Charismathics Smart Security Interface ©

User Manual V 5.0

Contents

Thank you for purchasing the Charismathics Smart Security Interface (CSSI).

Charismathics Smart Security Interface provides modules that you need in order to integrate different smart cards, USB tokens and TPM chips into your applications. The functionality ranges from administration of the card to modules supporting the operating system to use the token. The following file structures (profiles) are supported:

- Charismathics corporate profile
- PKCS#15 profile
- Carta Nazionale dei Servizi (CNS) profile
- FINEID profile
- AET Profile
- PIV Profile
- IAS Profile
- A-Trust Profile
- EDU Profile

Charismathics Smart Security Interface is comprised of the following modules:

- the user tool - Charismathics Smart Security Interface Utility
- the CSSI Extension Tool for adding new ATR/OS associations
- the CSP
- the PKCS#11-module
- Charismathics Key Storage Provider
- CSSI Setting tool
- the TSS module for TPM chips (optional)
- CardOS V4.x mini driver (optional)

The user tool **Charismathics Smart Security Interface Utility** allows changing your user PIN and registering your smart card or USB token.

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 interface. PKCS#11-Modules are in use by Netscape and in Novell environments.

Charismathics Key Storage Provider, implementation of crypto Next Generation, supported under windows vista and above. Enable use of SHA2 family hashing algorithm and ECC keys.

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

1 About this Manual

The **Charismathics Smart Security Interface** Security token configurator tool is described in chapter 3: “Charismathics Security Token Configurator”. It contains information on how to manage keys and certificates, changing PINs, unlocking, initializing and personalizing smart cards.

The **Charismathics Smart Security Interface** user edition is described in chapter 4: “User Tool: CSSI Utility”. It contains information on how to change PINs and unlock PIN.

Furthermore, you will find additional information regarding the Register Tool, CSSI Extension Tool, CSP and PKSC#11 and which applications may be upgraded by hardware tokens. Application developers can find further information on how to access modules (e.g. accessing PKCS#11) of **Charismathics Smart Security Interface** in the appendices, if they intend to develop a proprietary application. An explanation on how to configure environments of Microsoft or other producers exceeds the scope of this manual. In these cases, please consult the documentation of the corresponding supplier.

Note: To understand this manual you need basic knowledge in IT-security. Especially, you should be familiar with the following notions: certificate, private and public key, secret key, digital signature, PKI, etc. Please consult the glossary on IT security on the Charismathics homepage (http://www.charismathics.com/support/it-references/it-security-glossary/) if you want to consolidate your knowledge.

2 Installation

Before you can install **Charismathics Smart Security Interface,** the card reader you intend to use must be installed according to the manufacturer's guidelines and be fully operational. 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.

2.1 Installation Requirements

If not explicitly required otherwise in the following:

- Microsoft Windows XP
- Windows Vista
- Windows 2000
- Windows Server 2003
- Windows Server 2008
- Windows 7

Note: During the installation process the CSP Module is registered automatically with the Windows operating system. The following applications are supported:

- Smart card login to a Windows 2000 or 2003 or 2008-Domain:
  ADS, Enterprise CA, Windows 2000 or 2003 or 2008 Server and as Client: Windows 2000 Professional or Windows XP Professional or Windows Vista or Windows 7 or Windows Server
- SSL- Authentication with smart card using Internet Explorer:
  Microsoft Internet Explorer Version 5.0, 5.5, 6.0, 7.0, 8.0, 9.0 and 10 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
  MS Office 2003, 2007, 2010
- 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
  Windows 2003 Server and as Client: Windows 2000 or XP
  Windows 2008 Server and as Client: Windows XP or Vista or Windows7
- 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 Google Chrome
- SSL- Authentication with smart card with Mozilla Firefox:
  Mozilla Firefox Version 1.5 and 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 Netscape Messenger:
  Netscape Messenger 4.72 (High Encryption), 4.73, 4.76, 7.x
- Email-Security via smart cards with Mozilla Thunderbird 1.5 and above
- 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 for Betrusted Unicert V5.2 for Windows
- Compatibility/Smart card administration of the Entrust-PKI (PKCS#11): Security Manager Administration 7.0
- Compatibility/Smart card administration of the Ecos-PKI Appliance BB5000 (PKCS#11)
- Terminal Server: Microsoft, Citrix, SunRay (oracle)

Note: The mentioned products do not require any further client software. Please refer to the manual of your software application if it is not listed above.

Furthermore, CSSI ties in with the following preboot/ harddisk encryption environments:

- CheckPoint or Pointsec
- Utimaco
- McAfee
- PGP
- Secude

2.2 Supported Smart Cards

For the complete list of CSSI supported smart card follow the link below:

http://www.charismathics.com/products/charts/cssi-supported-profiles/

Following smart cards/tokens are tested with Charismathics Smart Security Interface - standard Version:

- ACOS A-Trust Card
- ACOS EMV A03
- ACOS A04
- ACOS A05
- ACOS SMARTMX
- ActivIdentity Card
- Axalto Cyberflex Access V2c
- CardLogix Java 2.2.1
- Feitian FIPCS COS
- Feitian FTJCOS
- Siemens CardOS M4.01(a)
- Siemens CardOS V4.20
- Siemens CardOS V4.2B
- Siemens CardOS V4.2c
- Siemens CardOS 4.2C DI

- Siemens CardOS V4.30
- Siemens CardOS V4.3B
- Siemens CardOS V4.4
- Gemalto EMV – PKI
- Gemalto TOP IM GX4
- Gemalto IAS ECC
- GemXpresso Pro R3.2
- JCOP 20
- JCOP 21
- JCOP 30
- JCOP 31
- JCOP 41
- JCOP J2
- JCOP J3
- JCOP J4
- jTOP JCX32/36
- KONA 10
- KONA 132
- KONA 25
- KONA 26
- Keepod
- Micardo EC 2.x
- Morpho Orga YPS-ID2
- Morpho YPS-ID3 IAS ECC
- NetKey E4/2000
- NetKey PKS/2000/E4
- Oberthur Cosmo V5.2 PIV
- Oberthur Cosmo v5.4
- Oberthur Cosmopo RSA V5.x
- Oberthur CosmopolIC 64K V5.2
- Oberthur Cosmo ID-One V5.2 PIV
- Oberthur ID-One Cosmo V7.0
- Oberthur ID-One Cosmo V7.0 DI
- Oberthur ID-One Cosmo V7.0 – n
- Oberthur ID-One Cosmo V7.0 - a
- Oberthur ID-One v7 IAS ECC
- PAV Card ABACOS
- Privaris PlusID 60,75,90
- Setec SetCard
- Sm@rtCafe Expert 2.0
- Sm@rtCafe Expert 2.1
- Sm@rtCafe Expert 3.0
- Sm@rtCafe Expert 3.1
- Sm@rtCafe Expert 3.2
- Sm@rtCafe Expert 64k
- Sm@rtCafe Expert 5.0
- StarCOS 3.0
- StarCOS SPK 2.3
- StarCOS SPK 2.4
- StarCOS SPK 3.0
- TCOS 2.x
- Wibu Code Meter Dongle
- Watchdata TimeCOSPK

Following PIV/CAC smart cards are tested with Charismathics Smart Security Interface - PIV Version:

- Cyberflex Access 64K V1 SM 4.1
- CosmopolIC 64K V5.2 Fast ATR (2)
- Cyberflex Access 64K V2c
- Gemalto TOP DL - protiva PIV applet V1.55
- Gemalto TPC DM 72K PIV
- Gemalto TOP DL V2 - protiva PIV applet V1.55
- Gemalto TOP DL GX4 144K FIPS
- GEMALTO GCX4 72K DI
- Gemalto TOP DM GX4 72K (FIPS)
- GemXpresso PRO 64K R3 FIPS V2 #2
- Gemalto TOP DL GX4 PIV

- GoldKey PIV Token
- Oberthur ID one Cosmo V5 - PIV applet V1.08 Oberthur
- Oberthur ID One Cosmo 64 V5.2 - AI PIV End Point Applet
- Oberthur ID One PIV (Type A) Large - ID One PIV applet Suite2.3.2
- Oberthur ID-One Cosmo V5.2 - AI PIV End pont applet
- Oberthur ID-One Cosmo V7.0 – n PIV
- Oberthur ID-One Cosmo V7.0 -n type A Standard D - ID one PIV applet suite 2.3.2
- Oberthur ID-One Cosmo V7.0 type B – Large D - ID one PIV applet suite 2.3.2
- Oberthur ID-One Cosmo 128K v5.5 #2
- Oberthur ID One V5.2a Dual
- Oberthur CosmopolIC 64K V5.2 Fast ATR (1)
- SIPRNet token

Charismathics Smart Security Interface supports the following TPM chips:

- Atmel TPM
- Broadcom TPM
- Infineon TPM
- Intel TPM
- ST TPM
- Nuvoton TPM

2.3 Tested Card Readers

Please make sure your PC/SC smartcard reader has been installed according to the producer's specifications and is fully operational. **Charismathics Smart Security Interface** has been tested with the following card readers:

- ACS38 USB
- charismathics plug'n'crypt
- Eutron cryptoidentity CCID
- Eutron Digipass 860
- Fujtsu Siemens Computer Smartcase KB SCR PRO
- Fujtsu Siemens Computer Smartcase KBPC CX
- Fujtsu Siemens Computer Smartcase SCR USB
- Fujtsu Siemens Computer Smartcase SCR USB internal
- Fujtsu Siemens Computer Smartcase Token USB
- KOBIL KAAN advanced
- Omnikey Cardman 1010 serial
- Omnikey Cardman 2011 serial
- Omnikey Cardman 2020 USB
- Omnikey Cardman 3021 USB
- Omnikey Cardman 3121 USB
- Omnikey Cardman 3620 USB
- Omnikey Cardman 3621

- Omnikey Cardman 3821
- Omnikey Cardmann CM4040 (PC-Card)
- ORGA Card Mouse USB
- SCM SCR 331 USB
- SCM SCR 3310 USB
- SCM SCR 3340 (Express-Card)
- SCM SCR 532 serial/USB
- SCM SCR241 PCMCIA
- SCM SCR333
- SCM SCR335 USB

Additionally a great number of readers not explicitly mentioned above, but built upon compatible hardware, are supported.

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.

2.4 Secure Pin Entry (SPE)

A number of card readers come equipped with their own PIN-pad. It has been tested with following smart card reader:

- Cherry Keyboard G83-6644
- Omnikey 3621 USB
- OmniKey 3821 USB
- SCM SPR532

Additionally a great number of readers not explicitly mentioned above, but built upon compatible hardware, are supported.

Please make sure your windows device drivers are up to date if you want to use PC/SC 2.0 with SPE.

To enable/disable SPE, edit the registry setting at

[HKEY_LOCAL_MACHINE\SOFTWARE\charismathics\smart security interface]
To activate SPE, use: "USE_PINPAD"=hex:01

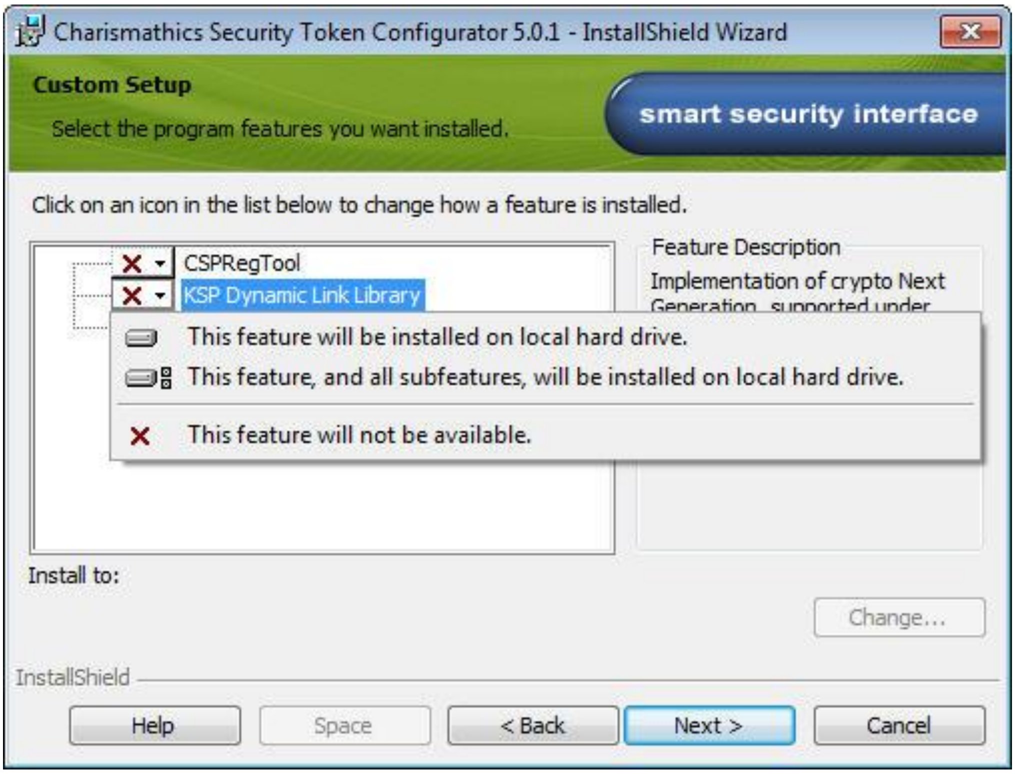
To deactivate SPE, use: "USE_PINPAD"=hex:00

Although CSSI supports alphanumeric PINS in general, SPE obviously only supports digits. Please make sure the PINs used for the card can be entered by using SPE if you intend to use it.

