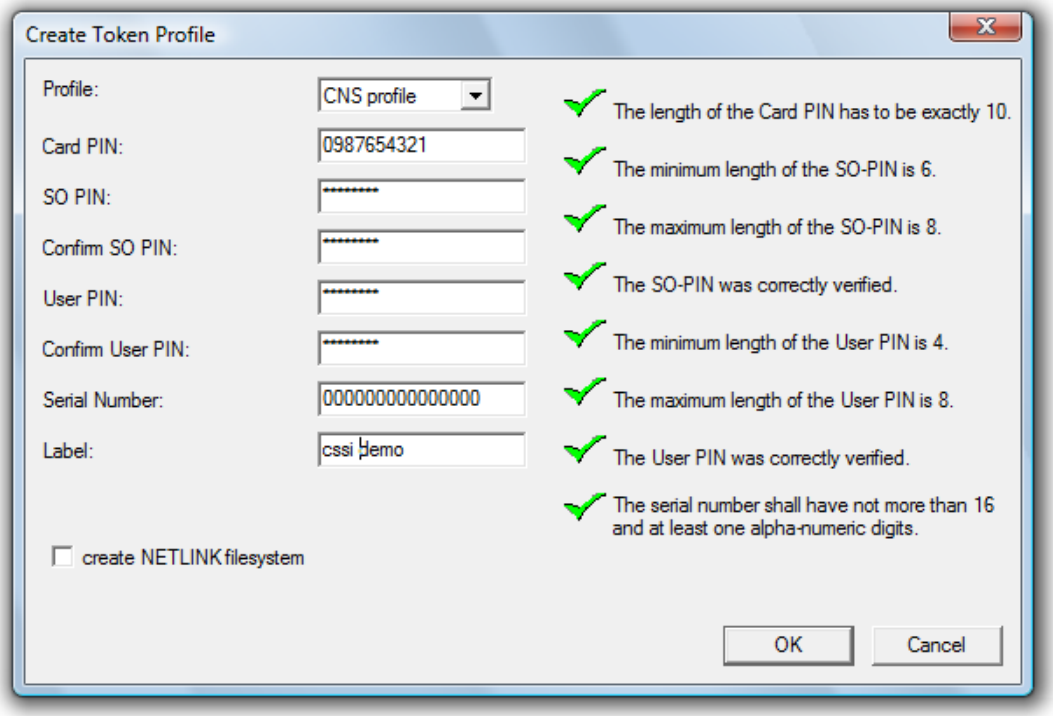
Manager menu



- "Open Token": To view the contents of a smart card, select the reader which contains the smart card from the hierarchy and select "Open Token" from the "Manager" menu. Clicking the plus-icon in from of the reader to expand the hierarchy serves the same purpose.
  At first, only public information is available, e.g. name of the smart card, the profile and

free card memory. In this example, it is a CardOS V4.3B smart card with the corporate profile. Furthermore, certificates, public keys, container and data are displayed.

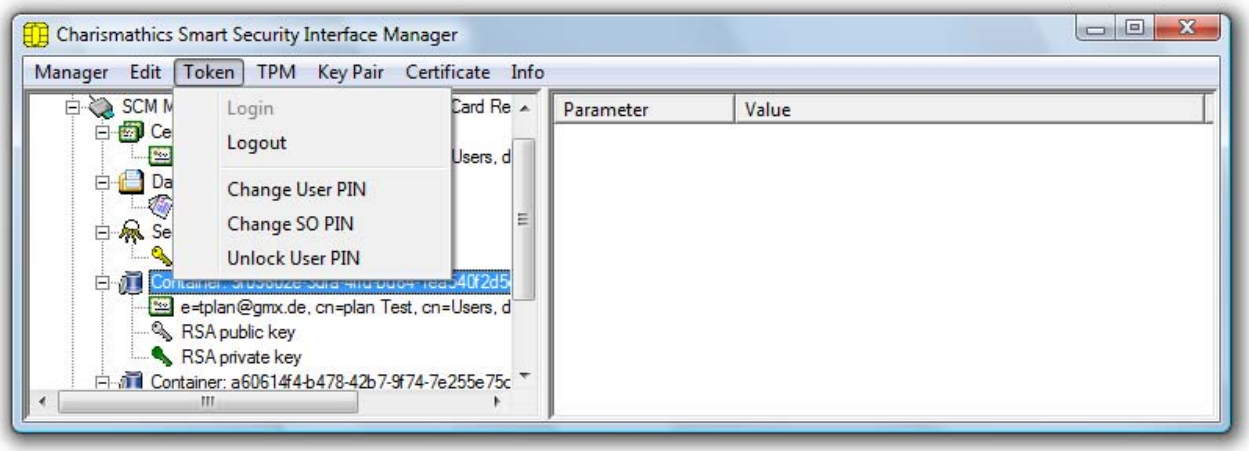
- "Create Token Profile": This option deletes the current profile, if present, and creates a new one on the smart card. This feature is described in detail in 4.7 Preparing a Smart Card (Initialization and Personalization)



Edit menu/ Context menu

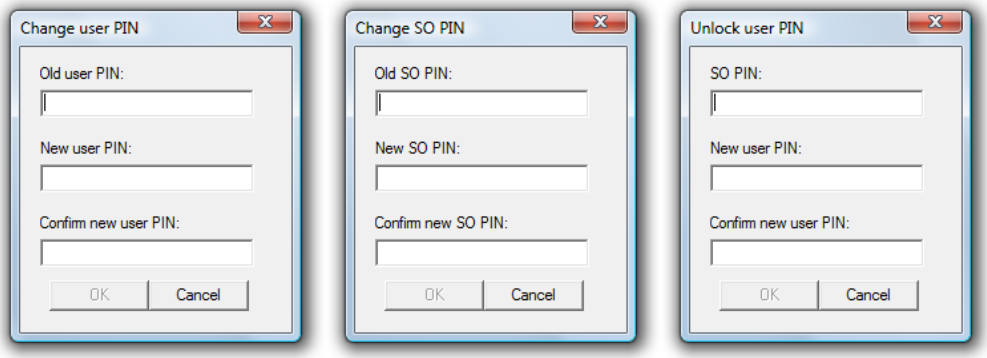
The content and availability of the "Edit" menu changes according to the item selected in the main hierarchy view. Most functions of the "Edit" menu are also accessible by right-clicking an item in the hierarchy. See also 4.9 Further Functions

Token menu



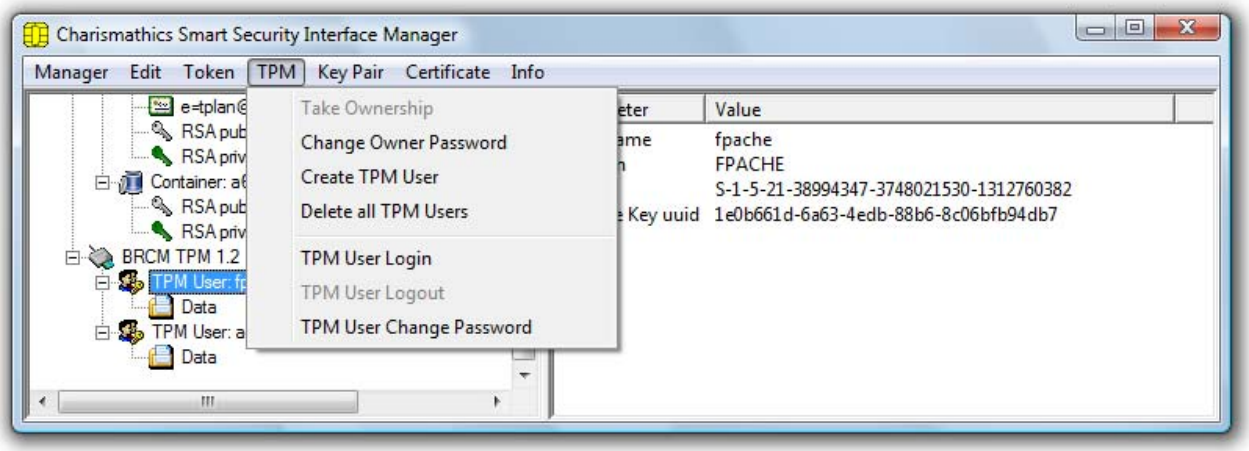
For the "Token" menu to contain any active entries, the Token must have been opened in advance e.g. by using "Manager"→"Open Token".

- “Login”: Operations on the card require the user to log in to the card. Logging in requires entering the User Pin. Once logged in, this option is disabled and additional information becomes available, both within the hierarchy and the properties view. Failing to enter the correct User PIN three times in a row locks the card. See “Unlock User PIN” on how to clear the lock.
  After successfully logging in to the token, certificates on the card can be registered with the windows certificate store. For each certificate which is not yet registered with the certificate store but stored on the token a dialog opens asking the user whether the certificate is to be registered.
- “Logout”: This item works analogous to the “Login” option.
- “Change User PIN”/ “Change SO PIN”/ “Unlock User PIN”



These functions work very similar to each other. These functions are always available and all require an authorization PIN to make a change. The changed value has to be entered twice to avoid typographic errors. All values are masked with asterisks to provide privacy.

TPM menu



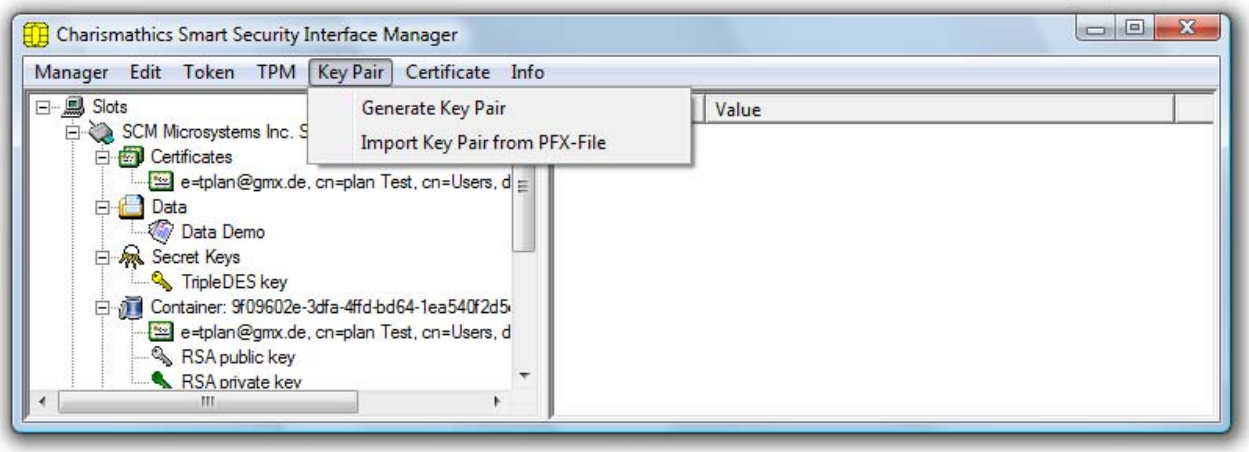
The TPM menu is only visible if the optional TSS module has been installed. The functions of the menu require that a TPM hardware has been selected in the hierarchy view. See also 4.8 TPM Management

- “Take Ownership”: this option is only available if Ownership of the TPM module has not yet been taken. Ownership is required for functions like TPM User creation and to work. Taking Ownership of the TPM requires the User to enter a password. This password is only required for operations concerning the TPM itself. There is no option to give up Ownership from within the CSSI. Refer to the documentation of the TPM regarding this matter.

- “Change Owner Password”: This function asks for the current Owner Password and the new Owner Password, which has to be repeated, to change the Owner Password.
- “Create TPM User”: The CSSI admin editor permits the creation of multiple TPM User accounts. A TPM User is required to have the same name as a Windows account, otherwise the creation will fail. For any user to be able to use the TPM as a secure storage, a TPM User must have been created in advance using this function.
- “Delete all TPM Users”: This option removes all Users after asking for confirmation. Deleting individual users is possible by selecting the TPM User in the hierarchy view and selecting “Delete TPM User” from either the “Edit” menu or the right-click context menu
- “TPM User Login”: Logging in to the TPM User allows importing key pairs from .pfx files using the “Key Pair” → “Import Key Pair from PFX-File”. Login to the TPM requires the current password of the user
- “TPM User Logout”: This function works analogous to “TPM User Login”
- “TPM User Change Password”: Changing the TPM User password requires entering the current password once and the new password twice.

There are no options to unlock TPM passwords since TPM does not use password locking when a password it entered incorrectly, regardless of the number of failed attempts

Key Pair menu



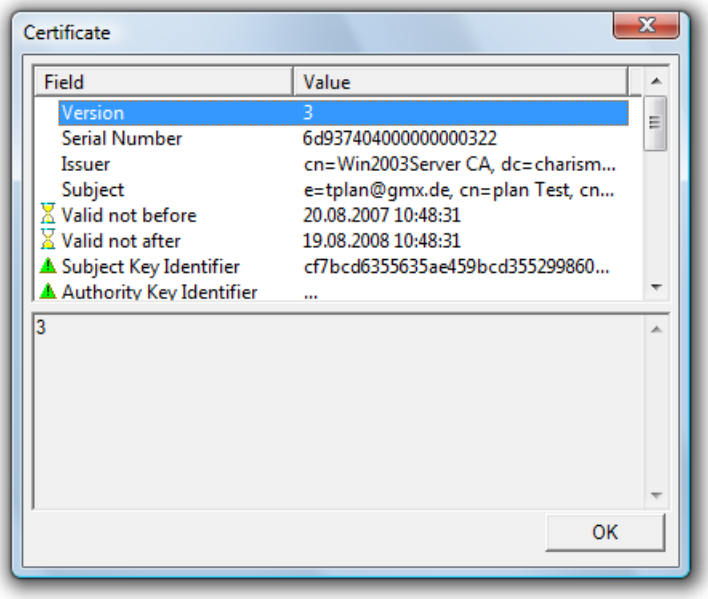
It is possible to generate several key pairs with corresponding certificates on the card. Each set comprised of private key, public key(optional) and certificate(optional) is stored in a separate container.