2.5 Krypto Service Provider (KSP) Installation

Microsoft requires a CNG component for SHA2 and ECC support under windows vista and above. Charismathics therefore provides key storage provider which works in concert with the CSP.

In order to install KSP component you need to run the setup package in Custom setup mode and select KSP dynamic link library for installation as shown in the screenshot below.



Charismathics Security Token Configurator 5.0.1 - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- CSPRegTool
- KSP Dynamic Link Library

Feature Description

Implementation of crypto Next Generation, supported under

- This feature will be installed on local hard drive.
- This feature, and all subfeatures, will be installed on local hard drive.
- This feature will not be available.

Install to:

2.6 Unattended Installation

Silent Mode Installation:

To install the CSTC edition**:**

Charismathics SSI 5.0.1 CSTC.msi /S /v"/qn"

With Virtual CCID reader driver:
Charismathics SSI 5.0.1.exe /S /v"CCID=1 /qn"

Without Virtual CCID reader driver:
Charismathics SSI 5.0.exe /S /v"CCID=0 /qn"

To install the User edition:

Charismathics SSI 5.0.1 User Edition.msi /S /v"/qn"

With Virtual CCID reader driver:
Charismathics SSI 5.0.1 User Edition.msi /S /v"CCID=1 /qn"

Without Virtual CCID reader driver:
Charismathics SSI 5.0.1 User Edition.msi /S /v"CCID=0 /qn"

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

To install the Charismathics Security Token Configurator tool:

```
msiexec /i "Charismathics SSI 5.0 CSTC.msi" /qn
```

To install the Evaluation edition:

```
msiexec /i "Charismathics SSI 5.0 Eval Edition.msi" /qn
```

To Un-install the CSSI Software:

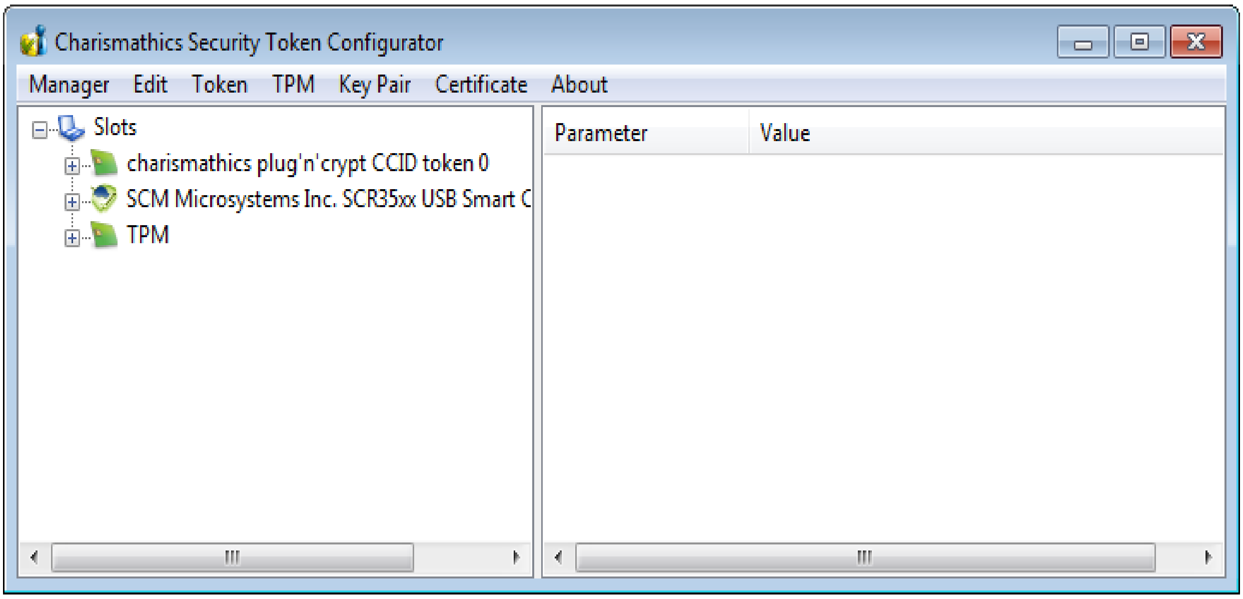
```
msiexec /x "path to .msi package"
```

3 Charismathics Security Token Configurator

Token Configurator tools enable personalizing the card, changing your PINs, unlocking tokens, importing certificate and pfx file, generating keys and self signed certificates and so on.

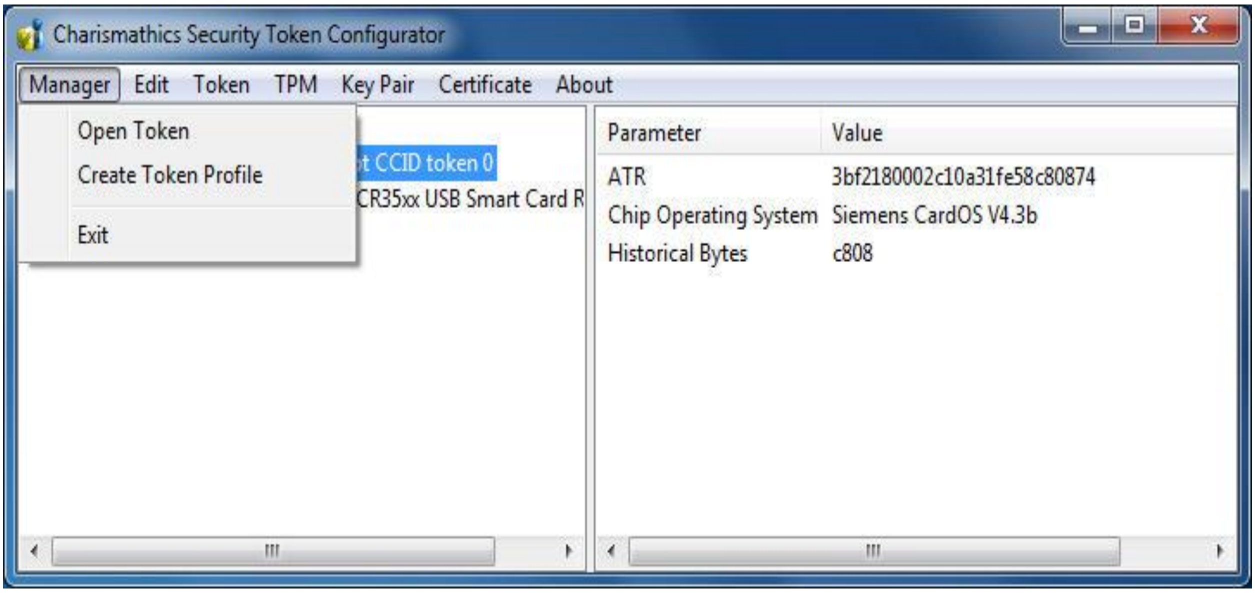
3.1 User Interface

After opening the CSTC tool you will see the interface you see below. The "TPM" Menu item is only visible if the optional TSS module has been installed and TPM hardware is present


Charismathics Security Token Configurator
Manager
Edit
Token
TPM
Key Pair
Certificate
About
Slots
charismathics plug'n'crypt CCID token 0
SCM Microsystems Inc. SCR35xx USB Smart C
TPM
Parameter
Value

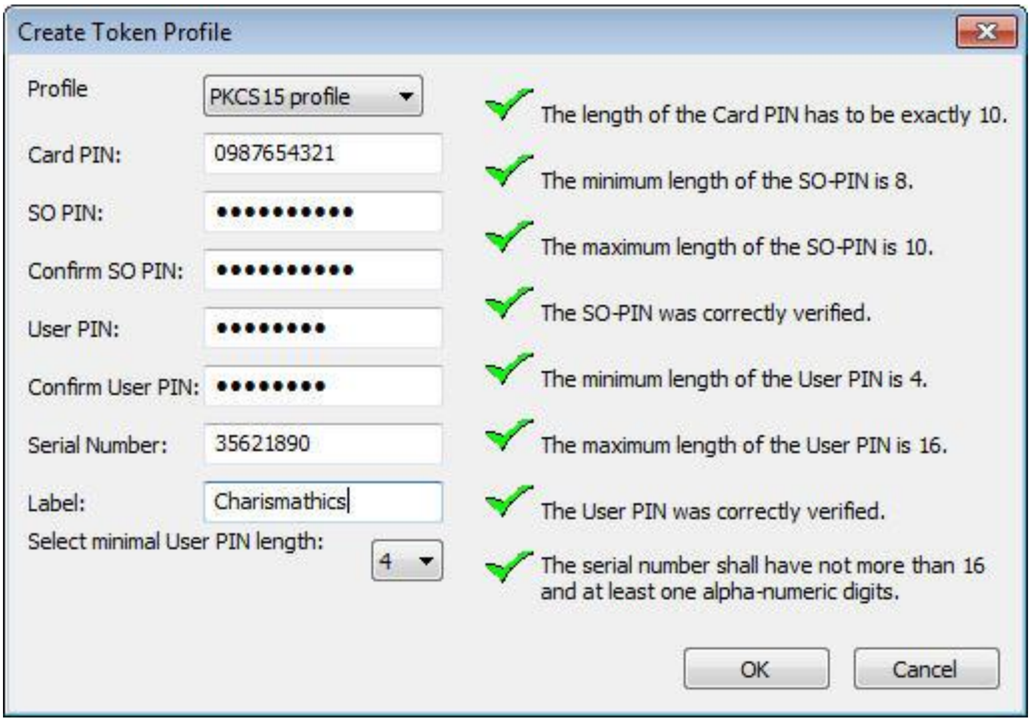
The left panel displays the list of smart card readers which are connected to the system. Hardware smart card readers, virtual USB token readers and TPM hardware are displayed in the same window. Once a token has been inserted, the hierarchy is extended. Selecting an item in the hierarchy view displays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

3.1.1 Manager Menu



Parameter	Value
ATR	3bf2180002c10a31fe58c80874
Chip Operating System	Siemens CardOS V4.3b
Historical Bytes	c808

- “Open Token”: To view the contents of a token, select the reader which contains the smart card, USB Token or TPM from the hierarchy and select “Open Token” from the “Manager” menu. Clicking the plus-icon in front of the reader to expand the hierarchy serves the same purpose.
  At first, only public information is available, e.g. label of the token, the profile and free memory. 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 or USB token. This feature is described in detail in 3.7 “Preparing a Token (Initialization and Personalization)”.



Profile	PKCS15 profile
Card PIN:	0987654321
SO PIN:	••••••••••
Confirm SO PIN:	••••••••••
User PIN:	••••••••
Confirm User PIN:	••••••••
Serial Number:	35621890
Label:	Charismathics
Select minimal User PIN length:	4

✓ The length of the Card PIN has to be exactly 10.

✓ The minimum length of the SO-PIN is 8.

✓ The maximum length of the SO-PIN is 10.

✓ The SO-PIN was correctly verified.

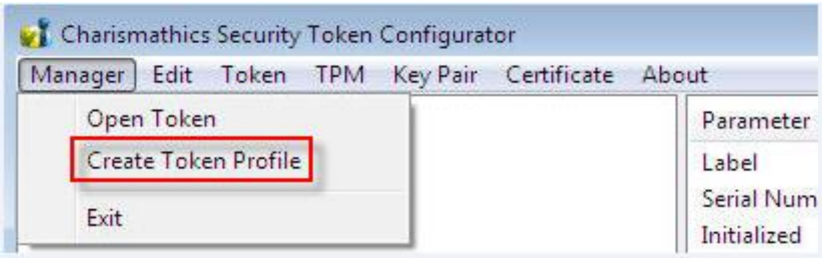
✓ The minimum length of the User PIN is 4.

✓ The maximum length of the User PIN is 16.

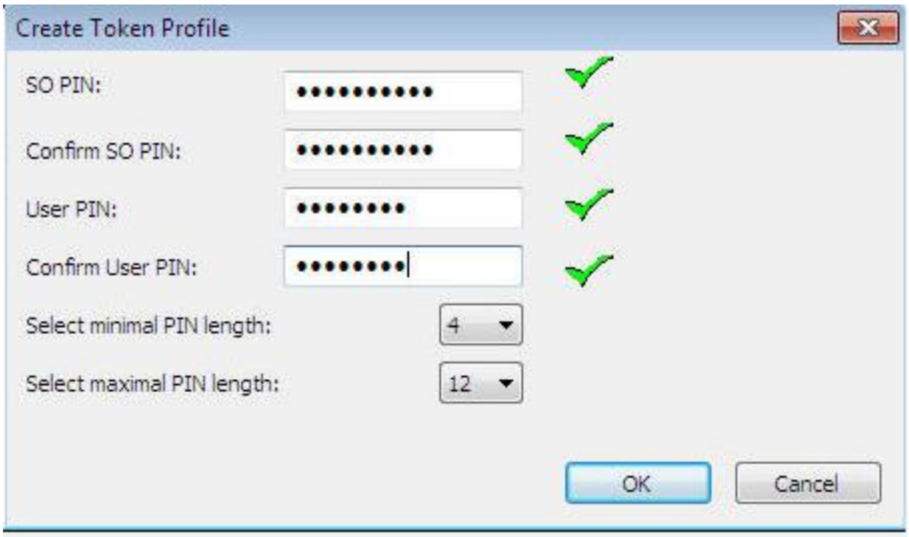
✓ The User PIN was correctly verified.