- “Generate Key Pair”: Keys can only be created on the token if the user has logged in before. Once a key pair has been created it can be used for a number of purposes. See also 4.4 Generating and Importing Keys and 4.5 Generation and Import of Certificates
- “Import Key Pair from PFX-File”: This item opens a dialog asking for the the PFX file to import.

Certificate menu

Most items of the certificate menu are also accessible from the context menu when a certificate, public or private key, the “Certificates” node in the hierarchy etc. are right-clicked.

- “Import Certificate”: After selecting this item, pick the certificate to import form the opened dialog. If the certificate can be associated with a private/public key pair, it is automatically inserted into the right container. Otherwise the certificate is added to the general “Certificates” node in the hierarchy. There is no way of manually associating a certificate with an unrelated key pair
- “Show Certificate”: Displays all information contained within the certificate. Select a field name in the upper half of the viewer to display the value in the lower half

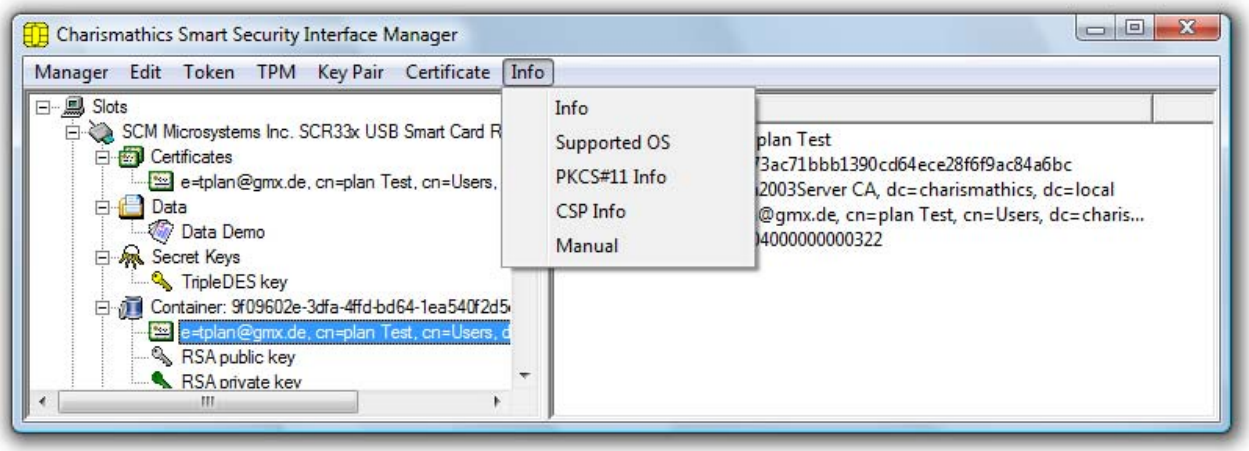


- “Export Certificate”: Exports the certificate in either BASE64 or DER format to a file of the users choosing. The association with the key pair is recovered once the certificate is imported again via “Import Certificate”
- “Register Certificate”: This option registers the certificate with windows, if not already done.
- “Create Certificate Request”: In order to receive a certificate for a private/public key pair, it is possible to prepare a certificate request. This request is stored in a BASE53 or DER

encoded file. Refer to 4.5 Generation and Import of Certificates for an description of the process

- “Create self-signed Certificate”: The requesting process is similar to the one in “Create Certificate Request”. However the request is not stored to a filed to be processed by a CA, but instead singed by the requesting.

Info menu



- “Info”: Displays general version information about the CSSI admin edition
- “Supported OS”: Displays the list of smart card operating systems supported by CSSI. This list includes only the predefined associations. Associations made with the CSSI Extension Tool (7 Charismathics Extension Tool)
- “PKCS#11 Info”: Displays Information on the PKCS#11 module, which ships with CSSI
- “CSP Info”: Information on the CSP
- “Manual”: This manual

4.2. Changing PINs

There are 3 PINs on a CardOS smart card: the User PIN, the SO PIN (PIN of the system operator, i.e. system administrator) and the Card-PIN. There are different functions to use with these 3 PINs:

The **User PIN** must be entered, if one wants to write on the card (e.g. key generation, storing a certificate), delete objects or when the cryptographic functions (e.g. signing or decryption) are used. The minimal length of the User PIN is four characters and the maximal length is ten characters. The Default-PIN is "11111111" (these are 8 ones).

IMPORTANT: *After three consecutive wrong inputs the User PIN will be locked.*

A locked User PIN can be unlocked by the **SO PIN**, which is also known as the PUK. The length of the SO PIN is fixed to ten characters. The Default-PIN is "1111111111" (these are 10 ones).

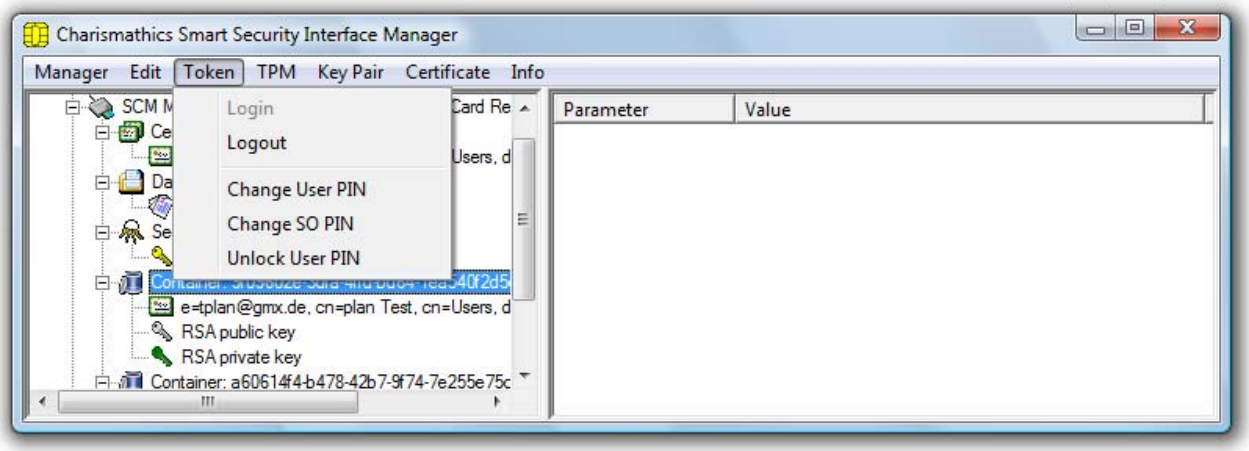
The SO PIN is used solely for unlocking the User PIN. There are no functions like Create or Delete.

IMPORTANT: *After ten consecutive wrong inputs the SO PIN will be locked.*

With the **Card-PIN** it is possible to delete an existing profile on a card by setting up a new profile. The Card-PIN will be determined during the initialization and can only be changed afterwards by creating a new. The length of the Card-PIN is ten characters.

IMPORTANT: *After ten consecutive wrong inputs the PIN is locked and the card cannot be deleted anymore. I.e. if the Card-PIN, the SO PIN and the User PIN are locked, the card is useless.*

You find all functions to change User and SO PIN in the menu "Token", as shown in the following figure:

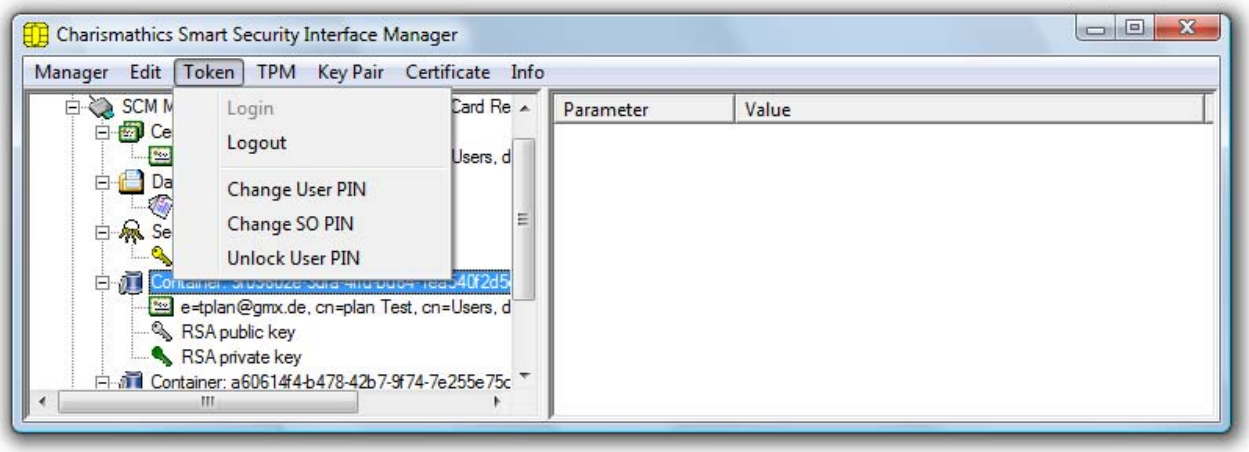


4.3. Unlocking Smart Cards

As a security measure a smart card will be locked, if a user enters a wrong PIN three times in a row. This provides security, because an unauthorized person could otherwise check all possible PINs by trial and error if you lost your smart card or it has been stolen.

But it might happen that you have entered the wrong PIN three times even as legitimate owner of the smart card. In this case the smart card will be locked as well. Therefore, you can unlock the smart card with **Charismathics Smart Security Interface**, if you know the SO PIN.

You need the SO PIN to unlock a User PIN. You find the function "Unlock User PIN" in the menu "Token", as shown in the following figure:



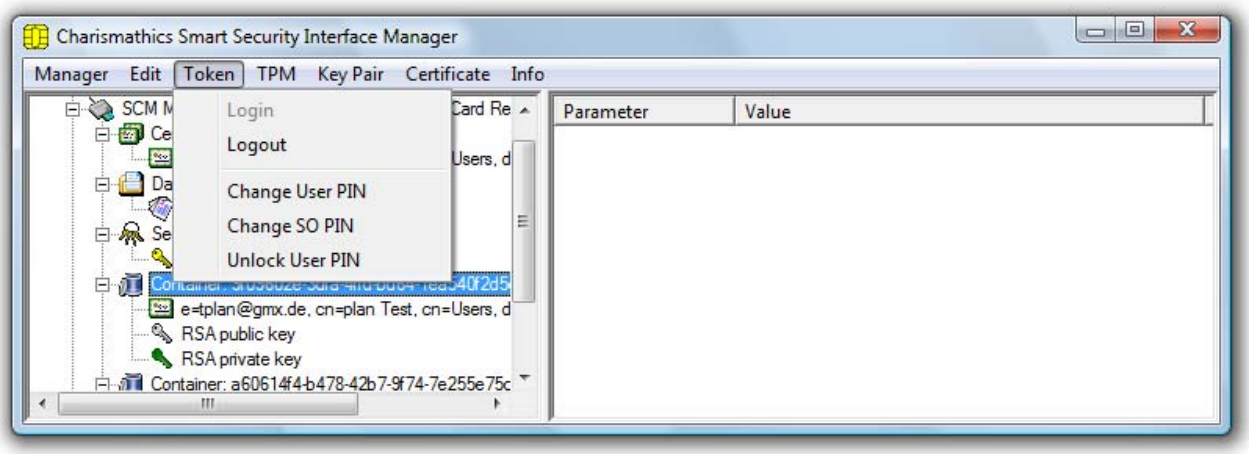
4.4. Generating and Importing Keys

To use the smart card for digital signatures or encryption, you need a key pair, which is composed of a private and a public key. The private key must be stored very secretly and the public key must be accessible to communication partners by a certificate. These keys and certificates can be generated and managed by the administration tool.

In principle there are two possibilities:

1. You can generate keys (key pairs comprising private and public keys and secret keys) with the administration tool of **Charismathics Smart Security Interface**.
2. You already own a key and/or key pair. Then, you can import the key pair if necessary together with certificate as a PFX-file. You can store Secret Keys by importing them e.g. with "Copy and Paste".

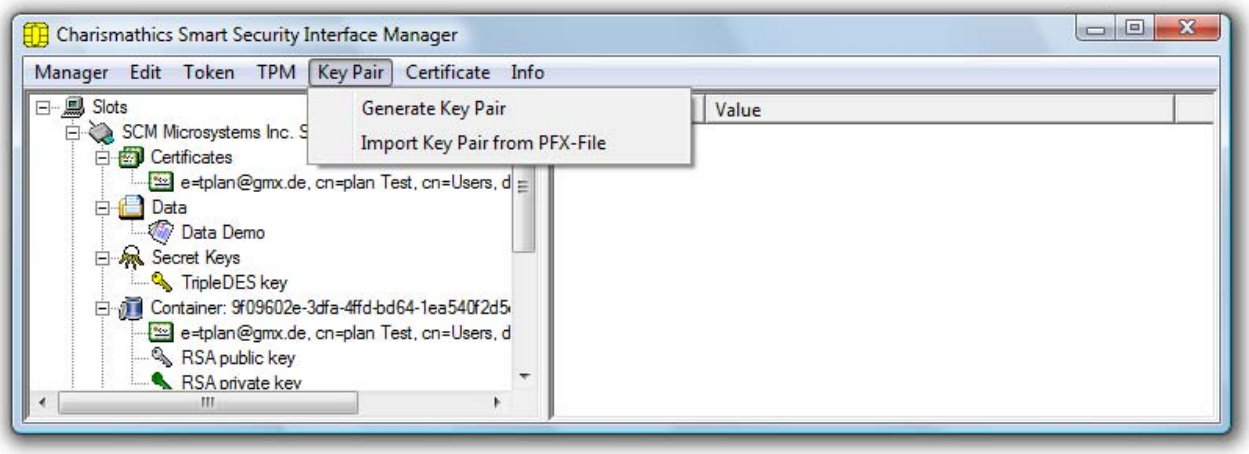
Use of these functions requires that you are logged in to the smart card: From the menu "Token", select the entry "Login" and enter your User PIN



You can find all the functions to generate and import keys in the menu "Key Pair" and to import certificates in the menu “Certificates”,.