✓ The serial number shall have not more than 16 and at least one alpha-numeric digits.

- Initializing Wibu Code Meter Dongle: The Charismathics Security Configurator tool is able to initialize the Wibu Code Meter Dongle. Insert the wibu code meter dongle and select "Create Token Profile" from the security token configurator tool menu as shown in the screenshot below.



Enter the relevant information and click OK to initialize.



SO PIN: •••••••••••

Confirm SO PIN: •••••••••••

User PIN: ••••••••

Confirm User PIN: ••••••••

Select minimal PIN length: 4

Select maximal PIN length: 12

With SO PIN it is possible to erase completely the old profile and re-initialize the cod meter dongle.

Note: the default card PIN for the Wibu Code Meter Dongle is "CodeMeter", which is assigned during the pre-initialization.

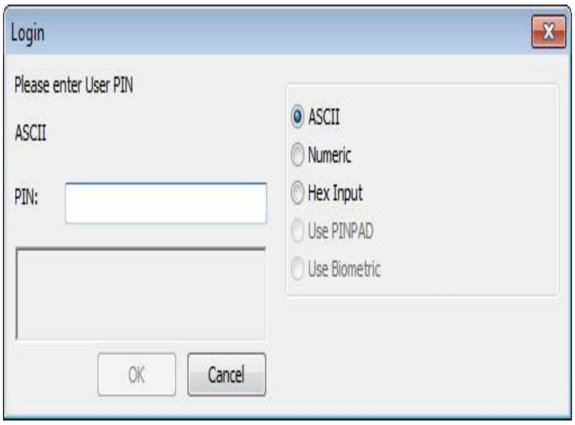
3.1.2 Edit menu/ Context menu

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 chapter 3.9 "Further Functions"

3.1.3 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": Prior to operations on the token, the user is required to log in. Logging in requires 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.



Login

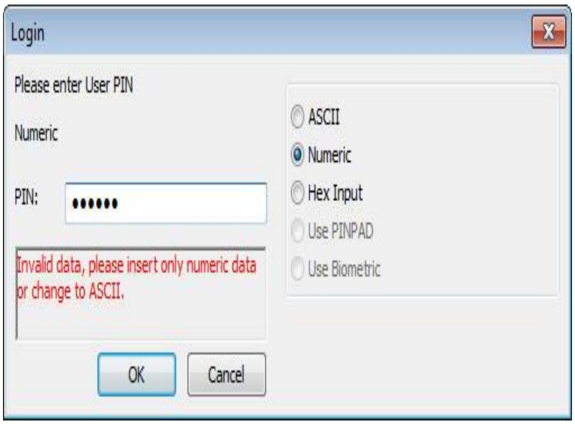
Please enter User PIN

ASCII

PIN:

● ASCII
○ Numeric
○ Hex Input
○ Use PINPAD
○ Use Biometric

OK Cancel



Login

Please enter User PIN

Numeric

PIN: ••••••

Invalid data, please insert only numeric data or change to ASCII.

○ ASCII
● Numeric
○ Hex Input
○ Use PINPAD
○ Use Biometric

OK Cancel

The hardware configuration and user settings determine the initial PIN entry method. To change the method use the dialog extension symbols ">>".

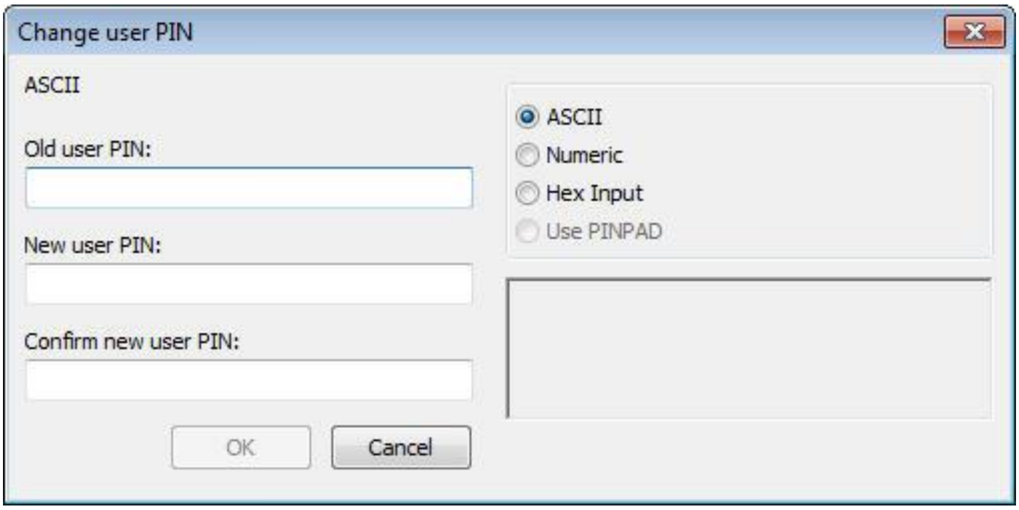
Supported entry methods are:

- **ASCII:** each character of the PIN needs to be according to the ASCII table
- **Numeric:** each character of the PIN needs to be a digit ('0'…'9'). This can be used to ensure PINPAD compatibility.
- **Hex Input:** the PIN has to be entered in a hexadecimal format. That means the length of the PIN has to be even and only characters '0'-'9' and 'a'-'f' are valid.
- **Use PINPAD:** this option is enabled only when the authentication to the token is possible via secure PIN entry. When this option is selected, the edit text for the PIN will be disabled and the user must input the PIN from the corresponding SPE reader.
- **Use Biometric:** this option is enabled only when biometric authentication is possible by using a corresponding token. When this option is selected, the other PIN types will be disabled and a "Scan" button can be selected in order to start the biometric authentication.

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.

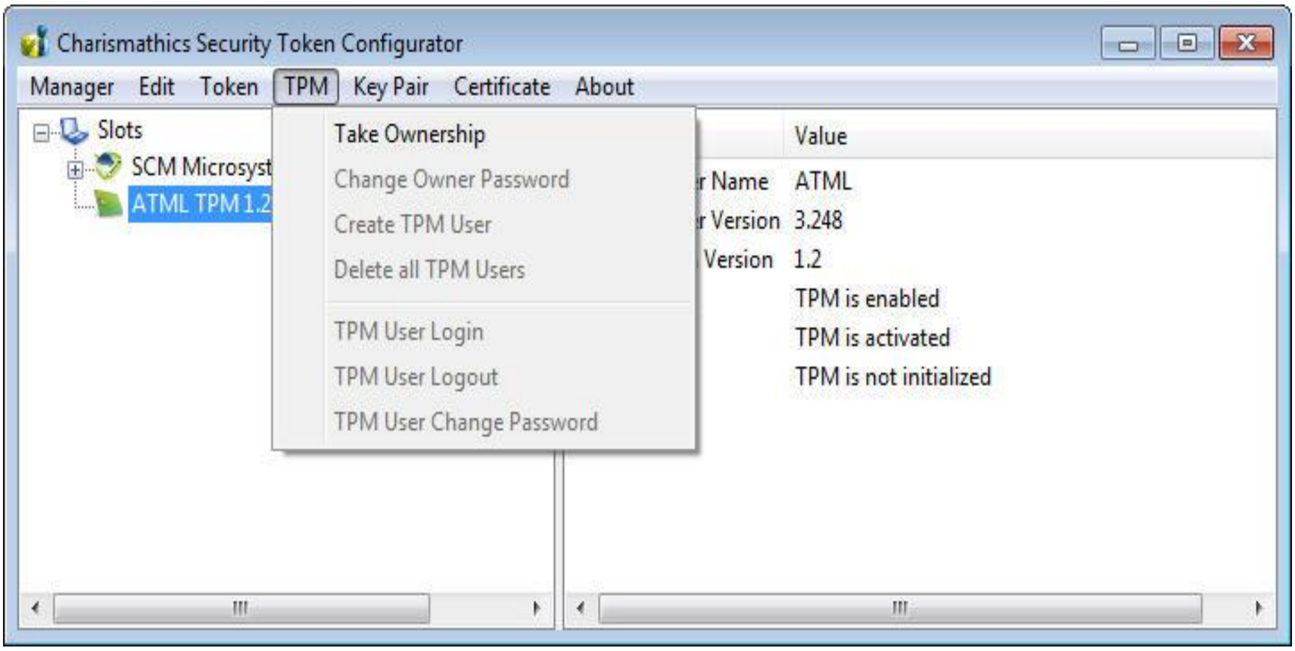
- "Logout": This item works analogous to the "Login" option.

- “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. The PIN entry method can be changed the same way as in the login dialog.

3.1.4 TPM menu



The TPM menu is only visible if the optional TSS module has been installed. The functions of the menu require that TPM hardware has been selected in the hierarchy view. See also chapter 3.8 “TPM Management”

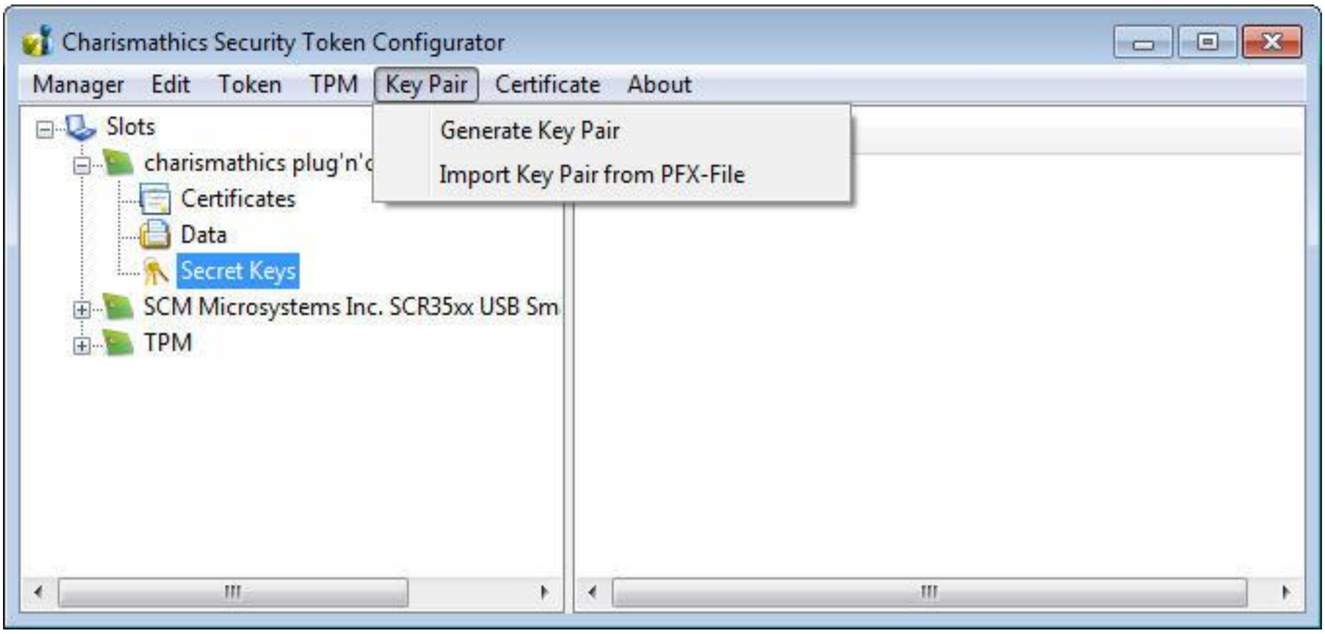
- “Take Ownership”: This option is only available if Ownership of the TPM module has not yet been taken. Ownership is required for functions like TPM User creation to work. Taking Ownership of the

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": Security Token Configurator 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 is entered incorrectly regardless of the number of failed attempts.

3.1.5 Key Pair menu

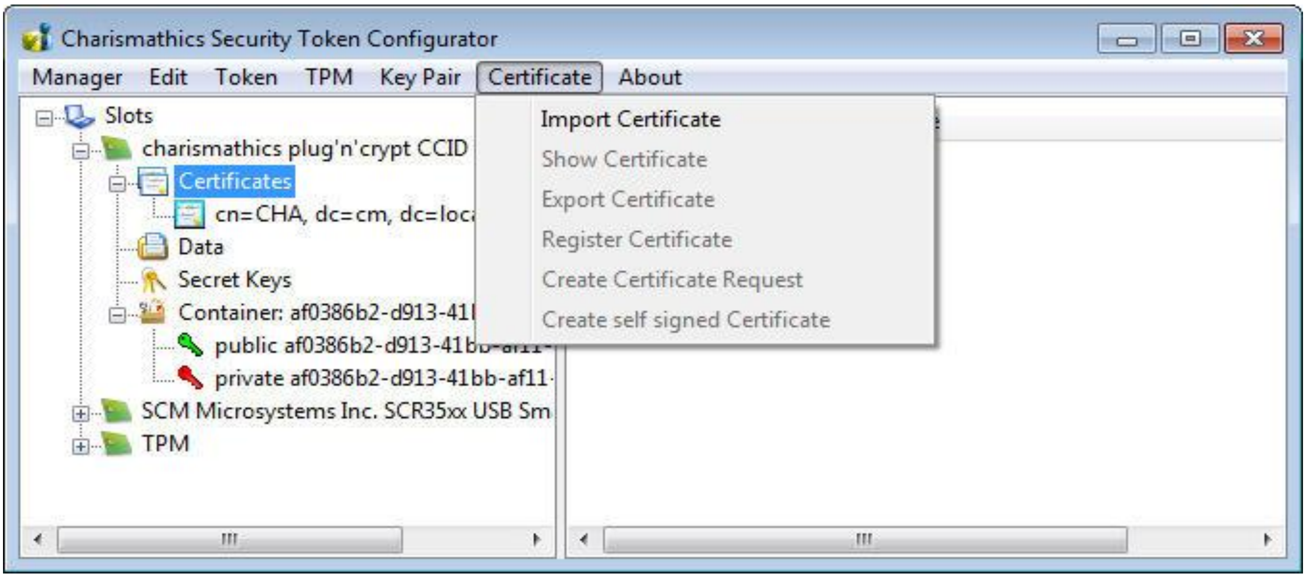


It is possible to generate several key pairs with corresponding certificates on the card. Each set comprised of private key, public key (optional) and certificate (optional) is stored in a separate container.

- "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 chapters 3.4 "Generating and Importing Keys" and 3.5 "Generating and Importing Certificates".
- "Import Key Pair from PFX-File": This item opens a dialog asking for the PFX file to import.

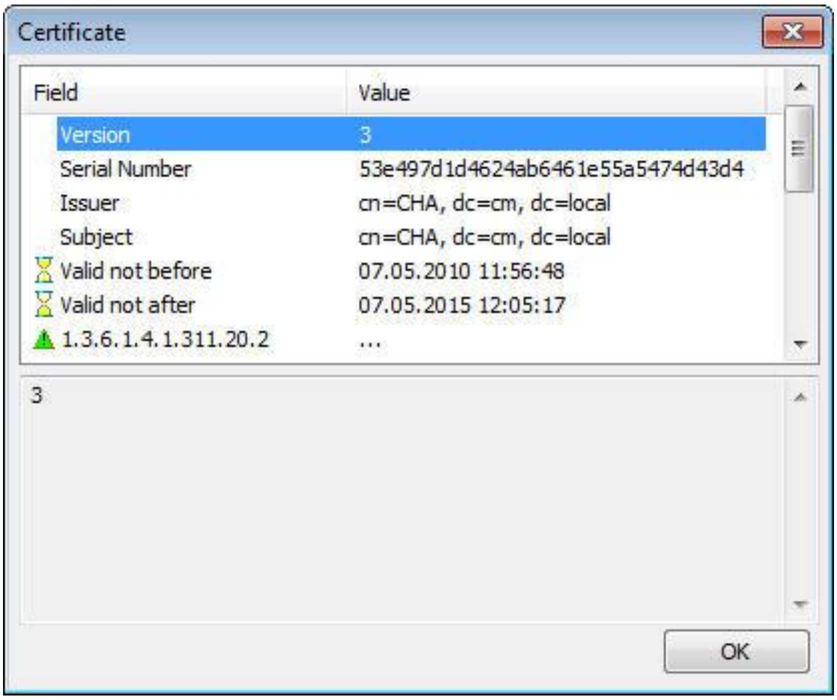
3.1.6 Certificate menu

Most items of the certificate menu are also accessible from the context menu when a certificate, public or private key, an object node, e.g. "Certificates" node in the hierarchy, is right-clicked.


Charismathics Security Token Configurator
Manager
Edit
Token
TPM
Key Pair
Certificate
About
Import Certificate
Show Certificate
Export Certificate
Register Certificate
Create Certificate Request
Create self signed Certificate
Slots
charismathics plug'n'crypt CCID
Certificates
cn=CHA, dc=cm, dc=loc
Data
Secret Keys
Container: af0386b2-d913-41
public af0386b2-d913-41bb-af11-
private af0386b2-d913-41bb-af11-
SCM Microsystems Inc. SCR35xx USB Sm
TPM

- "Import Certificate": After selecting this item, pick the certificate to import from the opened dialog. If the certificate can be associated with a private/public key pair, it is automatically inserted into the correct 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.

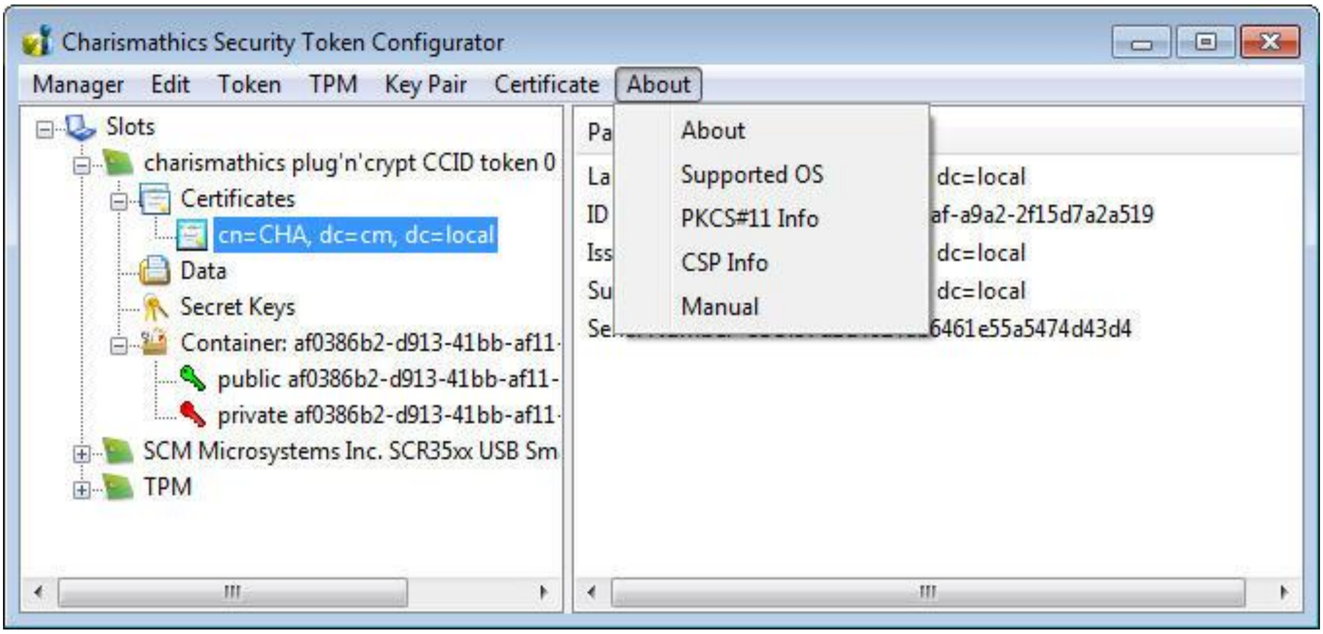


Field	Value
Version	3
Serial Number	53e497d1d4624ab6461e55a5474d43d4
Issuer	cn=CHA, dc=cm, dc=local
Subject	cn=CHA, dc=cm, dc=local
⌛ Valid not before	07.05.2010 11:56:48
⌛ Valid not after	07.05.2015 12:05:17
⚠ 1.3.6.1.4.1.311.20.2	...

3

- “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 3.5 “Generating and Importing Certificates” for a 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.

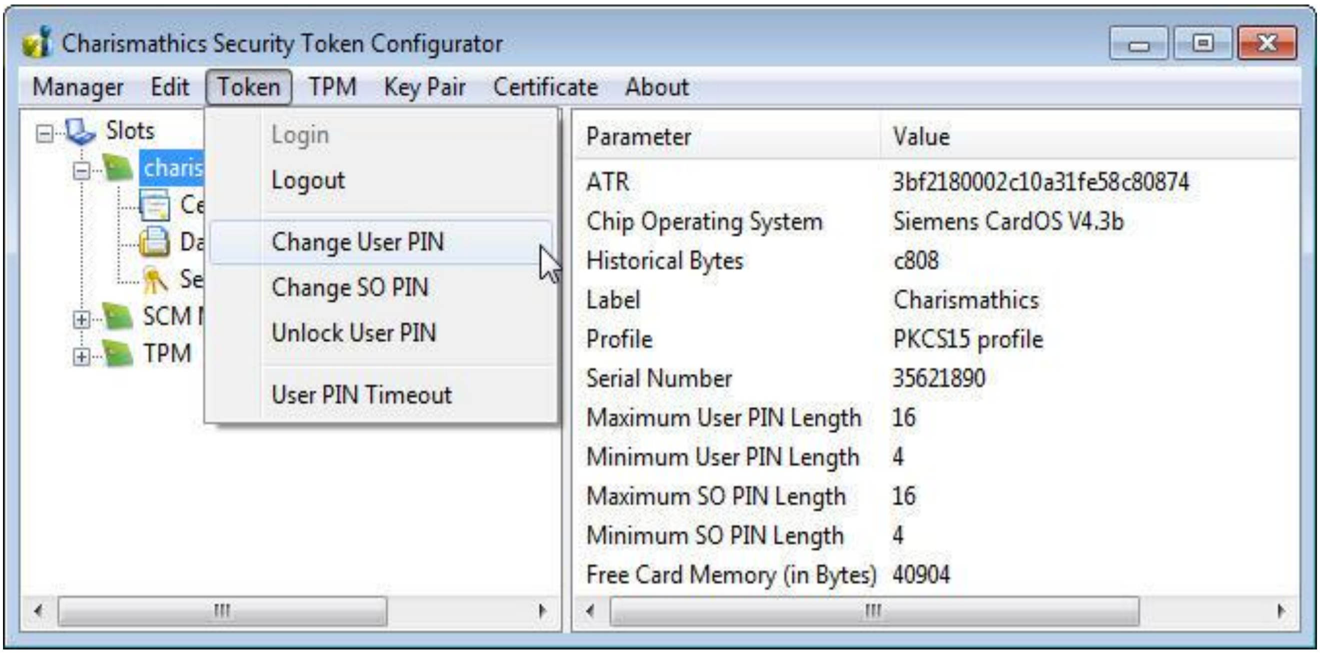
3.1.7 Info menu



- “About”: Displays general version information about the CSTC edition.
- “Supported OS”: Displays the list of smart card operating systems supported by CSSI. This list includes only the predefined associations. Additional associations can be created with the CSSI 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.

3.2 Changing PINs

Usually there are 3 PINs on a token: the User PIN, the SO PIN (PIN of the system operator, i.e. system administrator) and the Card PIN. The term Card PIN is used for USB Tokens as well. Please note that not all cards and tokens support changing all PINs. The CSSI supports alphanumeric PINs and is not restricted to numeric digits in general. Refer to Chapter 2.4 " ” on limitations. There are different functions to use with these 3 PINs:



Parameter	Value
ATR	3bf2180002c10a31fe58c80874
Chip Operating System	Siemens CardOS V4.3b
Historical Bytes	c808
Label	Charismathics
Profile	PKCS15 profile
Serial Number	35621890
Maximum User PIN Length	16
Minimum User PIN Length	4
Maximum SO PIN Length	16
Minimum SO PIN Length	4
Free Card Memory (in Bytes)	40904

The **User PIN** must be entered 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. Refer to the table below regarding default User PIN and User PIN length.

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. Refer to the table below regarding default SO PIN and SO PIN length.

The SO PIN is used exclusively for unlocking the User PIN. There are no other functions associated with the SO-PIN.

Important: After a number of consecutive wrong inputs the SO PIN will be locked. The number of retries depends on the card profile.

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

PIN (default)	Charismathics Profile	PKCS#15 Profile	CNS Profile
User PIN (11111111)	4- 8	4- 8	4- 8
SO PIN (1111111111)	8- 10	8- 10	4- 8
Card PIN (0987654321)	10	10	10

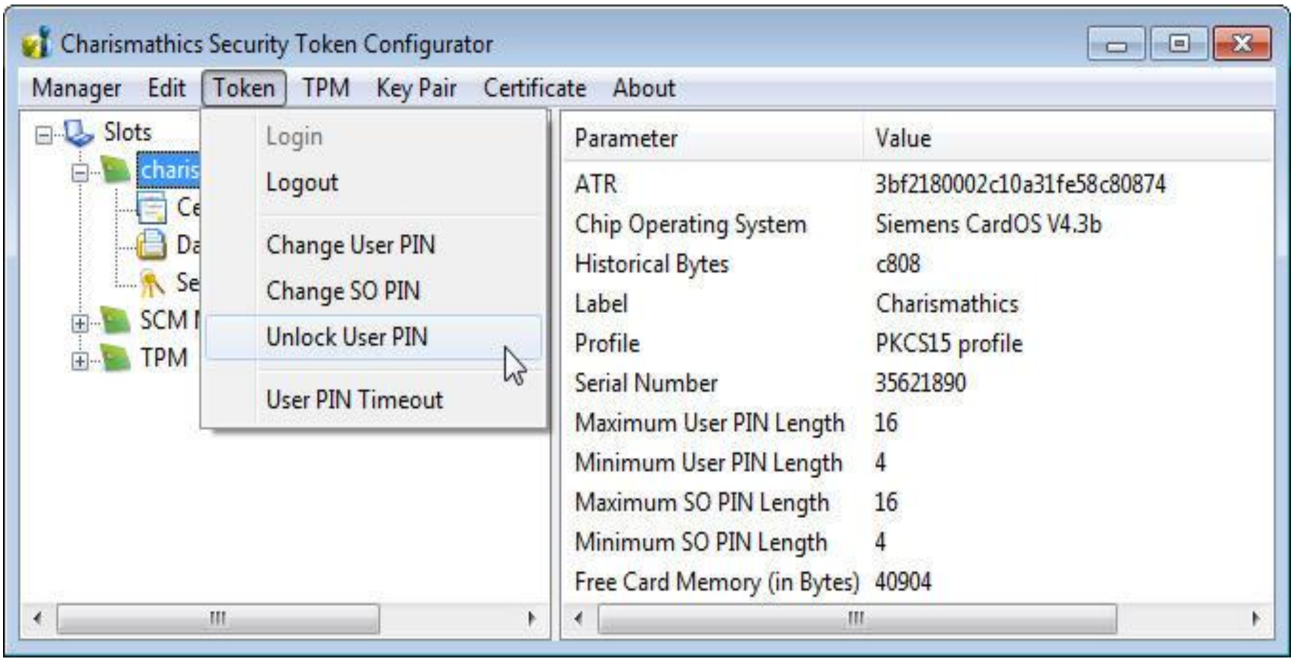
Note: For the Wibu Code Meter Dongle the default card PIN is CodeMeter.