Generation a Key Pair

The generation of a key pair (private and public key) is started from the menu "Key Pair" via the item "Generate Key Pair". Once the generation process is finished, you see these keys in the administration tool in the corresponding container under "public key" and under "private key".



If you have a CardOS M4.01, M4.01a or V4.20 smart card they are RSA keys with 512 or 1024 bit. If you have a CardOS V4.30 smart card you can additionally generate RSA-keys with 1536 or 2048 bit. To generate RSA keys with 2048 bit on a CardOS V4.20 smart card you need a package. There exists also aprofile with ECC support for CardOS M4.01a, which supports curves up to 256 bit length.

Importing a Key Pair

If you already own a key pair, that you intend to use, you can import it in the menu "Key Pair", selecting the item "Import Key Pair from PFX-File". The method requires you to enter your password for the file.

Remark: The key must be an RSA-key within a .pfx- or .p12-file.

Generation of a Secret Key

To generate a secret key for encryption, highlight “Secret Keys” and select the item “Generate Secret Key” in the menu “Edit” or the context menu

Here, you can generate a Triple-DES-key with 192 bits, a Triple-DES-key with 128 bits or a DES-key with 64 bits.

Algorithm	Key strength	Note
Triple-DES	192 bit	
Triple-DES	128 bit	
DES	64	Not recomended

***Note**: Algorithms with at least 128 bits (Triple-DES) are recommended. According to present day standards, lesser key lengths can not be considered as secure any more.*

Importing a Secret Key

If you own a secret key, that you want to use, you can import it in the menu "Edit" via the menu item "Store Secret Key". The Secret Key must be specified in hexadecimal representation and be of the correct length: 192 or 128 bits for Triple-DES and 64 bits for DES. Please note that a single

hex-digit covers 4 bit. Importing takes place by inserting the bits into the field "Secret Key (hexa-decimal)", e.g. copy and paste.

4.5. Generation and Import of Certificates

In order to use the smart card for digital signatures or encryption you need a key pair comprised of a private key and a public key. The public key should be accessible to communication partners by a certificate. These certificates can be generated and managed by the administration tool.

In principle there are several possibilities:

1. You can sign the certificate corresponding to a public key by your self or make a certificate request, such that another instance e.g. a trust center will authenticate the public key.
2. You already have a key and/or certificates. Then, you can import certificates, if needed together with the corresponding key.

Generating self signed Certificates and Certificate Requests

You can generate the certificate belonging to a public key by signing it yourself or make a certificate request, such that another instance e.g. a trust center authenticates the public key. To this end you highlight the Private Key and select one of the “Create…” entries from the “Certificates” menu.

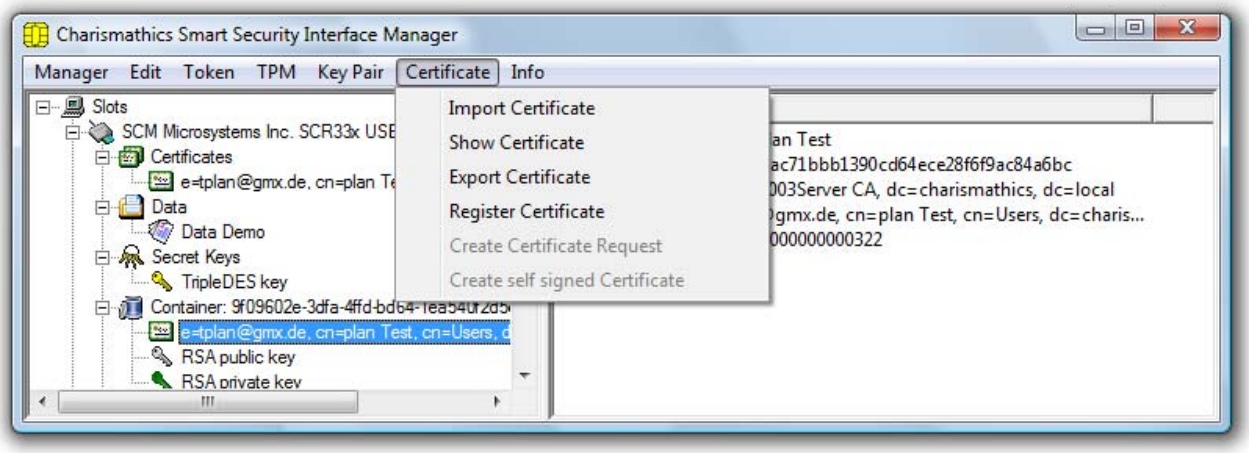
In order to generate the certificate, resp. request you enter the data into the corresponding fields. In case of a certificate request you create a file to send it to the authority, that should sign the certificate (e.g. trust center). Therefore you store the request as a p10-file in a directory and follow the instructions of the corresponding authority intended to sign the certificate.

Once the certificate has been returned by the issuer, you have to import the certificate using the menu item "Import Certificate".

Note: *There is an explanation of the certificate attributes and how to employ the keys in the appendix B of this manual.*

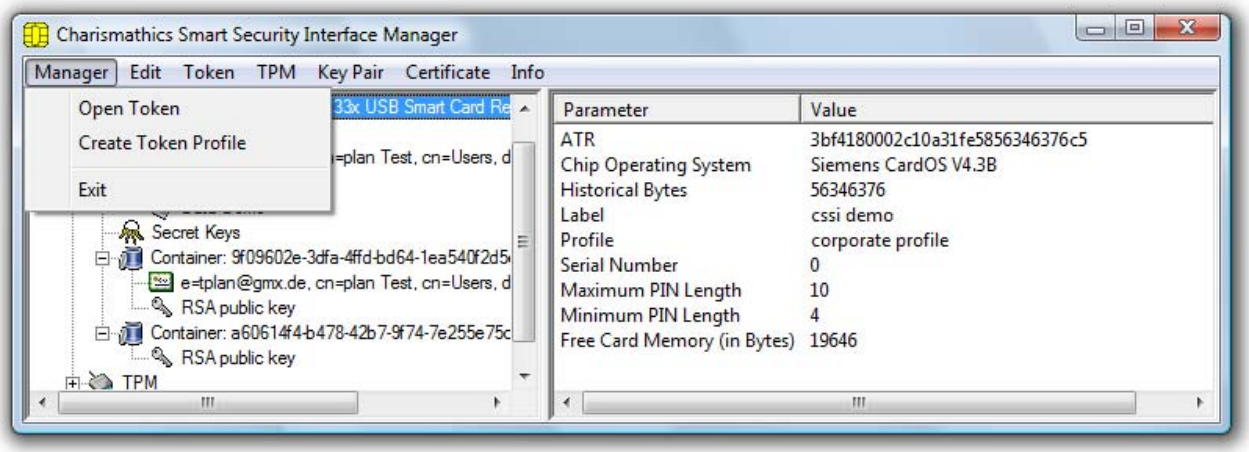
Import of Certificates

In case you already own certificates, that you intent to employ, you can import them over the menu "Certificate" over the item "Import Certificate". Certificates, which belong to key pairs, are directly assigned to the associated "container" after the import. Certificates without keys - as for example CA certificates - are assigned to the file "Certificates".



4.6. Creating Profiles …

If you want to use a smart card, there must be a profile on this smart card. In a first step you have to setup the corporate profile on this smart card. Click the menu "Manager"→"Create Token Profile".



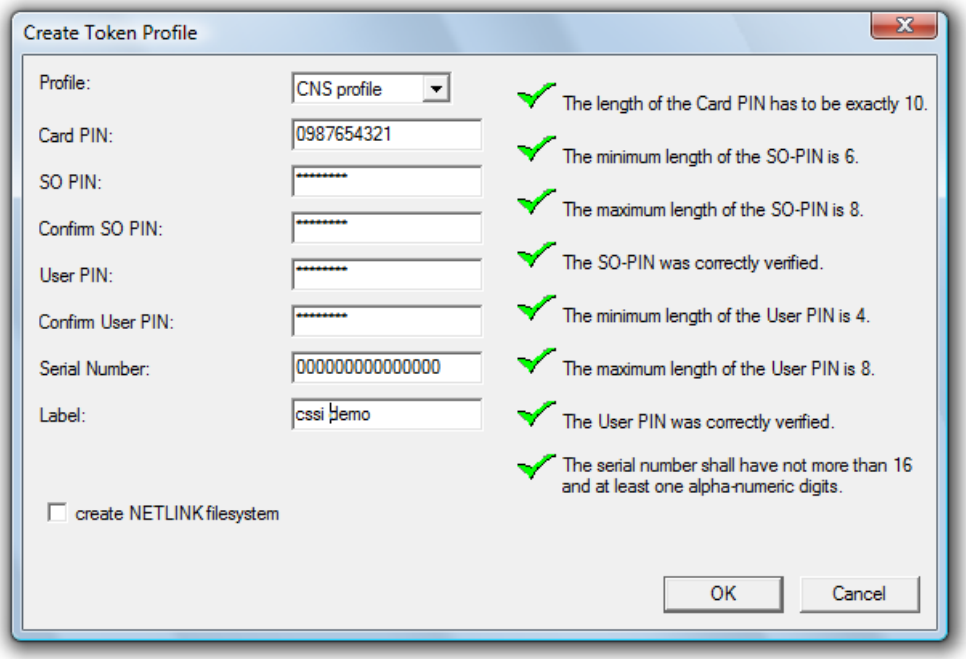
… in the case of a smart card with profile

If there is already a profile on the card and you want to create a new one, the existing one will be deleted as a first step. To this end enter the Card-PIN. If you have created the profile yourself, you have to enter the Card-PIN you have assigned to the card. The default Card-PIN is "0987654321".

The further proceedings are the same, as in the following section "...in the case of an empty smart card". Please follow the instructions, which are described below.

… in the case of an empty smart card

If the profile is setup (Initialization) on an empty smart card, the "Card-PIN", the "SO PIN", the “User PIN” and a Serial Number must be defined. Additionally a Label for the token can be assigned. If multiple profiles are available you can choose one now. CSSI supports three profiles (corporate, PKCS#15 and CNS) for CardOS V4.x smartcards, and supports two profiles (corporate and PKCS#15) for JCOP smartcards.



With the help of the Card PIN, the smart card can be deleted later again. With the SO PIN the smart card can be unlocked. Therefore you should not assign "simple" PINs. The input of the SO PIN and the User PIN is also not displayed in plain text, but through * in the input mask. The input must be also confirmed. Further explanations regarding the PINs can be found in the section 4.2.

4.7. Preparing a Smart Card (Initialization and Personalization)

In order that a user can employ his smart card, it must be prepared, i.e. the smart card must be initialized and personalized. In a first step you have to setup a profile on the smart card and in a second step setup keys and certificates on the smart card.

First Step: Creating a Profile (Initialization)

As a first step you must setup a profile on an empty smart card. You proceed as described in section 4.6 "Creating Profiles".

Second Step: Creating Keys and Certificates (Personalization)

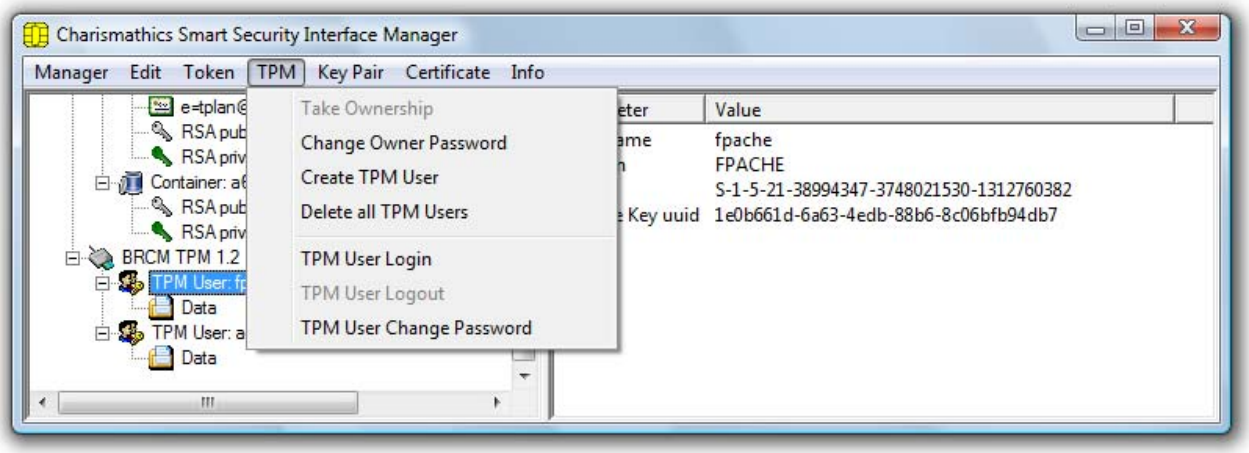
As a second step you must setup for a user key and certificate on the smart card. You have the possibility to either generate keys and certificates or to import them. Refer to section 4.4 "Generating and Importing Keys" and section 4.5 "Generation and Import of Certificates".

4.8. TPM Management

TPM management functions are only available if you installed the charismathics TSS module and the computer is equipped with TPM hardware, please ask charismathics sales for details about the license of charismathics TSS module. The CSSI covers two aspects of the TPM lifecycle: Ownerless Modules and Owned Modules

Operations on TPM without owner

After the TPM Token has been opened using either the plus sign in front of the label within the main hierarchy view or using “Management”→”Open Token” ownership of the TPM can be taken



Once prompted, enter the password for the TPM Ownership. The TPM owner password is used only for TPM specific, but user unrelated operations.