3.3 Unlocking Tokens

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

But it might happen that you have entered the wrong PIN three times even as a 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. "Unlock User PIN" is available from the "Token" menu, as shown in the following figure:



Parameter	Value
ATR	3bf2180002c10a31fe58c80874
Chip Operating System	Siemens CardOS V4.3b
Historical Bytes	c808
Label	Charismathics
Profile	PKCS15 profile
Serial Number	35621890
Maximum User PIN Length	16
Minimum User PIN Length	4
Maximum SO PIN Length	16
Minimum SO PIN Length	4
Free Card Memory (in Bytes)	40904

3.4 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 securely stored and the public key must be accessible to communication partners by a certificate. These keys and certificates can be generated and managed by the Charismathics Security Token Configurator tool.

In principle there are two possibilities:

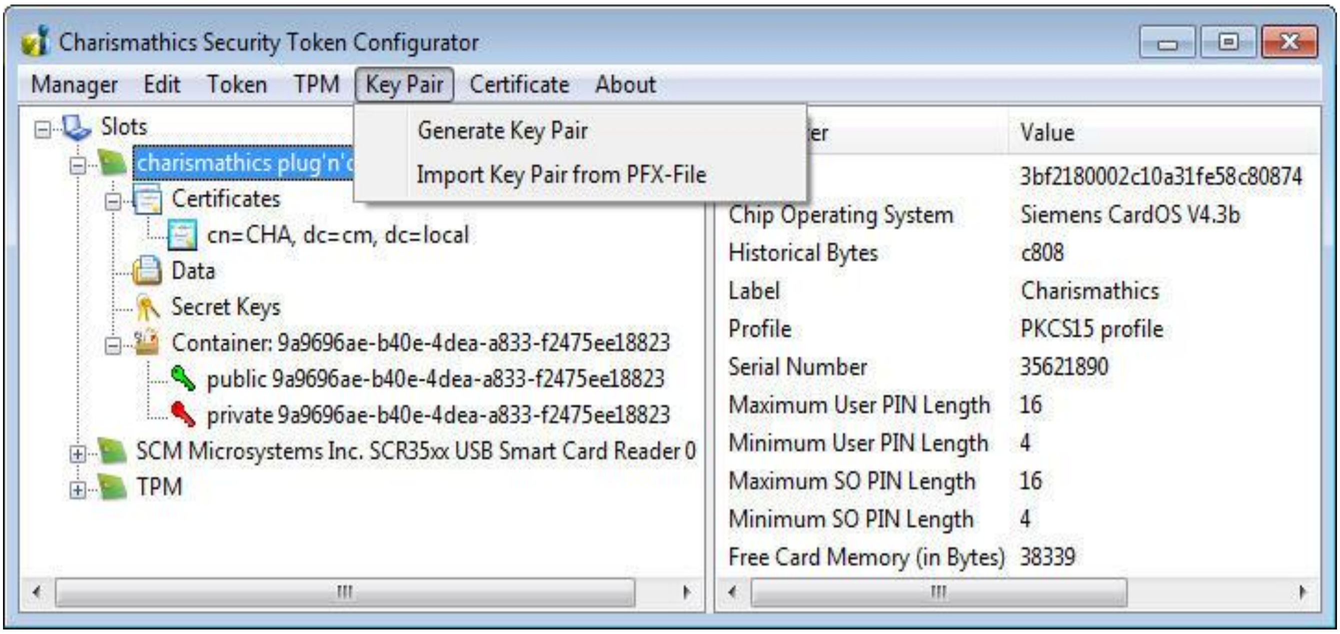
1. You can generate keys (key pairs comprising private and public keys and secret keys) with the administration tool - **Charismathics Security Token Configurator Tool.**
2. You already own a key and/or key pair. Then, you can import the key pair if necessary together with certificate as a PFX-file. 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”.

3.4.1 Generation of 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".


Charismathics Security Token Configurator
Manager
Edit
Token
TPM
Key Pair
Certificate
About
Generate Key Pair
Import Key Pair from PFX-File
Slots
charismathics plug'n'c
Certificates
cn=CHA, dc=cm, dc=local
Data
Secret Keys
Container: 9a9696ae-b40e-4dea-a833-f2475ee18823
public 9a9696ae-b40e-4dea-a833-f2475ee18823
private 9a9696ae-b40e-4dea-a833-f2475ee18823
SCM Microsystems Inc. SCR35xx USB Smart Card Reader 0
TPM

…er	Value
	3bf2180002c10a31fe58c80874
Chip Operating System	Siemens CardOS V4.3b
Historical Bytes	c808
Label	Charismathics
Profile	PKCS15 profile
Serial Number	35621890
Maximum User PIN Length	16
Minimum User PIN Length	4
Maximum SO PIN Length	16
Minimum SO PIN Length	4
Free Card Memory (in Bytes)	38339

The type of key and the key strength depend on the available hardware. Make sure your reader has support for Extended APDUs if you want to create and use 2048 bit keys.

3.4.2 Generation of ECC key pair

To generate an ECC key pair, go to “Generate Key pair” from the menu “Key Pair” and select Algorithm as ECC from the drop down menu.

3.4.3 Importing a Key Pair

If you already own a key pair that you intend to use, you can import it with 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 or ECC-key within a .pfx- or .p12-file.

3.4.4 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 recommended

Note: Algorithms with at least 128 bits (Triple-DES) are recommended. According to present day standards, lesser key lengths cannot be considered secure anymore.

3.4.5 Importing a Secret Key

If you own a secret key that you want to use, you can import it with 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 bits. Importing takes place by inserting the bits into the field "Secret Key (hexadecimal)", e.g. copy and paste.

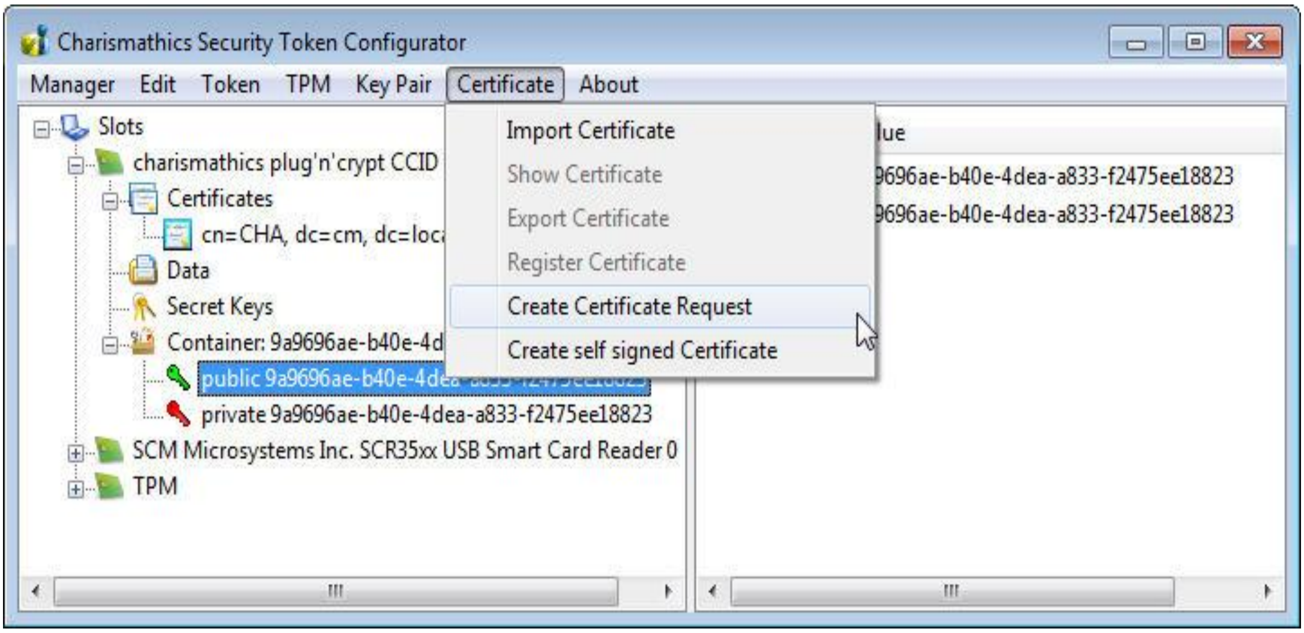
3.5 Generating and Importing Certificates

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 has to be accessible to communication partners via a certificate. These certificates can be generated and managed by the Charismathics Security token configurator tool. These options to create a certificate from within the Security Configurator tool are:

1. You can sign the certificate corresponding to a public key by you 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.

3.5.1 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.


Charismathics Security Token Configurator
Manager
Edit
Token
TPM
Key Pair
Certificate
About
Slots
charismathics plug'n'crypt CCID
Certificates
cn=CHA, dc=cm, dc=loc
Data
Secret Keys
Container: 9a9696ae-b40e-4d
public 9a9696ae-b40e-4dea
private 9a9696ae-b40e-4dea-a833-f2475ee18823
SCM Microsystems Inc. SCR35xx USB Smart Card Reader 0
TPM
Import Certificate
Show Certificate
Export Certificate
Register Certificate
Create Certificate Request
Create self signed Certificate
lue
9696ae-b40e-4dea-a833-f2475ee18823
9696ae-b40e-4dea-a833-f2475ee18823

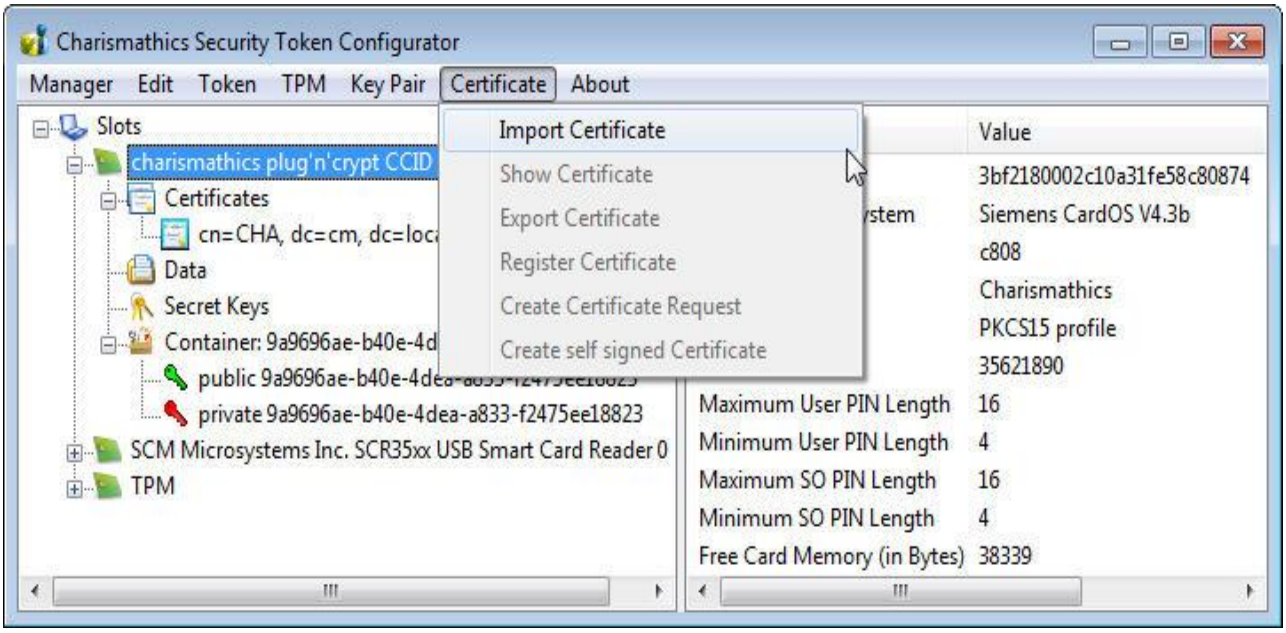
In order to generate the certificate request you enter the data into the corresponding fields. In case of a certificate request, you create a file to send it to the authority that should sign the certificate (e.g. Trust Center). Therefore, you store the request as a p10 file in a directory and follow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

3.5.2 Importing Certificates

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

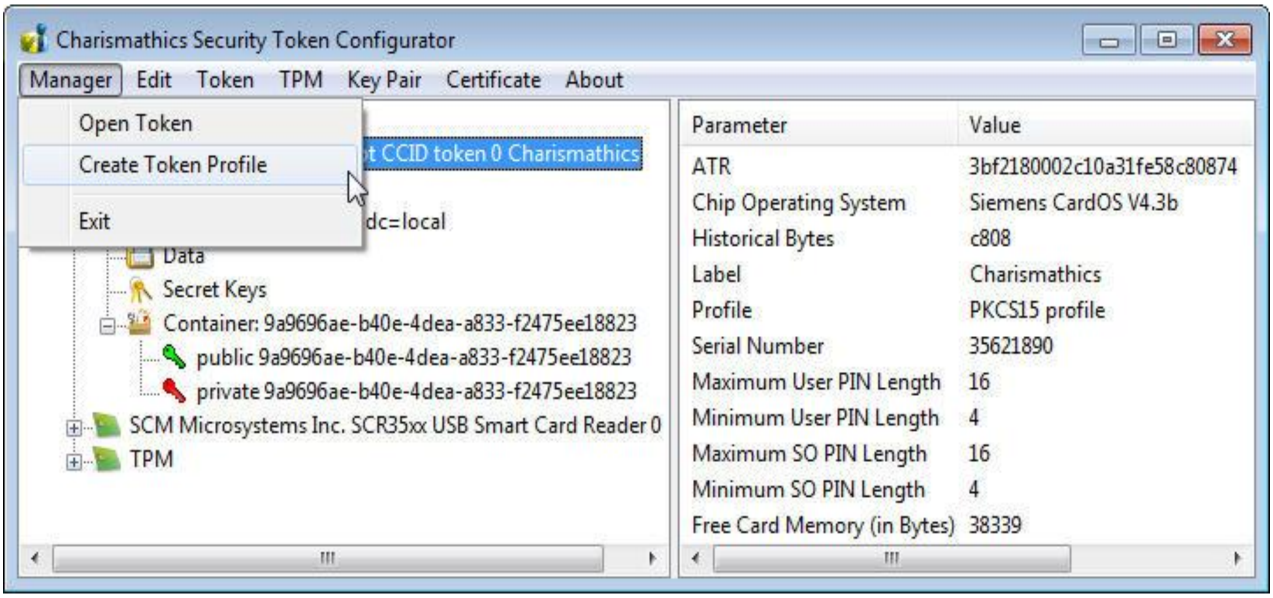


Slots
charismathics plug'n'crypt CCID
Certificates
cn=CHA, dc=cm, dc=loc
Data
Secret Keys
Container: 9a9696ae-b40e-4d
public 9a9696ae-b40e-4dea-a833-f2475ee18823
private 9a9696ae-b40e-4dea-a833-f2475ee18823
SCM Microsystems Inc. SCR35xx USB Smart Card Reader 0
TPM

	Value
	3bf2180002c10a31fe58c80874
ystem	Siemens CardOS V4.3b
	c808
	Charismathics
	PKCS15 profile
	35621890
Maximum User PIN Length	16
Minimum User PIN Length	4
Maximum SO PIN Length	16
Minimum SO PIN Length	4
Free Card Memory (in Bytes)	38339

3.6 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 set-up the corporate profile on this smart card. Click the menu "Manager"→"Create Token Profile".


Charismathics Security Token Configurator
Manager
Edit
Token
TPM
Key Pair
Certificate
About
Open Token
Create Token Profile
Exit
t CCID token 0 Charismathics
dc=local
Data
Secret Keys
Container: 9a9696ae-b40e-4dea-a833-f2475ee18823
public 9a9696ae-b40e-4dea-a833-f2475ee18823
private 9a9696ae-b40e-4dea-a833-f2475ee18823
SCM Microsystems Inc. SCR35xx USB Smart Card Reader 0
TPM

Parameter	Value
ATR	3bf2180002c10a31fe58c80874
Chip Operating System	Siemens CardOS V4.3b
Historical Bytes	c808
Label	Charismathics
Profile	PKCS15 profile
Serial Number	35621890
Maximum User PIN Length	16
Minimum User PIN Length	4
Maximum SO PIN Length	16
Minimum SO PIN Length	4
Free Card Memory (in Bytes)	38339

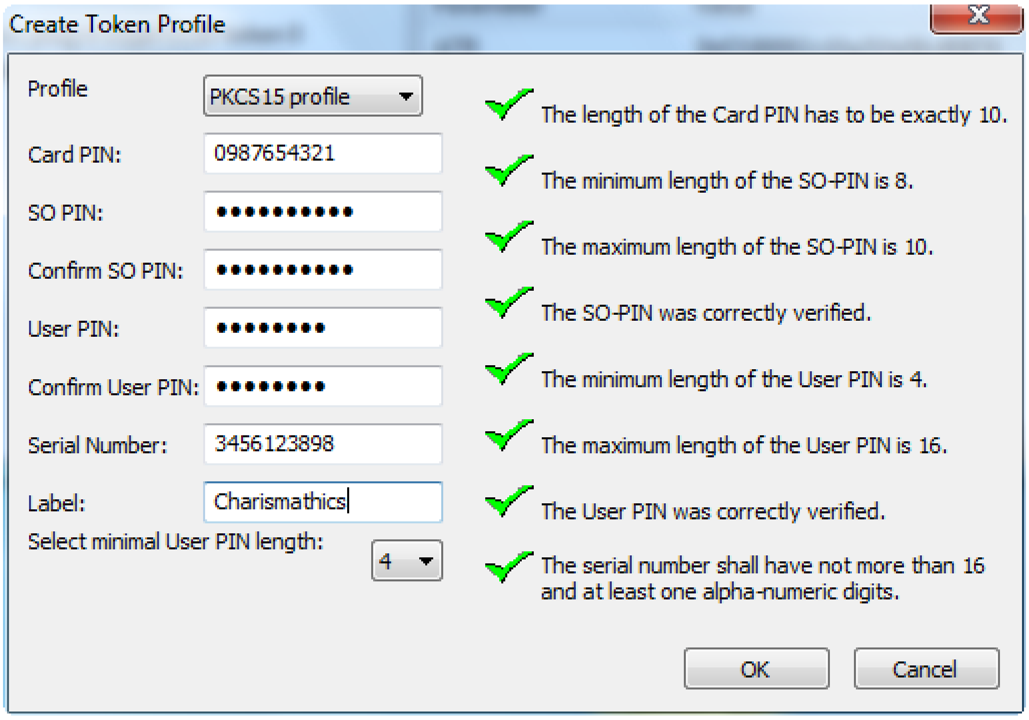
3.6.1 Smart Card with Profile

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.

3.6.2 Empty Smart Card

If the profile is set up (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. Using CSSI tool you can initialize the cards with six different profiles (Corporate, PKCS#15, CNS, FineID, IAS and PIV) depending upon the smartcards used. For AET profile, you cannot initialize the cards with this profile but CSSI middleware is backward compatible with cards that have been initialized with this profile. Meaning we can read these cards, access data, create data on them, but not initialize the card with this particular profile.



Create Token Profile

Profile: PKCS15 profile

Card PIN: 0987654321

SO PIN: ••••••••••

Confirm SO PIN: ••••••••••

User PIN: ••••••••

Confirm User PIN: ••••••••

Serial Number: 3456123898

Label: Charismathics

Select minimal User PIN length: 4

✓ The length of the Card PIN has to be exactly 10.

✓ The minimum length of the SO-PIN is 8.

✓ The maximum length of the SO-PIN is 10.

✓ The SO-PIN was correctly verified.

✓ The minimum length of the User PIN is 4.

✓ The maximum length of the User PIN is 16.

✓ The User PIN was correctly verified.

✓ The serial number shall have not more than 16 and at least one alpha-numeric digits.

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 with asterisks (*) in the input mask. The input must also be confirmed. Further explanations regarding the PINs can be found in section 4.2.

Note: PIV card is supported only with the special release, CSSI for PIV.

3.7 Preparing a Token (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 the keys and certificates on the smart card.

3.7.1 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".

3.7.2 Second Step: Creating Keys and Certificates (Personalization)

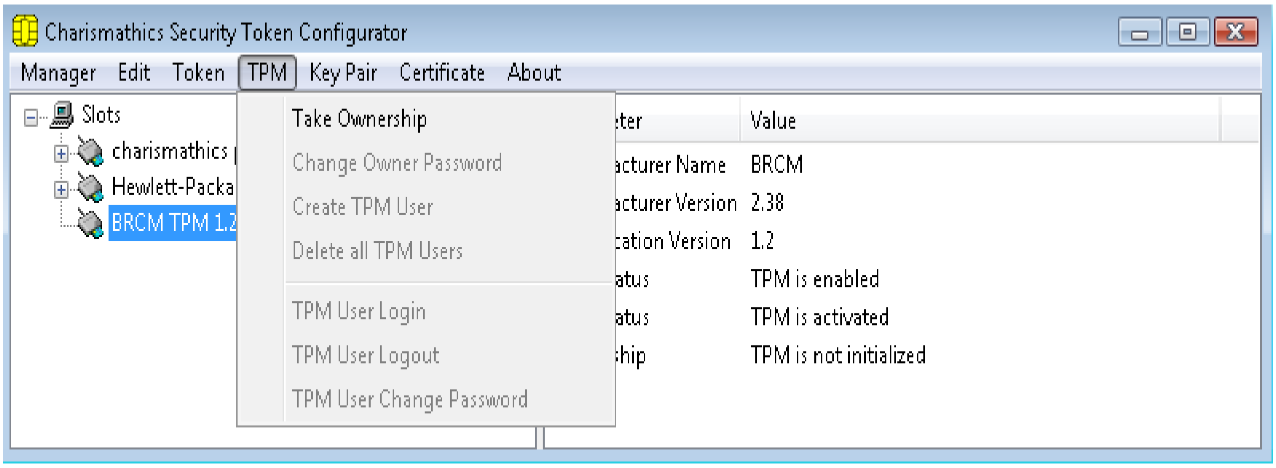
As a second step you must set up a user key and certificate on the smart card. You have the possibility to either generate keys and certificates or to import them. Refer to section 4.4 "Generating and Importing Keys" and section 4.5 "Generation and Import of Certificates".

3.8 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.

3.8.1 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 “Manager”→”Open Token”, ownership of the TPM can be taken.



ıter	Value
ıcturer Name	BRCM
ıcturer Version	2.38
ɾation Version	1.2
atus	TPM is enabled
atus	TPM is activated
;hip	TPM is not initialized

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.

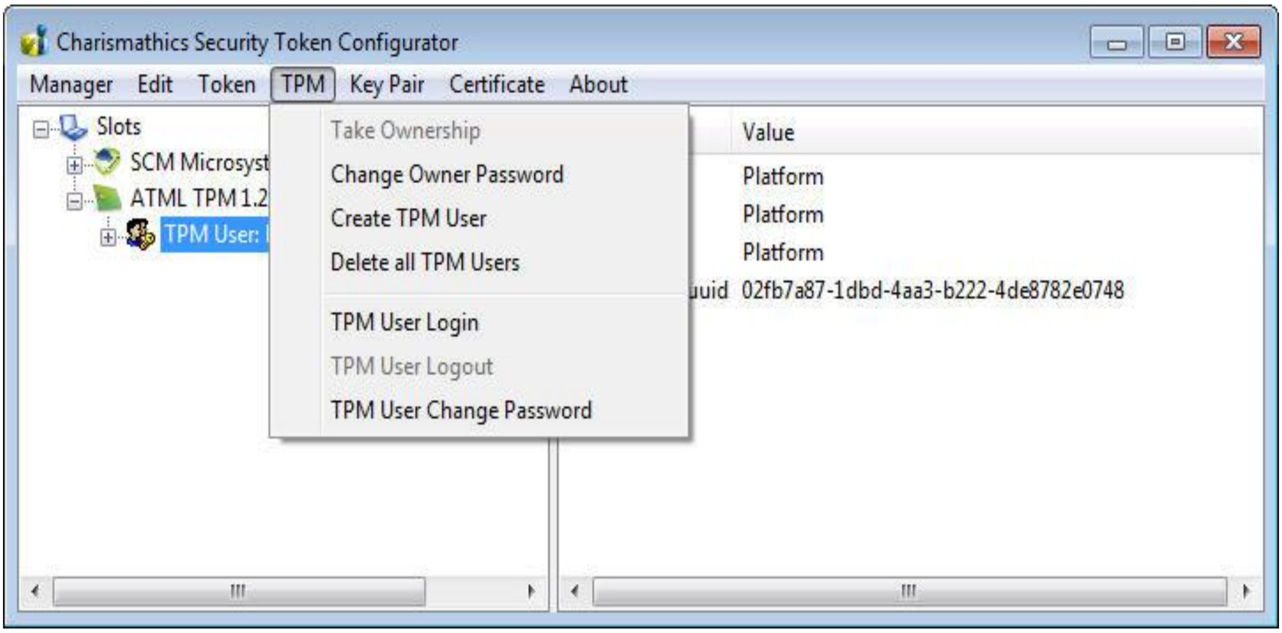
3.8.2 Changing the current TPM Owner Password

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.

3.8.3 Creating TPM User

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



	Value
	Platform
	Platform
	Platform
uuid	02fb7a87-1dbd-4aa3-b222-4de8782e0748

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

3.8.4 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.