Once ownership has been taken, it can no longer be relinquished using CSSI. Refer to the documentation of your TPM hardware (usually within the BIOS) if you want to give up the ownership.

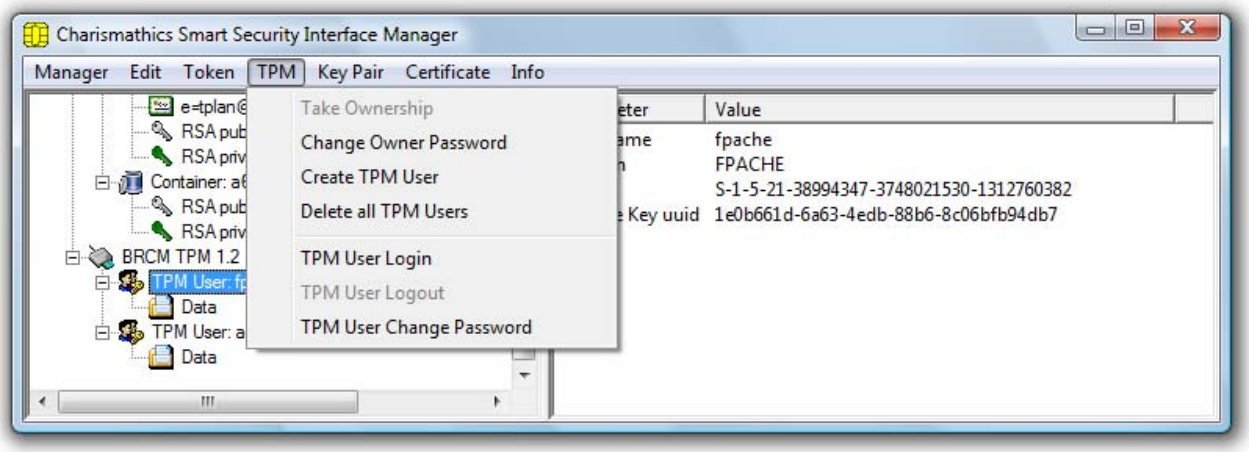
Changing the current TPM Owner Password

The current password can be changed later using “TPM”→”Change Owner Password”

At this point you will be asked to enter the old password and verify the new password by entering it twice

Creating TPM User

In order to make the TPM usable for a windows user a TPM User has to be created.



The TPM User has to be equal to the name of a windows user account, otherwise the TPM User creation fails

Deleting TPM User

TPM User can be deleted together or individually. To delete all Users at once, select “TPM”→”Delete all TPM Users”. And confirm the following dialog

Alternatively it is possible to delete TPM User individually by right-clicking the User account and selecting “Delete TPM User” from either the context menu or the “Edit”. Deleting a user in this fashion requires confirmation as well

Inspect TPM User private information

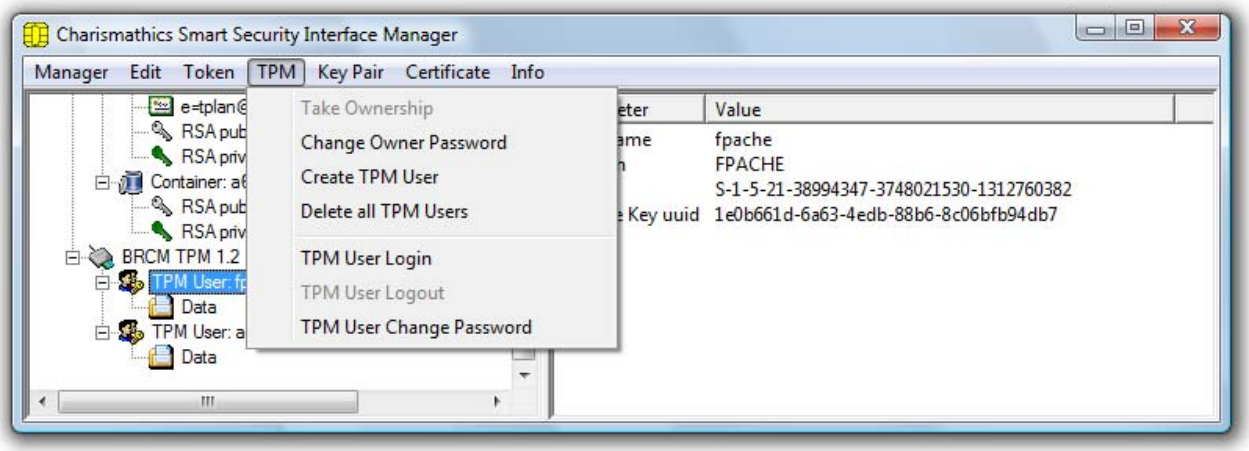
To view the information associated with a user, use “TPM”→”Login”

Login to the TPM User requires entering the password of the selected account.

TPM does not know a locking mechanism like smartcards do with PINs. Instead TPM hardware increases the delay between login attempts.

Changing the TPM User Password

The password of the selected User can be changed via “TPM”→“TPM User Change Password”



Confirm the password change by entering the old password and entering the new password twice when asked.

Importing a key pair from a PFX file

Instead of generating the public and private key pair on the TPM, it can also be imported from a PFX file. Select “Key Pair” → “Import Key Pair from PFX File” and select the PFX file using the dialog.

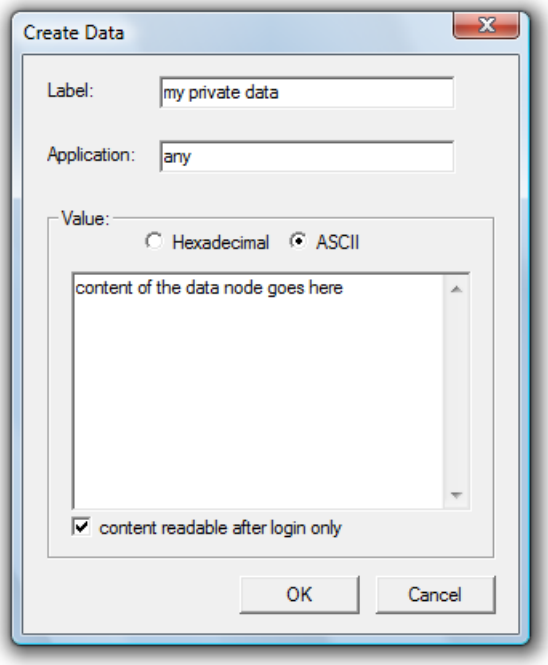
4.9. Further Functions

Directory "Certificates"

There is the directory “Certificates” for all certificates that are not directly corresponding to a key. These are intermediate certificates that have to be imported into this directory. For this purpose select the item “Import Certificate” in the menu “Certificate” or choose the context menu using the right mouse button.

Directory "Data"

A smart card is the safest environment for the private key. Furthermore, the smart card is necessary for application with at least daily logins or authentication. Thus, it is often or always carried around. Therefore it makes sense to store sensitive or necessary data on this medium, e.g. a text file with your PINS. To create data highlight “Data” and select the item “Create Data” in the menu “Edit”. Then, a further window is displayed for you, where you can create your data:



There you have the possibility to access the actual data only, if one is logged on to the smart card. To this end tick the field “content readable after login only”. Your existing data can be deleted, updated or exported via the “Edit” menu

Function "Open Token"

The function "Open Token" of the menu "Manager" transfers data from the smart card to the user interface. This is recommended, if you work with different cards or card readers.

Function "Delete all" and "Delete Object"

You can delete all objects, as keys and certificates with the function "Delete all" of the menu "Edit".

The function "Delete Object" offers you the possibility to remove objects, keys and certificates. You obtain this second function over the context menu as well: highlight the object, that you want to delete, right-click and there chose the item "Delete Object".

Function "Set Default Container"

The function "Set Default Container" of the menu "Edit" is relevant to you only if you use a smart card for login to a Windows-2000 domain via CSP.

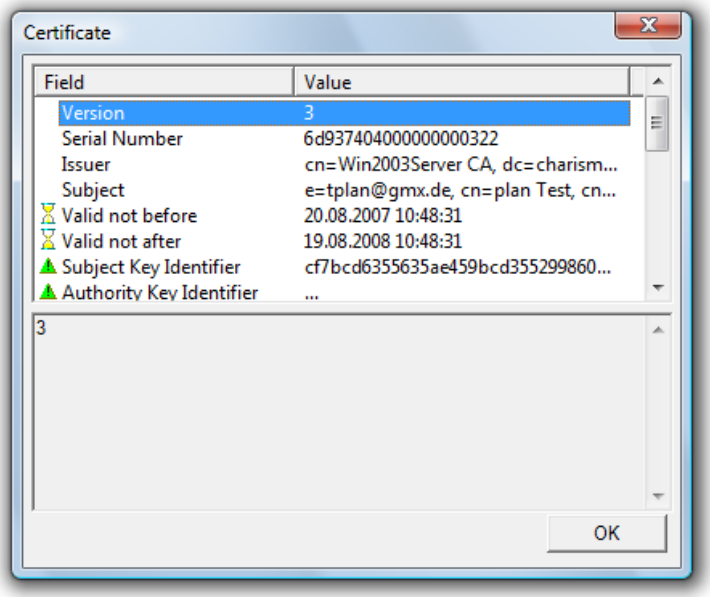
If you do not choose a container as Default Container, Windows will take the first key from the list for the login to a Windows-2000 domain via CSP.

If you have chosen a Container as Default Container, it will show in bold face in the interface of the administration tool

Function "Show Certificate"

If you want to display a certificate, use the function "Show Certificate" from the menu "Certificate".

You can access this function over the context menu as well: highlight the certificate, that you want to display, right-click and select the item "Show Certificate". Then you obtain the information contained in the certificate:



Function "Export Certificate"

If you want to employ a certificate for other applications, you can export it from the smart card with the function "Export Certificate" from the menu "Certificate". You can also access this function from the context menu: highlight the certificate, that you want to export, right-click and choose the item "Export Certificate".

Function "Register Certificate"

The function "Register Certificate" from the menu "Certificate" installs the certificate, that you want to register to make it accessible for Windows-applications (like Internet Explorer or Outlook Express).

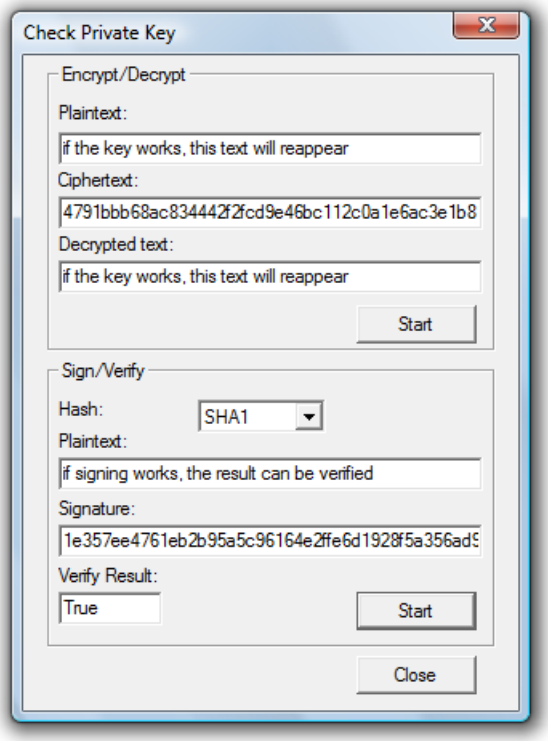
You can also acess this function from the context menu: highlight the certificate, that you want to register, right click and choose the item "Register Certificate".

Configuration of the settings regarding the registration is done in the *Register Tool*. Read more about this in chapter 6 Register Tool.

Function "Check Private Key"

With this function you can test generated keys, e. g. for signing or decryption. First you must be logged on, then highlight the private key you want to test and chose the function “Check Private Key” from the menu “Edit” or the context menu.

To test the decryption key write text in the field “Plaintext” and click on the button “Start”. If the decrypted text is the same as the Plaintext, the decryption key works all right.



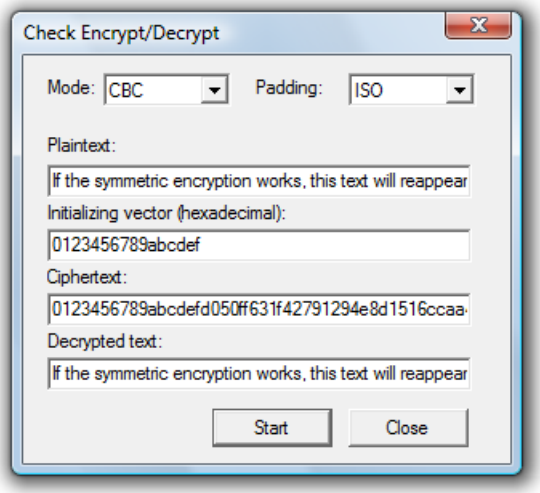
To test the signing key you can chose the hash algorithm. If the Verify Result is true, the signing key works all right.

Function "Check Secret Key"

With this function you can test generated keys for encryption. First you must be logged on, then highlight the private key you want to test and chose the function “Check Secret Key” from the menu “Edit”.

You can choose the cryptographic mode for testing the key. The different versions are the Cipher Block Chaining (CBC) and the Electronic CodeBook (ECB). And you can choose ISO or PKCS5 as Padding.

To test the encryption key write text in the field “Plaintext” and click on the button “Start”. If you know the initializing vector you can insert it; otherwise it will be filled with zero. Is the decrypted text the same as the Plaintext, the encryption key works all right.

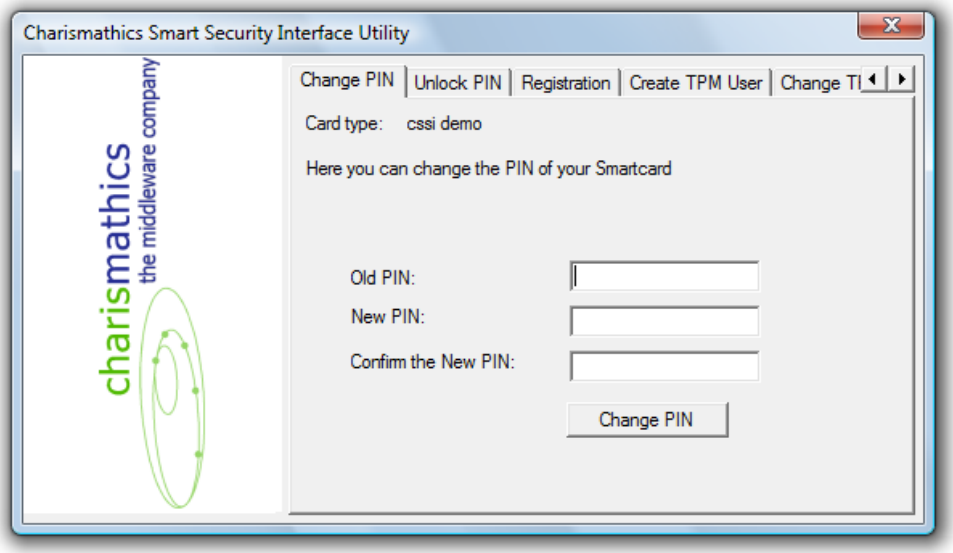


5. User Tool: Charismathics Smart Security Interface Utility

This tool exposes all relevant functions if you acquired **Charismathics Smart Security Interface** in the user edition. Changing your pin and the registration of your key/certificates of the smart card are available as well as TPM management functions. Insert your smart card in the reader and open **Charismathics Smart Security Interface** Utility by following the path:

"Programs"->"charismathics "->"smart security interface" ->"smart security interface utility".

5.1. Change PIN

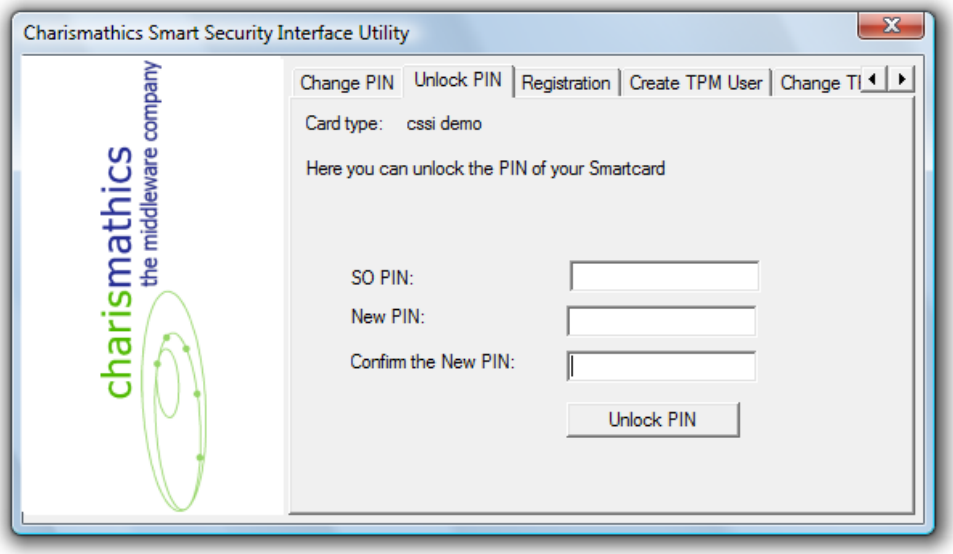


To change your PIN, insert the old PIN followed by the new PIN, which must be entered a second time as confirmation. The minimum length of the User PIN is four characters and the maximal length is ten characters.

Click on the button "Change PIN" and you receive a window with the confirmation.

IMPORTANT: *After three consecutive wrong inputs the User PIN will be locked. Please choose a PIN, which you can remember well, but which cannot be easily guessed. Avoid e.g. birthdays or simple sequences of numbers like 1234 or 1111.*

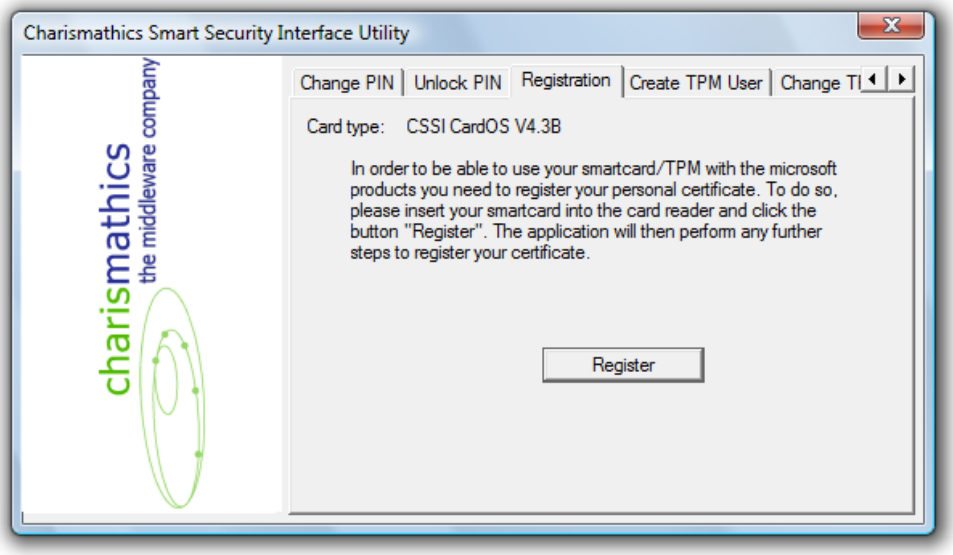
5.2. Unlock PIN



To unlock your PIN, enter the SO PIN followed by the new PIN, which must be entered a second time as confirmation. The minimal length of the User PIN is four characters and the maximal length is ten characters.

Click on the button "Unlock PIN" and a confirmation window opens.

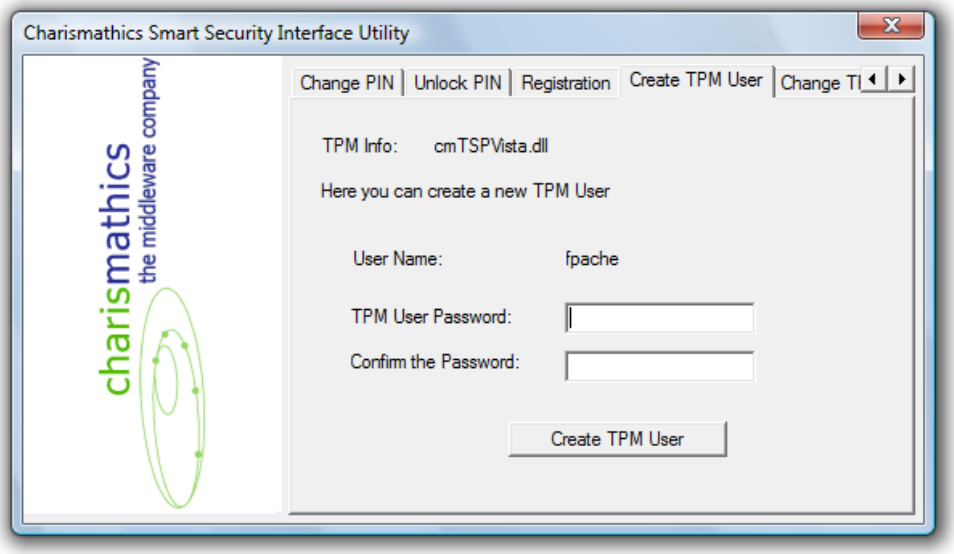
5.3. Registration



Your smart card may contain multiple certificates and keys. These certificates must be registered once, so that applications can use these. Particularly it concerns the registration of the certificate/keys with the Microsoft Windows certificate data base.

IMPORTANT: THE REGISTRATION NEEDS TO BE DONE ONLY ONCE FOR EACH CARD.

5.4. Create TPM User

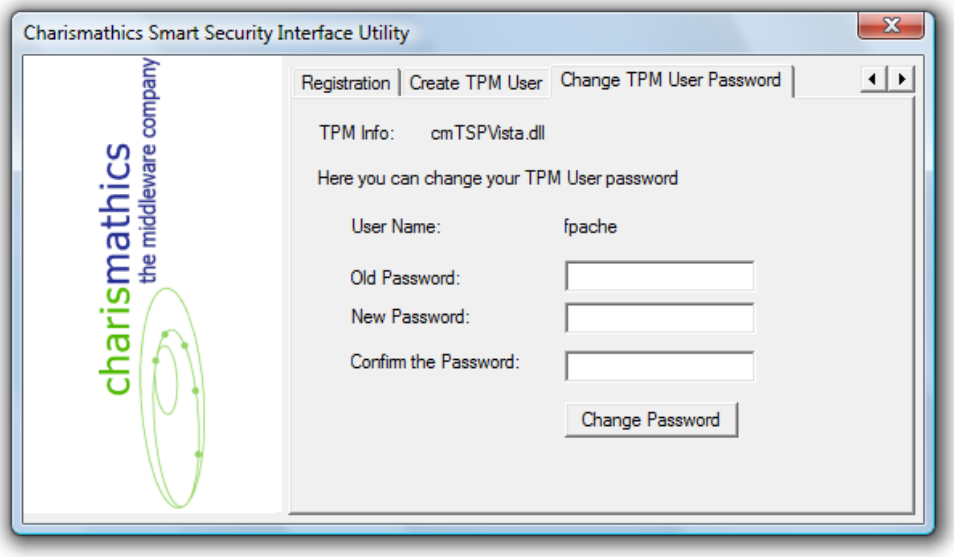


Creating a TPM User only works on systems which meet the following requirements:

- TPM hardware has to be present
- TSS module has to be installed
- TPM Ownership must have been taken, e.g. with CSSI admin edition
- A TPM User for the current user does not yet exist

A TPM User can only be created for the currently logged in.

5.5. Change TPM Password



Changing a TPM User only works on systems which meet the following requirements:

- TPM hardware has to be present
- TSS module has to be installed
- TPM Ownership must have been taken, e.g. with CSSI admin edition

- A TPM User for the current has been created

Changing the TPM Password requires entering the old password once and the new password twice in the according fields.

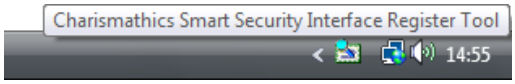
6. Register Tool

If you acquired **Charismathics Smart Security Interface** in the Admin or in the User edition, this Register Tool makes more functions available for you.

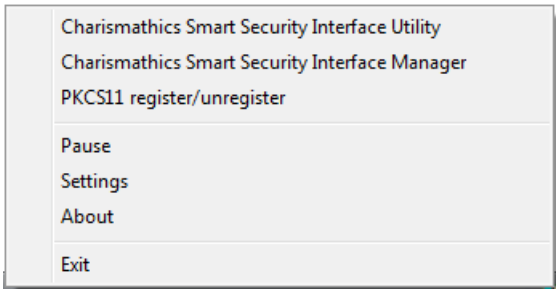
To make certificates accessible for Windows-applications like Internet Explorer or Outlook Express, you can automatically register the certificates from your smart card in the certificate store of Windows. The settings for this registration are configured in this Register Tool.

The default functionality is as follows: as soon as a smart card is inserted into the card reader, the certificates are automatically registered, as long as the Register Tool is active. On smart card removal, the certificates are not automatically unregistered. If this is desired, you can adjust this using the "Settings".

You can call the Register Tool of **Charismathics Smart Security Interface** either over the Start menu or over the tray icon:



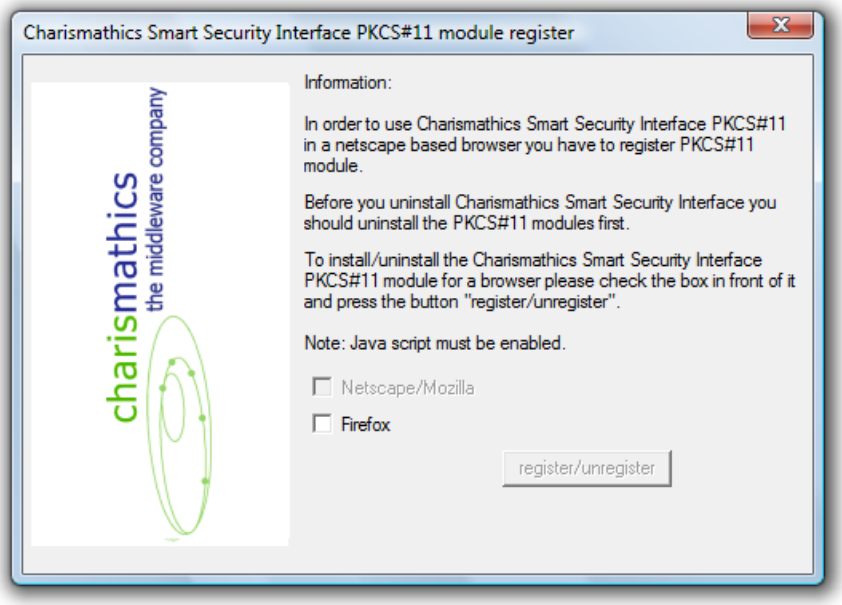
Then you get the possibilities of starting the Administration Tool sc/interface Manager or the User Tool sc/interface Utility, to Pause the Register Tool, to configure Settings, to read information or to terminate the Register Tool, which is now explained.