3.8.5 Inspect TPM User private information

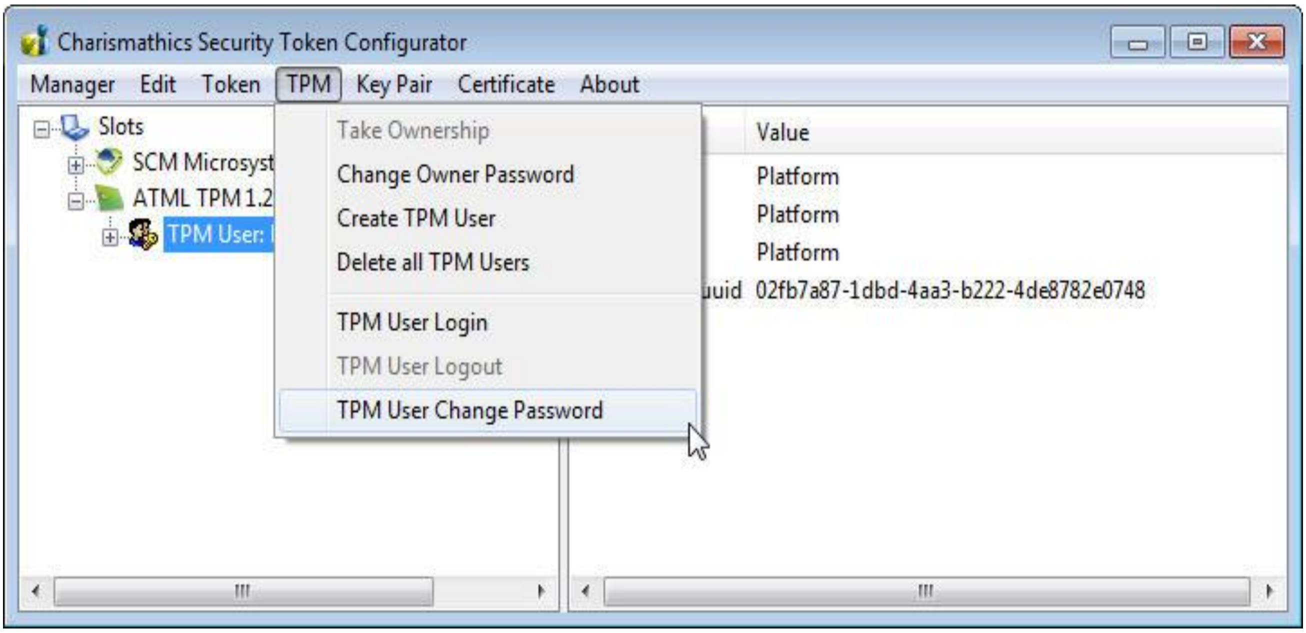
To view the information associated with a user, use "TPM"→"Login".

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.

3.8.6 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.

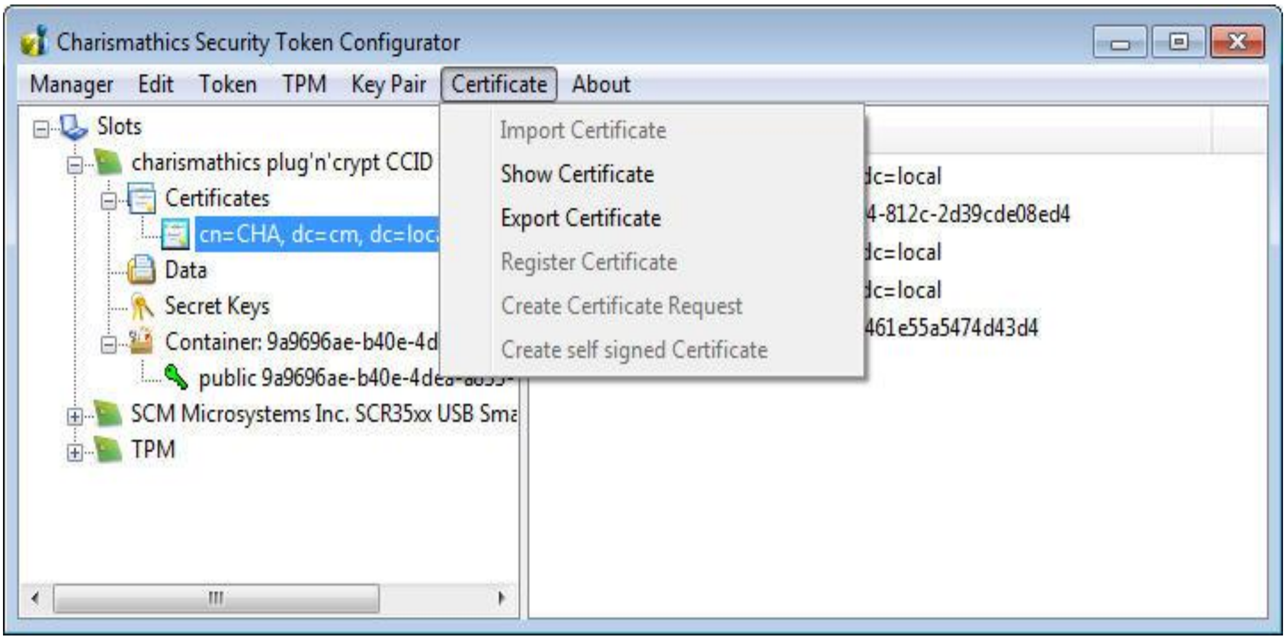
3.8.7 Importing a key pair from a PFX file

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.

3.9 Further Functions

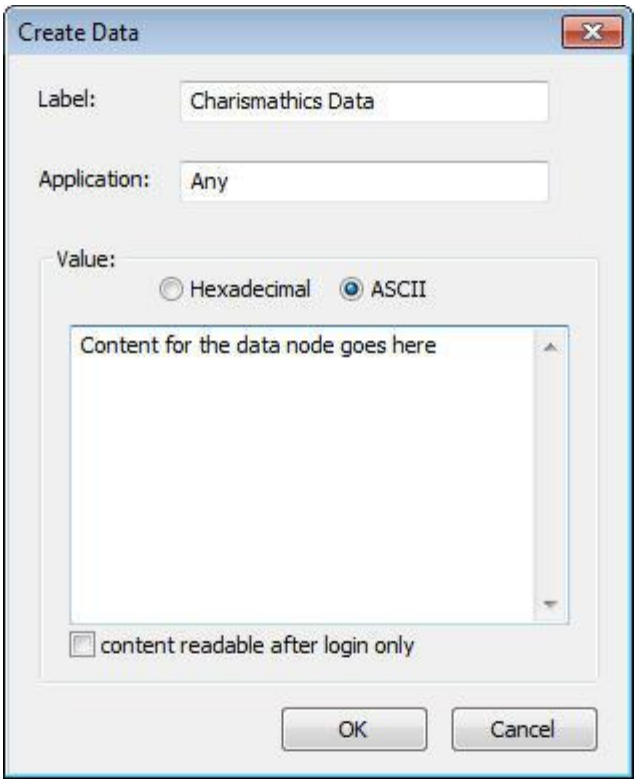
3.9.1 Directory "Certificates"

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.



3.9.2 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:



Create Data

Label: Charismathics Data

Application: Any

Value: ○ Hexadecimal ● ASCII

Content for the data node goes here

□ content readable after login only

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.

3.9.3 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.

3.9.4 Function "Delete all" and "Delete Object"

You can delete all objects, 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 choose the item "Delete Object".

3.9.5 Function "Set Default Container"

The function "Set Default Container" of the menu "Edit" is only relevant to you 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 chose a Container as Default Container, it will show in bold face in the interface of the Security Token Configurator tool.

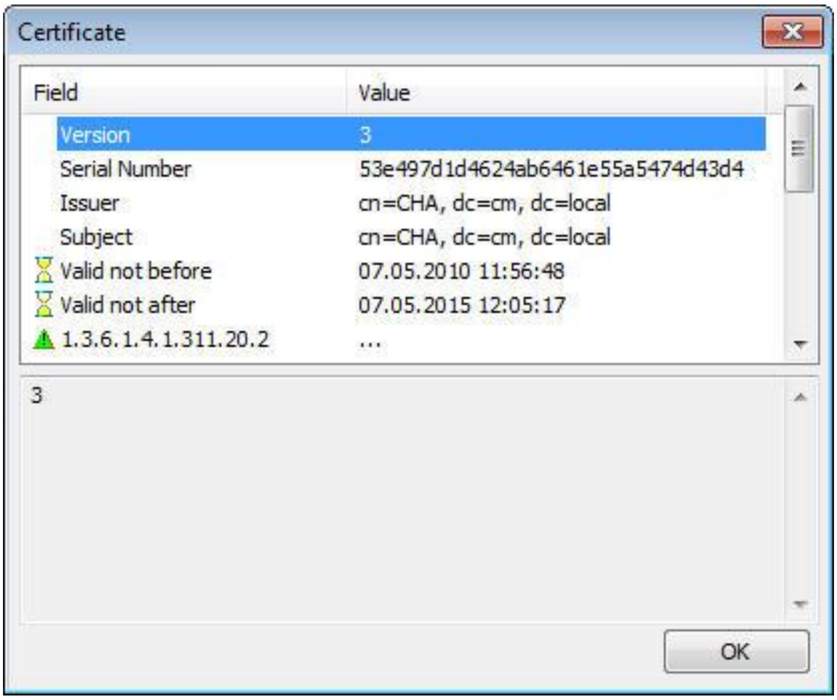
3.9.6 Function "Change Container Label"

The function "Change Container Label" of the menu "Edit" allows the user to change the friendly name of the container. Please be aware that once a certificate was registered in the Microsoft Certificate Store, you need to register the certificate again after renaming the container. Otherwise the certificate cannot be used for any operation via CSP.

3.9.7 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:



Field	Value
Version	3
Serial Number	53e497d1d4624ab6461e55a5474d43d4
Issuer	cn=CHA, dc=cm, dc=local
Subject	cn=CHA, dc=cm, dc=local
Valid not before	07.05.2010 11:56:48
Valid not after	07.05.2015 12:05:17
1.3.6.1.4.1.311.20.2	...

3

3.9.8 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".

3.9.9 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).

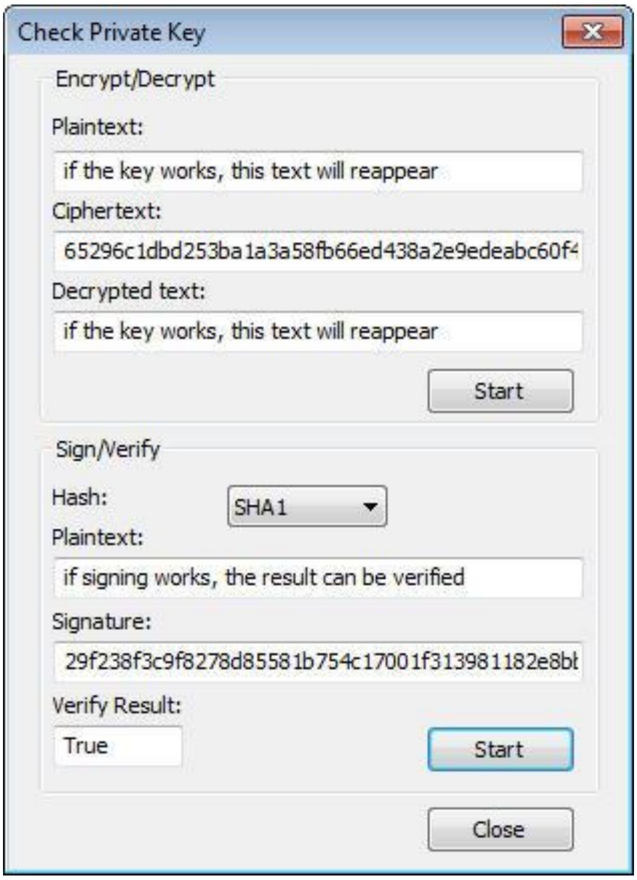
You can also access this function from the context menu: highlight the certificate that you want to register, right click and choose the item "Register Certificate".

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

3.9.10 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.



Plaintext: if the key works, this text will reappear

Ciphertext: 65296c1dbd253ba1a3a58fb66ed438a2e9edeabc60f4

Decrypted text: if the key works, this text will reappear

Hash: SHA1

Plaintext: if signing works, the result can be verified

Signature: 29f238f3c9f8278d85581b754c17001f313981182e8bt

Verify Result: True

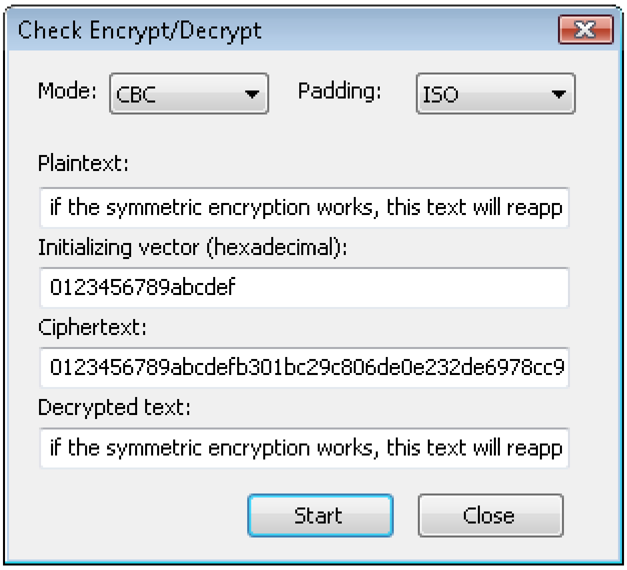
To test the signing key you can choose the hash algorithm. If the Verify Result is true, the signing key works all right.

3.9.11 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 choose 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 Code Book (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. If the Decrypted text is the same as the Plaintext, the encryption key works all right.