6.1. Start CSSI Manager and Start CSSI Utility

If you have the Admin Edition the function “Start Charismathics Smart Security Interface Manager” gives you the possibility to start the Administration Tool “Charismathics Smart Security Interface Manager”. If you have the User Edition with the function “Start Charismathics Smart Security Interface Utility“ you can start the User Tool Charismathics Smart Security Interface Utility. Further explanations concerning this Administration Tool you find in chapter 4 and concerning the User Tool you find in chapter 5.

6.2. PKCS11 register/ unregister



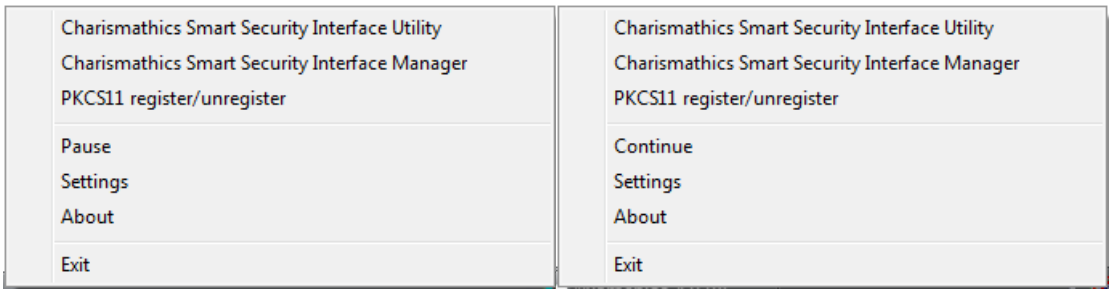
For the smartcard to be usable in the Netscape/Mozilla family of products a PKCS#11 module has to be registered with the products. This dialog offers a convenient way of installing the module. If the checkbox in front of the product name is not checked, the product is not configured to use the Charismathics PKSC#11 module. A marked checkbox signifies a PKCS#11 enabled product. Use the “register/unregister” button to apply the changes made.

A few things to keep in mind when using this feature:

- Firefox and Thunderbird share the same configuration files. Installing the module in firefox enables it in Thunderbird as well.
- Most Applications have to be closed at the time “register/unregister” is selected, otherwise the operation fails.
- It is possible that the Register Tool considers the PKSC#11 module registered, while is actually is not, or vice versa. This may be due to failed installation/ un-installation attempts or manual changes to the configuration.
  In this case, repeat the “register/unregister” process (remember to close all confirmation windows), until the desired effect sets in. This should take no more than 3 iterations.
  To avoid these problems, it is advisable to use only the Register Tool to change the configuration while all applications being changed have been closed.

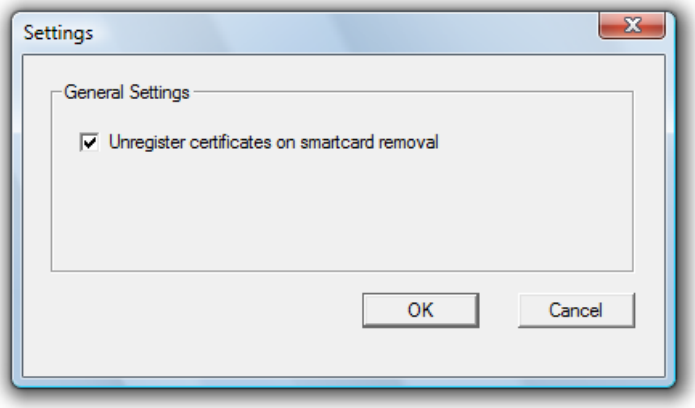
6.3. Pause / Continue

If it is not desired that the certificates of the smart card are registered automatically, you can pause the Register Tool. For it you select the point "Pause" in the pop-up menu of the tray icons. Thereupon the tray icon changes, so that one recognises that the Register Tool is set to pause. In order to continue with the automatic registration, you select the now appeared point "Continue" in the pop-up menu of the tray icons:



6.4. Settings

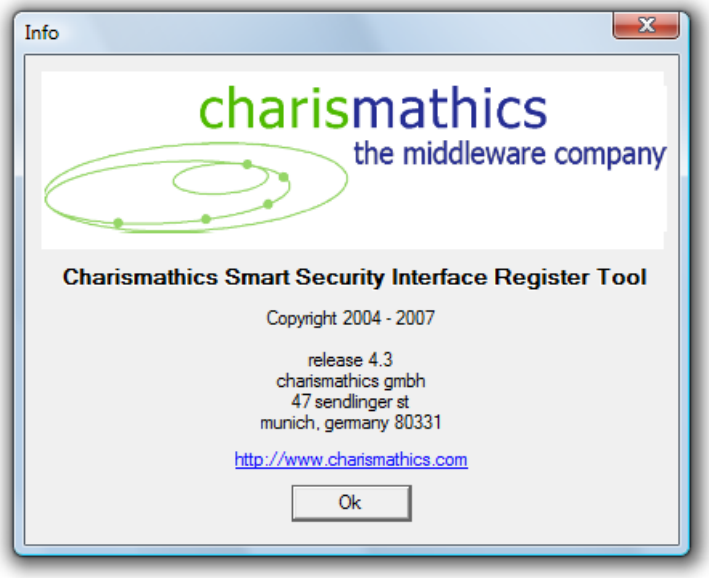
The default functionality of the Register Tool is, that certificates are registered automatically, as soon as a smart card is inserted into the card reader. On smart card removal the certificates are unregistered automatically. If this is desired, you can configure this over the "Settings". For this you select the point "Settings" in the pop-up menu of the tray icons and you receive the following-dialog:



If you want, that the registered certificates are removed from the certificate store, if you remove the smart card from the card reader, you must activate the field.

6.5. About

For information about the version of the Register Tools and the manufacturer charismathics gmbh select "About" in the menu of the tray icons:

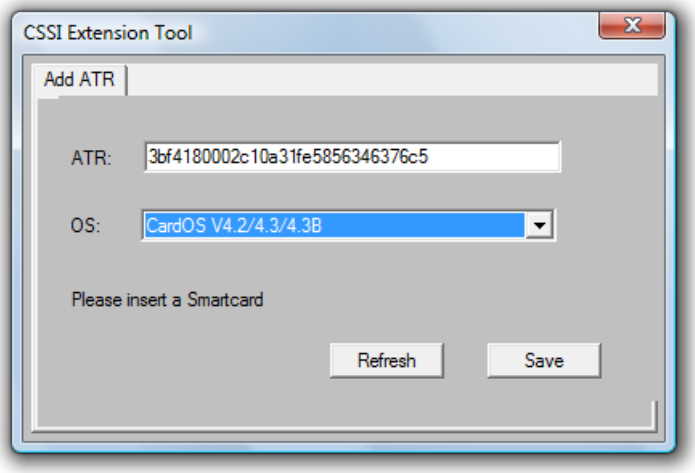


6.6. Exit

With „Exit“ in the menu of the tray icon you can end the Register Tool.

7. Charismathics Extension Tool

The Charismathics Extension Tool can be used to associate smart card operating systems with new ATRs. Without a valid association, correct operation of the smart card can not be guaranteed.



Follow these steps to make a new ATR/ Card OS association:

1. insert the smart card into the reader
   The card ATR is displayed in the upper field
   a. if an OS is associated with the ATR, the OS field is locked and can not be changed while the card is in the reader.
   b. if no OS is associated with the ATR, select the correct OS, or a as close as possible match.
2. press “Save” to store the information

If the actual Operating System on the card is either unknown or not available, select one that matches the OS most closely. E.g. select the generic “JCOP” OS entry if the exact JCOP xx version number is not known.

8. CSP of Charismathics Smart Security Interface

The Windows operating system supports cryptographic functionalities like encryption and digital signature by the so-called Crypto-API. Furthermore, CSPs (Cryptographic Service Providers) enable programs to support smart cards. During the installation of **Charismathics Smart Security Interface** the **Charismathics Smart Security Interface-CSP** – abbr. cmCSP – will be added.

Now with this cmCSP you can use certain programs and functionalities delivered with Windows 2000, like Outlook Express, Internet Explorer, network login and VPN-login with the smart card. They will be explained in the following.

***NOTE**: Here, you will not find a description how to configure your Microsoft environment for the use of smart cards. Please consult the help files for Outlook Express and the Internet Explorer. To configure the network login and the VPN-login for smart cards please consult the documentation of the Windows 2000 Server.*

If you need support for the implementation or realization, charismathics's team can help you. Feel free to contact your account manager.

8.1. General Proceedings

General precondition is the installation of the cmCSP. **Charismathics Smart Security Interface** installs it automatically. In the following some general notes to employ the cmCSP will be given:

> If you want to use a Microsoft product in connection with the CSP for the first time on a certain computer, you must register the certificate that you want to use. Please read in chapter 6 "Register Tool" or in section 4.8 "Register Certificate", if you need to know how to register your own certificate.

> You as a user need keys and certificates on the smart card. There are several different possibilities. The most popular are:

- Generation of key pair and corresponding certificate directly on the smart card with the functions of standard browsers, like Internet Explorer or Netscape. This ensues an access on the modules of **Charismathics Smart Security Interface**, i.e. correspondingly on cmCSP or cmP11.

NOTE: Enter into the browser http://<Servername of Enterprise-CA>/certsrv .

- Generation of key pair and corresponding certificate directly on the smart card with the Microsoft Certificate Server (in "Enterprise CA" and in "Stand Alone" mode).

- Import of existing keys and certificates on the smart card, that were generated by other CAs or trust centers, resp. request of certificate from a trust center.

- Generation of key pair and corresponding self signed certificate directly on the smart card by the administration tool **Charismathics Smart Security Interface**. Please observe, that the employment of self signed certificates makes sense only in environments without a PKI or for testing.

***Note**: If you request a certificate from a trust center, you might be requested to choose a security module, e.g. a token. In this case choose the corporate profile, the cmCSP or the cmP11. Furthermore, your smart card has to be inserted in the card reader, so that certificates can be written on it.*

> Programs must be configured, so that they work with your smart card.

> The programs must be configured, so that they work with your keys and certificates. There you have to take into account the preconditions of the programs, that need certain input. E.g. some programs need root-certificates, that must be in certain directories or for other programs you must register your certificate.

In the following chapters only the special features of the corresponding application will be explained.

8.2. Smart Card Login to a Windows 2000 Domain

Here you should have very good command in the administration of Windows 2000 Servers. You proceed according the following steps:

Step 1	Setup of ADS. Please observe the correct configuration of the DNS-Server.
Step 2	Installation of the Enterprise CA and at least the templates "Enrollment Agent", "Smartcard Logon" and Smartcard User".
Step 3	Then an Enrollment-Agent-Certificate must be generated and registered on the computer, where the smart cards should be personalized.
Step 4	After that the smart cards for users may be issued over the Enrollment Station.

Furthermore, observe that "Set Default Private Key" must set the private key on the client (see in section 4.8).

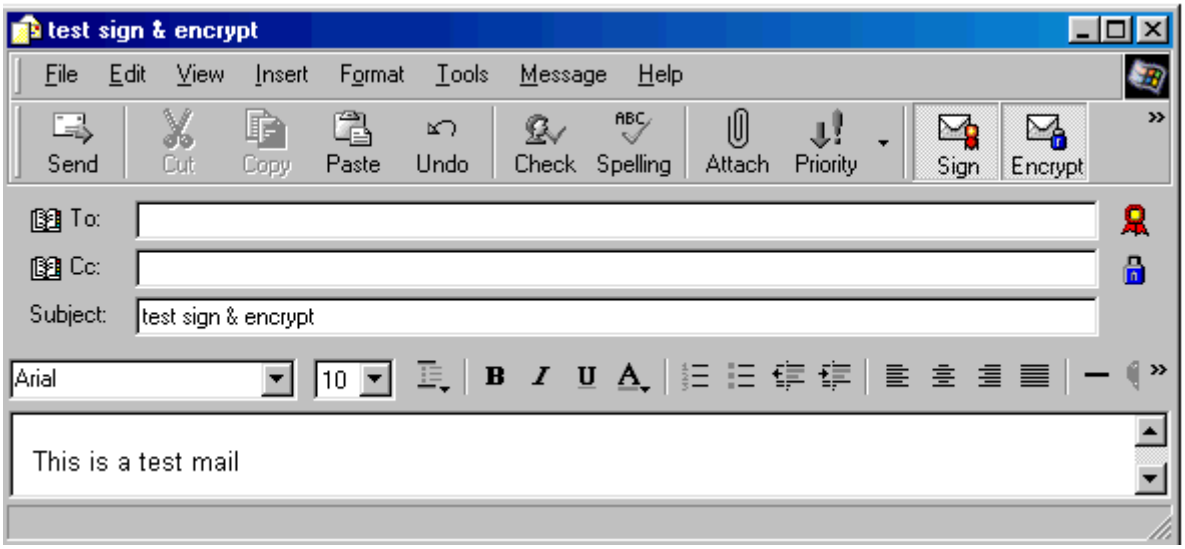
8.3. SSL- Authentication with Smart Card over the Internet Explorer

Here you must register the certificate with the administration tool of **Charismathics Smart Security Interface** (see in chapter 6 “Register Tool” or in section 4.8 "Register Certificate").

8.4. Outlook Express with Electronic Signature and Encryption via Smart Card

Here you must register the certificate with the administration tool of **Charismathics Smart Security Interface** (see in chapter 6 “Register Tool” or in section 4.8 "Register Certificate"). Then choose the desired certificate for signing and encryption over "Tools -> Accounts -> E-Mail -> Preferences -> Security".

Normally, there are pull down menus in the email windows, that you may click encryption and/or signing an email in order to use the security functionalities. The verification of incoming signed emails uses for instance the red "signet" symbol in the right corner of the email window, like here in the example:



In order that Outlook Express automatically acknowledges the right key, resp. certificate, the certificates should lie in the address book, i.e. the certificate should be imported into the "Digital IDs": e.g. highlight the name in the address book and choose the tab "Digital IDs" over the context menu. On this tab you can import the certificate for the chosen contact.

8.5. Windows VPN-Login with Smart Card

You should generate keys and certificates with the Microsoft Enterprise-CA. Furthermore, you must register the certificate with the administration tool of **Charismathics Smart Security Interface** (see in chapter 6 “Register Tool” or in section 4.8 "Register Certificate").

9. PKCS#11-Module of Charismathics Smart Security Interface

If you use software, that supports PKCS#11, you can employ **Charismathics Smart Security Interface-PKCS#11** -abbreviated cmP11- with the smart card. Here it is a matter of applications and functionalities with smart cards, like network login, SSL, email security with Netscape, certain Microsoft applications and products of other producers, that are explained briefly.

NOTE: *Here is no description, how to configure your environment for the employment with smart cards. For this purpose please consult the corresponding help-files of the corresponding programs.*

IMPORTANT: *cmP11 is a DLL with the name "cmP11.dll and is after the installation in the system directory, e.g. in \WINNT\system32.*

Remark: Despite strict measures for the quality of PKCS#11 modules by the different manufacturers, charismathics gmbh can not guarantee for the compatibility with each PKCS#11 Module of a foreign manufacturer.

9.1. General Methodology

In the following some general notes are made for the employment of cmP11. General precondition is the installation of cmP11. This will be installed automatically by **Charismathics Smart Security Interface**.

> You as a user need keys and certificates on the smart card. There are several different possibilities. The most prevalent are mentioned below:

- Generation of key pairs and corresponding certificate directly on the smart card with the functions of standard browsers, like Internet Explorer or Netscape. This ensues access to the modules of **Charismathics Smart Security Interface**, i.e. corresponding to cmCSP or cmP11.

NOTE: For this purpose enter in the browser http://<Servername_of_Enterprise_CA>/certsrv.

- Generation of key pair and corresponding certificate directly on the smart card with Novell's Certificate Server.

- Generation of key pair and corresponding certificate directly on the smart card with Microsoft's Certificate Server (in "Enterprise CA" mode and in "Stand Alone" mode).

- Import of existing keys and certificates on the smart card, that were generated by other CAs or trust centers, resp. requesting a certificate from a trust center.

- Generation of key pair and corresponding self signed certificate directly on the smart card with the delivered administration tool of **Charismathics Smart Security Interface**. Please observe that the employment of self signed certificates makes sense only in environments without PKI or for the purpose of testing.

***NOTE**: If you request a certificate from a trust center, you might be requested to choose a security module. Please choose in this case the corporate profile, the cmCSP or the cmP11. Furthermore, your smart card has to be inserted in the card reader, so that certificates can be written on it.*

As in section 3.3 described, the possibility is offered, to install charismathics's PKCS#11-Module here in Netscape. There is the possibility to install the module manually with the help of the file "InstallNetsca-pePKCS11.html" and uninstall with the help of the file "UninstallNetscapePKCS11.html".

> The programs must be configured, so that they can work with your smart card.

> The programs must be configured, so that you can work with keys and certificates. Here you must take into account the preconditions of the programs, that have certain inputs. E.g. some programs need root certificates, that must be in certain directories or for other programs you have to register your certificate.

In the following chapters only the special features of the respective application will be explained.

9.2. Smart Card Login to a Novell eDirectory (formerly NDS)

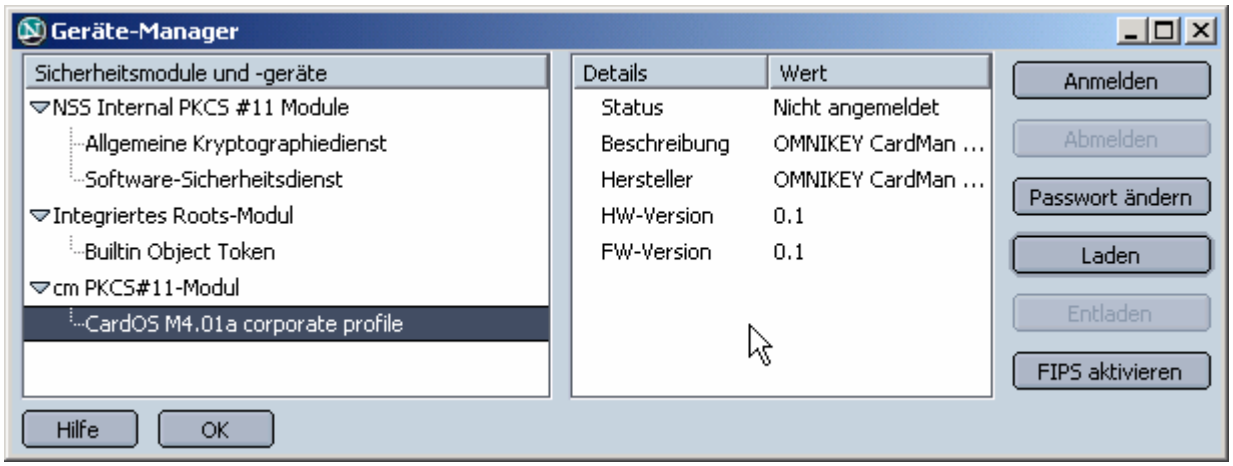
Here you should have a very good command in the administration of Novell servers and observe the installation preconditions. To realize a smart card login to an eDirectory you explicitly need the product NMAS and the corresponding Universal Smartcard Login Method.

9.3. SSL- Authentication with Smart Card over Netscape

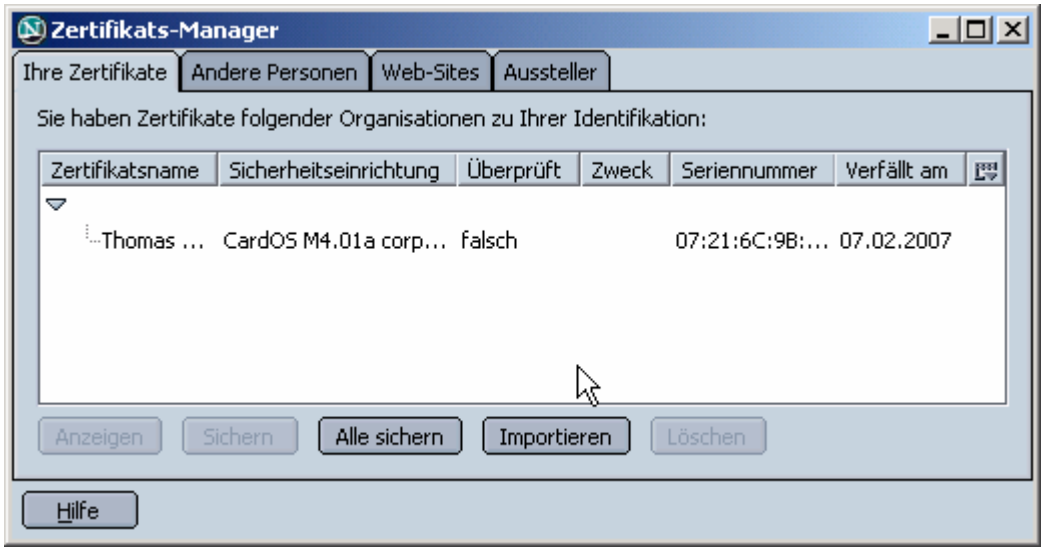
The notes for the employment of Netscape are presented by the example of version 7.

Example: Netscape 7.01

You can call "Manage Security Devices" in Netscape 7.01 over "Edit"->"Preferences"->"Privacy & Security"->"Certificates". There you can load the cmP11, so that applications like SSL and emails can be employed with smart cards:



Furthermore, you can call the Certificate Manager of Netscape on the same tab by clicking "Manage Certificates...".



9.4. Email-Security by Smart Cards with Netscape's Messenger

The notes for the employment of Netscape and screen shots to manage certificates and modules are available in the example of version 7 in the previous section.

Normally, there pull-down menus in the email windows, where you can tick whether an email should be encrypted and/or signed, resp. a function for verification of received signed emails, to employ the security functionality.

10. References

[PKCS#5] http://www.rsasecurity.com/rsalabs/pkcs/index.html

[PKCS#11] http://www.rsasecurity.com/rsalabs/pkcs/index.html

[MS_CA] HOW TO: Configure a Certificate Authority to Issue Smart Card Certificates in Windows 2000:
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313274&sd=tech

Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities:
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q281245

[MS_SC] Windows 2000 Server Documentation, Smart card Administration:
http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_SC_admin.htm

11. Information / Export Restrictions

Charismathics GmbH
47 Sendlinger St
80331 Munich
Germany

Release Date: May 31, 2006

Trade Mark

All mentioned software and hardware names are in most of the cases trade marks and are liable to legal requirements.

Please observe !

The product delivered to you is liable to export control. Please observe the legal requirements of specific countries. For export out of the EU an export approval is necessary.

Appendix A: Reference for Developers

In this appendix there are detailed specification regarding the supported functions of the PKCS#11-standard, a synopsis of particular functions and a list of objects and mechanisms. These information are useful and necessary for application developers, who want to develop their own applications supporting the cmP11.

Functions according to PKCS#11-Standard

In the following there are three lists of functions according to PKCS#11-Standard. The list are supported, incompletely supported, and not supported functions by **Charismathics Smart Security Interface**:

Supported Functions:

- C_Finalize
- C_GetInfo
- C_GetFunctionList
- C_GetSlotList
- C_GetSlotInfo
- C_GetMechanismList
- C_GetMechanismInfo
- C_InitPIN
- C_SetPIN
- C_CloseSession
- C_CloseAllSessions
- C_GetSessionInfo
- C_Login
- C_Logout
- C_CreateObject
- C_DestroyObject
- C_GetAttributeValue
- C_SetAttributeValue
- C_FindObjectsInit
- C_FindObjects
- C_FindObjectsFinal
- C_EncryptInit
- C_Encrypt
- C_EncryptUpdate
- C_EncryptFinal
- C_DecryptInit

- C_Decrypt
- C_DecryptUpdate
- C_DecryptFinal
- C_DigestInit
- C_Digest
- C_DigestUpdate
- C_DigestFinal
- C_SignInit
- C_Sign
- C_SignUpdate
- C_SignFinal
- C_VerifyInit
- C_Verify
- C_VerifyUpdate
- C_VerifyFinal
- C_VerifyRecoverInit
- C_VerifyRecover
- C_GenerateKeyPair
- C_GenerateKey
- C_GenerateRandom
- C_WrapKey
- C_UnwrapKey
- C_CancelFunction (returns CKR_FUNCTION_NOT_PARALLEL)
- C_InitToken

Incompletely Supported Functions / Deviations

- C_Initialize
- C_WaitForSlotEvent
- C_OpenSession
- C_GetTokenInfo
- C_GetObjectSize
- C_SignRecoverInit (use C_SignInit)
- C_SignRecover (use C_Sign)

Not supported functions:

- C_GetOperationState
- C_SetOperationState
- C_CopyObject
- C_DigestKey
- C_DigestEncryptUpdate
- C_DecryptDigestUpdate
- C_SignEncryptUpdate
- C_DecryptVerifyUpdate
- C_DeriveKey
- C_SeedRandom
- C_GetFunctionStatus

Synopsis of specific functions

C_Finalize

Parameter:	pReserved (CK_VOID_PTR)
Description:	Sessions will be closed. Slots will be closed. Reserved Memory will be freed.
Deviation:	pReserved will be ignored. C_Finalize will be called automatically on Finish. If C_Initialize is called n times in succession (without C_Finalize in between), C_Finalize will only be carried out after the n time.

C_GetObjectSize

Parameter:	hSession CK_SESSION_HANDLE hObject CK_OBJECT_HANDLE pulSize CK_ULONG_PTR
Description:	The size of an object will be returned
Deviation:	The returned size, is the minimum size of an object, which means it do not contain the size for extra attributes like label, or id. The size of private objects are default values.

C_GetSlotList

Parameter:	tokenPresent (CK_BBOOL) pSlotList (CK_SLOT_ID_PTR) pulCount (CK_ULONG_PTR)
Description:	Returns a list of identified Slots. It might occur, that installed but not connected Slots will be in the list. The number of Slots may be obtained by passing pSlotList a Null-Pointer. If you want only the Slots with an inserted card, set tokenPresent to true.

C_GetTokenInfo

Parameter:	slotID (CK_SLOT_ID) pInfo (CK_TOKEN_INFO_PTR)
Description:	Returns whether a card is inserted in a Slot. If the card is not inserted, CKR_TOKEN_REMOVED will returned.
Special Feature:	Inserting or removing a card from a Slot, is an Event (see C_WaitForSlotEvent). If C_GetTokenInfo will be called, the Event will be finished, even if the card was removed and C_GetTokenInfo CKR_TOKEN_NOT_PRESENT has been returned.

C_Initialize

Parameter:	CinitArg (CK_VOID_PTR_PTR)

Description:	Libary will be initialized. Slots will be created. Inserted cards are read.
Deviation:	CinitArg is expected in the format CK_C_INITIALIZE_ARGS. From these the flags are picked out, in particular CKF_LIBRARY_CANT_CREATE_OS_THREADS which decides over Multi threading. The rest is ignored. If C_Initialize is called several times, CKR_CRYPTOKI_ALREADY_INITIALIZED is returned. The number is taken in account (see C_Finalize).

C_OpenSession

Parameter:	slotID (CK_SLOT_ID) flags (CK_FLAGS) pApplication (CK_VOID_PTR) Notify (CK_NOTIFY) phSession (CK_SESSION_HANDLE_PTR)
Description:	Opens a new session on the Slot.
Deviation:	Notify and pApplication are ignored and should be set to NULL_PTR. Sessions can only be opened, if a card is inserted.
Special Feature:	If a session is opened and then the card will be removed, all sessions on the Slot will return CKR_DEVICE_REMOVED. If there is an error with CKR_ DEVICE_REMOVED, CKR_TOKEN_NOT_RECOGNIZED or CKR_TOKEN_NOT_PRESENT a pauseAllSessions is automatically produced on this Slot. If a paused session is used again, this session will be reopened automatically. If a card is inserted into or removed from a Slot, then this is an Event (see C_WaitForSlotEvent). If C_OpenSession is called, the Event will be finished, even if the card has been removed and C_OpenSession returned CKR_TOKEN_NOT_PRESENT.

C_WaitForSlotEvent

Parameter:	flags	(CK_FLAGS)	
	pSlot	(CK_SLOT_ID_PTR)	
	pReserved	(CK_VOID_PTR)	= NULL_PTR
Description:	flag = 0; The method waits until a Slot reports an Event. Then it returns the Slot with the Event in pSlot. flag = CKF_DONT_BLOCK The method displays the Slot with Event in pSlot. If there is no Event, CKR_NO_EVENT will be returned.		
Special Feature:	If more Slots have an Event, they will be returned interchangeably. An Event persists until an access to the card occurs (e.g. by C_OpenSession or C_GetToken_Info), even if an error will be returned to the card.		

Objects

All objects will be stored on the card (CKA_TOKEN = true). Session- or other software-objects will not be supported.

The ID (CKA_ID) indicates, which objects belong together.

CKO_CERTIFICATE (CKC_X_509)

Certificate in X.509 format

Attribute	**Value**	**Access**
CKA_CLASS	CKO_CERTIFICATE	Read only
CKA_LABEL	<alias>	Read/write
CKA_VALUE	<certificate> X509Format (DER)	read/write
CKA_ID	<number>	read/write
CKA_CERTIFICATE_TYPE	CKC_X_509	read only
CKA_TOKEN	TRUE	read only
CKA_PRIVATE	FALSE	read only(**)
CKA_SUBJECT	<alias>	read only
CKA_ISSUER	<alias>	read only
CKA_SERIAL_NUMBER	<number>	read only
CKA_MODIFIABLE	TRUE/FALSE	read only(**)

(**) returns no error on trying to write.

CKO_PRIVATE_KEY (CKK_RSA)

Attribute	**Value**	**Access**
CKA_CLASS	CKO_PRIVATE_KEY	read only
CKA_LABEL	<alias>	read/write
CKA_ID	<number>	read/write
CKA_KEY_TYPE	CKK_RSA	read only
CKA_TOKEN	TRUE	read only
CKA_PRIVATE	TRUE	read only
CKA_SUBJECT	<alias>	read only(*)
CKA_SENSITIVE	FALSE	read only
CKA_DECRYPT	TRUE	read only(**)
CKA_SIGN	TRUE	read only(**)
CKA_SIGN_RECOVER	FALSE	read only(**)
CKA_UNWRAP	FALSE	read only(**)
CKA_MODULUS	Pkcs12 Format	read only
CKA_PUBLIC_EXPONENT	Pkcs12 Format	read only

CKA_PRIVATE_EXPONENT	Pkcs12 Format	not readable
CKA_PRIME_1	Pkcs12 Format	not readable
CKA_PRIME_2	Pkcs12 Format	not readable
CKA_EXPONENT_1	Pkcs12 Format	not readable
CKA_EXPONENT_2	Pkcs12 Format	not readable
CKA_COEFICIENT	Pkcs12 Format	not readable
CKA_MODIFIABLE	TRUE	read only(**)
CKA_LOCAL	TRUE	(**)(***)
CKA_START	<empty>	(***)
CKA_STOP	<empty>	(***)
CKA_EXTRACTABLE[8]	FALSE	read only(**)
CKA_NEVER_EXTRACTABLE[2]	TRUE	read only(**)

(*) can only be read, if a corresponding certificate exists

(**) returns no error on trying to write.

(***) is not supported

CKO_PUBLIC_KEY (CKK_RSA)

Attribute	**Value**	**Access**
CKA_CLASS	CKO_PUBLIC_KEY	read only
CKA_LABEL	<alias>	read/write
CKA_ID	<number>	read/write
CKA_KEY_TYPE	CKK_RSA	read only
CKA_TOKEN	TRUE	read only
CKA_PRIVATE	FALSE	read only
CKA_SUBJECT	<alias>	read only(*)
CKA_ENCRYPT	TRUE	read only(**)
CKA_VERIFY	TRUE	read only(**)
CKA_VERIFY_RECOVER	TRUE	read only(**)
CKA_WRAP	FALSE	read only(**)
CKA_MODULUS	pkcs12 Format	read only
CKA_PUBLIC_EXPONENT	pkcs12 Format	read only
CKA_MODIFIABLE	FALSE	read only(**)
CKA_LOCAL	TRUE	(**)(***)
CKA_START	<empty>	(***)
CKA_STOP	<empty>	(***)

(*) can only be read, if a corresponding certificate exists

(**) returns no error on trying to write

(***) is not supported

CKO_DATA

General Data

Attribute	Value	Access
CKA_CLASS	CKO_DATA	read only
CKA_LABEL	<alias>	read/write
CKA_VALUE	<data>	read/write
CKA_TOKEN	TRUE	read only
CKA_PRIVATE	FALSE	read only(**)
CKA_APPLICATION	<alias>	read/write
CKA_ MODIFIABLE	TRUE	read only(**)

(**) returns no error on trying to write.

Mechanism

Sign (RSA):

Description: Signs data

Order: C_SignInit, C_SignUpdate, C_SignFinal
or C_SignInit, C_Sign
C_Sign works as if C_SignUpdate and then C_SignFinal were called.
C_SignUpdate processes the data immediately.

Special Feature: Order C_SignInit, C_Sign(C_SignUpdate, C_SignFinal), C_Sign (C_SignUpdate, C_SignFinal) where on the first C_Sign (resp. C_SignFinal) NULL_PTR will be passed for the signature and only the length of the signature will be returned. The signature will be returned on the second C_Sign (resp. C_SignFinal). If C_SignUpdate is called for the second time, the data must match with the data of the first time. A third call is not possible. For another signature C_SignInit must be called first.

Verify (RSA):

Description: Verifies a signature. VerifyRecover returns only the data (normally as a hash-value)

Order: C_VerifyInit, C_VerifyUpdate, C_VerifyFinal
or C_VerifyInit, C_Verify
or C_VerifyRecoverInit, C_VerifyRecover
C_Verify works as if _VerifyUpdate and then C_VerifyFinal were called.
C_VerifyUpdate stores data only temporarily.
C_VerifyRecover returns the signed data.

Special Feature: Order C_VerifyRecoverInit, C_VerifyRecover, C_VerifyRecover, where on the first C_VerifyRecover a NULL_PTR will be passed as data. It returns only the length of the data. The data will be returned on the second C_VerifyRecover. A third call is not possible. For further verifications C_VerifyRecoverInit must be called first.

Encrypt (RSA):

Description:	Encrypts data.
Order:	C_EncryptInit, C_EncryptUpdate, C_EncryptFinal or C_EncryptInit, C_Encrypt C_Encrypt works as if C_EncryptUpdate and then C_EncryptFinal were called.
Special Feature:	C_EncryptUpdate stores the data temporarily. And you can pick up finished data with C_EncryptUpdate. If you don't do this, you receive with C_EncryptFinal all data at one time. The data is however only once available!

Decrypt (RSA):

Description:	Decrypts data.
Order:	C_DecryptInit, C_DecryptUpdate, C_DecryptFinal or C_DecryptInit, C_Decrypt C_Decrypt works as if C_DecryptUpdate and then C_DecryptFinal were called.
Special Feature:	C_DecryptUpdate stores the data temporarily. And you can pick up finished data with C_DecryptUpdate. If you don't do this, you receive with C_DecryptFinal all data at one time. The data is however only once available!

Digest (Hashfunctions SHA1, MD2, MD5):

Description:	A hash value is calculated from the data.
Order:	C_DigestInit, C_DigestUpdate, C_DigestFinal or C_DigestInit, C_Digest C_Digest works as if C_DigestUpdate and then C_DigestFinal were called. C_DigestUpdate processes the data immediately.

Appendix B: Non-Standard Functions in PKCS#11 DLL

Two non-standard functions for the token initialization are added to the PKCS#11 library cmP11.

CK_RV *EraseProfile*(

```
CK_SLOT_ID      slotID,          /* ID of the token's slot */
CK_BYTE_PTR     pCardPIN,        /* CardPIN value */
CK_ULONG        ulCardPINLen     /* length of CardPIN value */
);
```

Description: Erase the existed profile on a token. In order to erase the profile, the Card-PIN must be verified.

CK_RV *CreateProfile* (

```
CK_SLOT_ID      slotID,                 /* ID of the token's slot */
CK_UTF8CHAR_PTR pProfile,               /* profile name, null terminated */
CK_BYTE_PTR     pSerNum,                /* serial number */
CK_ULONG        ulSerNumLen,            /* length of serial number */
CK_BYTE_PTR     pCardPIN,               /* CardPIN value */
CK_ULONG        ulCardPINLen,           /* length of CardPIN value */
CK_BYTE_PTR     pSOPIN,                 /* SO PIN value */
CK_ULONG        ulSOPINLen,             /* length of SO PIN value */
CK_BYTE_PTR     pUserPIN,               /* UserPIN value */
CK_ULONG        ulUserPINLen,           /* length of UserPIN value */
CK_UTF8CHAR_PTR pLabel,                 /* 32-byte token label (blank padded) */
CK_ULONG        ulUserPINRetry          /* retry counter of UserPIN */
);
```

Description: Create a profile. The possible profile names are “CORPORATE”, “PKCS15” and “CNS”. Usually, the token must be empty or the old profile must be erased before the new profile is written to the token.

Remark: Not all profiles are supported by all smartcards.

CardOS V4.x supports: CORPORATE, PKCS15, CNS

CardOS M4.0(a) supports: CORPORATE

JavaCards support: CORPORATE, PKCS15

ACOS supports: CORPORATE.

Appendix C: Log Information

Logging information may serve to find and correct errors but impacts performance. In general, logging should be disabled. The logger should only be used by experienced users or when asked to. The log-file format is as follows: Each entry contains the function name, the parameter before and after the function call and the result of the function. Private information is hidden by a static string "[----------]", so only the length is readable.

Convenience Files

To enable logging with the default settings .reg files can be found in the installation directory

`<program files>\Charismathics\smart security interface x.zz\`

`CSSI_Param.reg` contains logging parameters for PKCS#11 and the CSP

`CSSI_TSS.reg` contains logging parameters for TSS/TPM logging

Registry Settings

Logging is controlled by registry entries stored in

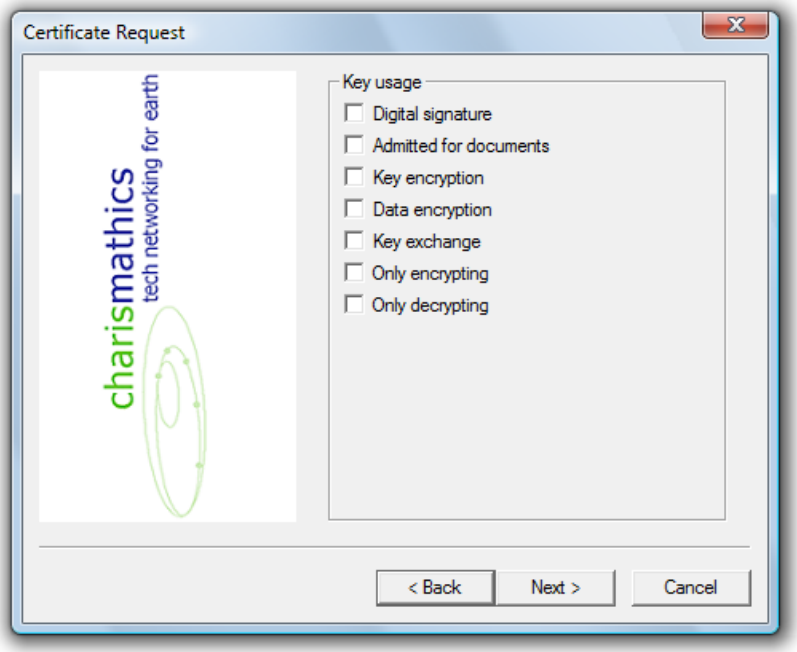
`[HKEY_LOCAL_MACHINE\SOFTWARE\charismathics\smart security interface]`

`"LogFile_mode"=dword:00000001`
Use 1 to enable logging, 0 to disable logging

`"CSP_DeactivateUnregister"=hex:00`
`"CSP_RegisterMachineStore"=hex:00`
Leave at default for logging

```
"PKCS11_LogFile_name"="c:\\temp\\cmP11.log"
"CSP_LogFile_name"="c:\\temp\\cmCSP.log"
"TSP_LogFile_name"="c:\\temp\\cmTSP.log"
"TCS_LogFile_name"="c:\\temp\\cmTCS.log"
```
Select a logging file and directory. Use only absolute paths names. Remember to to maintain backslash '\' doubling.

Appendix D: Certificate Attributes (Key Usage)



A short explanation of the options follows:

1. Digital Signature: Here you can verify digital signature (except those under two named purposes) e.g. authentication.
2. Admitted for Documents: Here you can verify signatures, that check the liability and bindingness of documents (except signatures of certificates and CRLs of CA).
3. Key encryption: Encryption of keys for the purpose of their transmission.
4. Data encryption: Encryption of data for the purpose of transmission, but not of keys.
5. Key exchange: Employment of the key to agree on other keys, e.g. a Diffie-Hellman key.
6. Only encrypting: This option is mutually exclusive with all other options
7. Only decrypting: This option is mutually exclusive with all other options