Check Encrypt/Decrypt

Mode: CBC

Padding: ISO

Plaintext: if the symmetric encryption works, this text will reapp

Initializing vector (hexadecimal): 0123456789abcdef

Ciphertext: 0123456789abcdefb301bc29c806de0e232de6978cc9

Decrypted text: if the symmetric encryption works, this text will reapp

3.9.12 SHA2 and ECC support

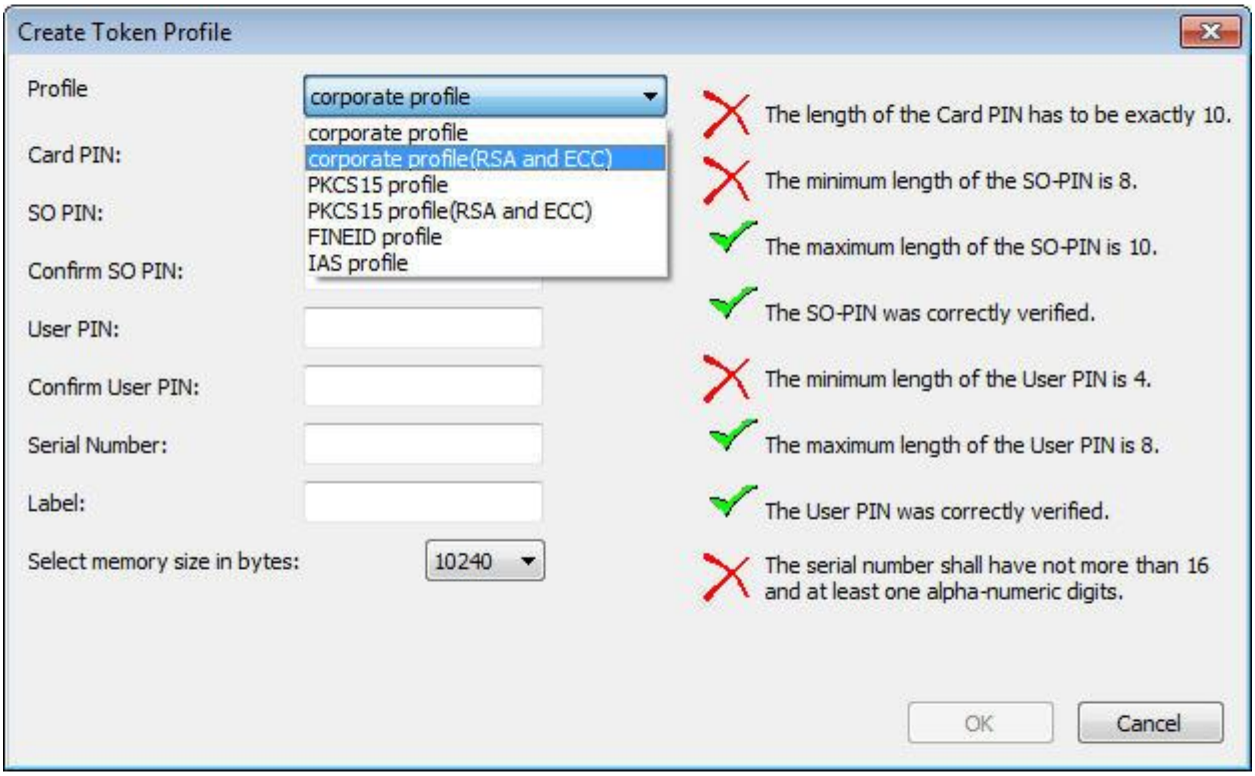
SHA2 support:

Charismathics middleware comes with KSP provider to support SHA2 under windows vista and above. SHA256, SHA384 and SHA 512 is supported with Charismathics RSA key storage provider – implementation of crypto Next Generation.

Note: When enrolling the certificate using browser like Internet explorer for signing the certificate request with SHA256, SHA 384 or SHA 512, select “Charismathics Smart Security Extended CSP” as your CSP.

ECC support:

In order to support ECC keys with CSSI smart card has to be initialized with Corporate profile (RSA and ECC) or PKCS15 profile (RSA and ECC), see the screenshot below on how to initialize the card with corportare profile (RSA and ECC) or PKCS15 (RSA and ECC). For supporting ECC, make sure that your card operating system support it. It is possible to support RSA and ECC at the same time.



Create Token Profile

Profile: corporate profile

Card PIN:

SO PIN:

Confirm SO PIN:

User PIN:

Confirm User PIN:

Serial Number:

Label:

Select memory size in bytes: 10240

✗ The length of the Card PIN has to be exactly 10.

✗ The minimum length of the SO-PIN is 8.

✓ The maximum length of the SO-PIN is 10.

✓ The SO-PIN was correctly verified.

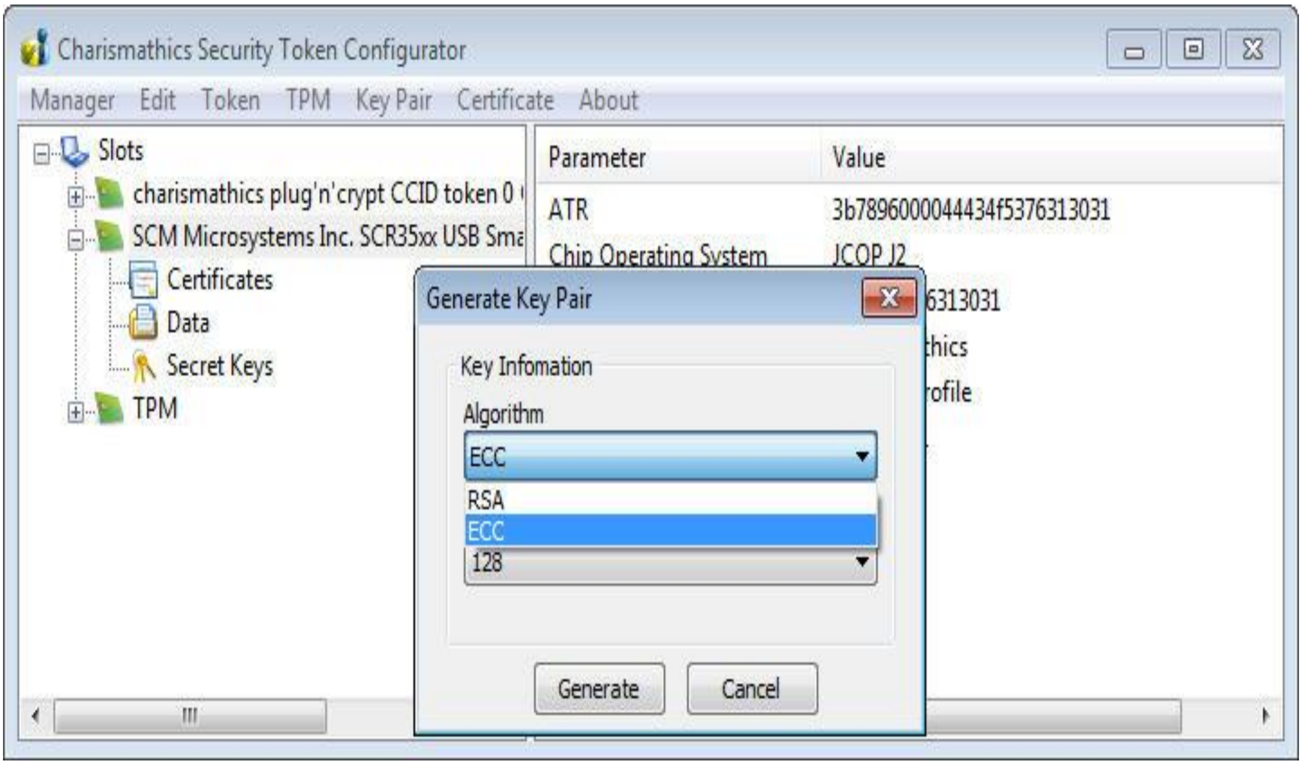
✗ The minimum length of the User PIN is 4.

✓ The maximum length of the User PIN is 8.

✓ The User PIN was correctly verified.

✗ The serial number shall have not more than 16 and at least one alpha-numeric digits.

To generate a ECC key with CSTC tool, select the item "Generate Key pair" in the menu and select ECC from Algorithm list.



Charismathics Security Token Configurator

Parameter	Value
ATR	3b7896000044434f5376313031
Chip Operating System	JCOP J2

Generate Key Pair

Key Infomation

Algorithm: ECC

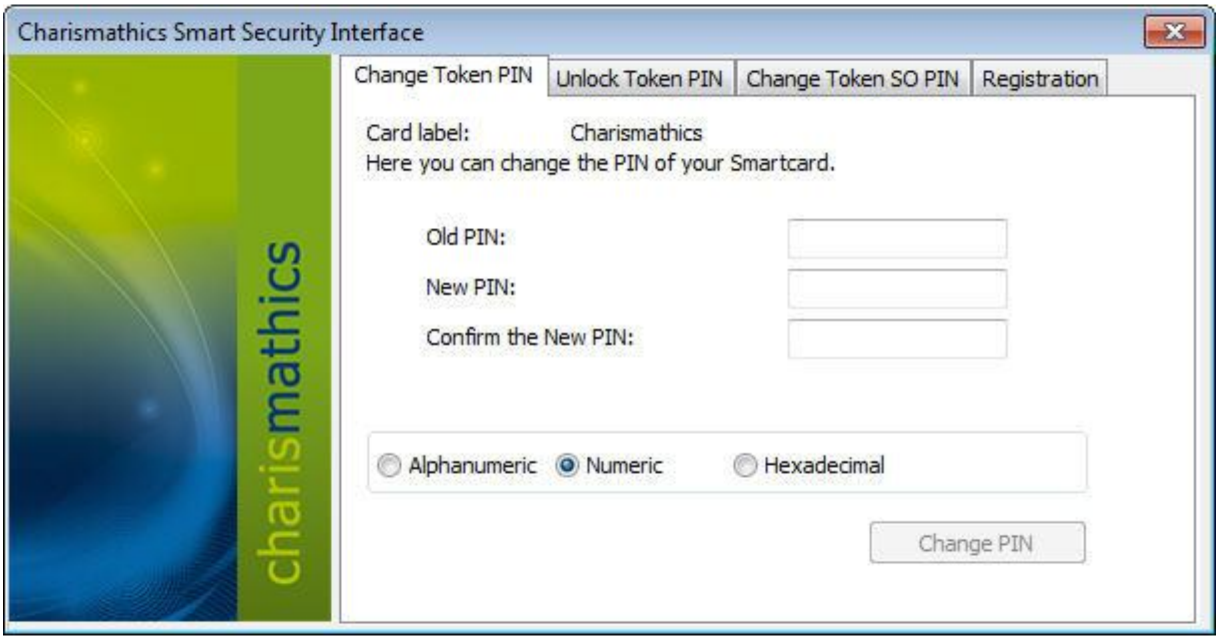
128

4 User Tool: CSSI 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".

4.1 Change PIN



Card label: Charismathics

Here you can change the PIN of your Smartcard.

Old PIN:

New PIN:

Confirm the New PIN:

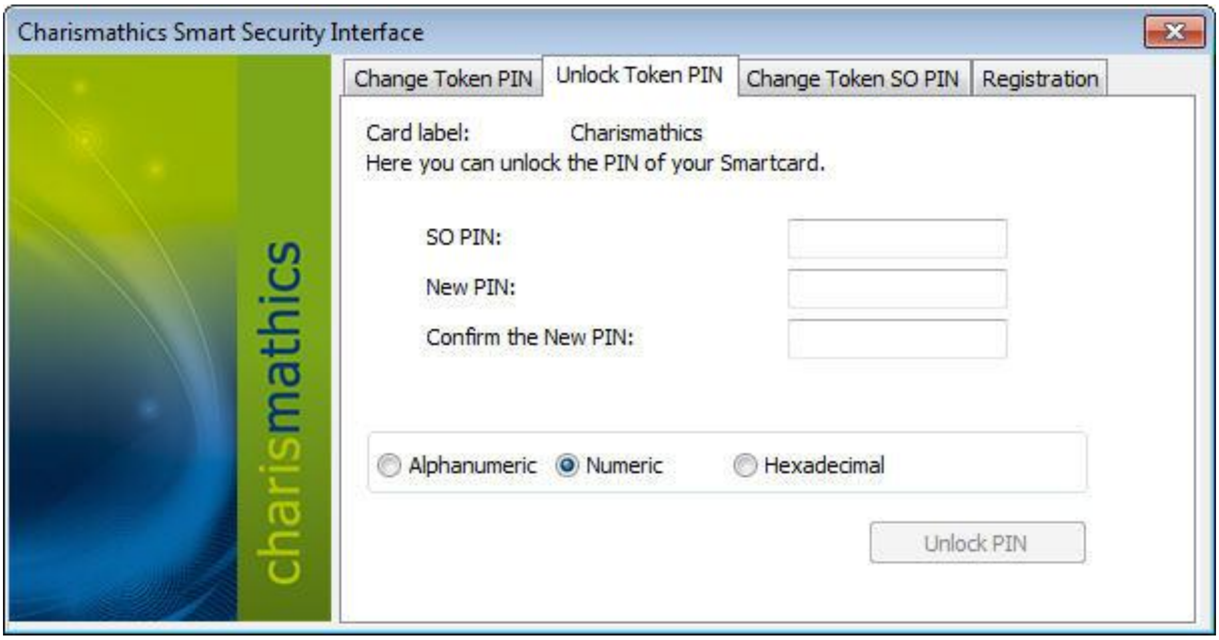
○ Alphanumeric ● Numeric ○ Hexadecimal

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 birthdays or simple sequences of numbers like 1234 or 1111.**

4.2 Unlock PIN



Charismathics Smart Security Interface

Change Token PIN | Unlock Token PIN | Change Token SO PIN | Registration

Card label: Charismathics

Here you can unlock the PIN of your Smartcard.

SO PIN:

New PIN:

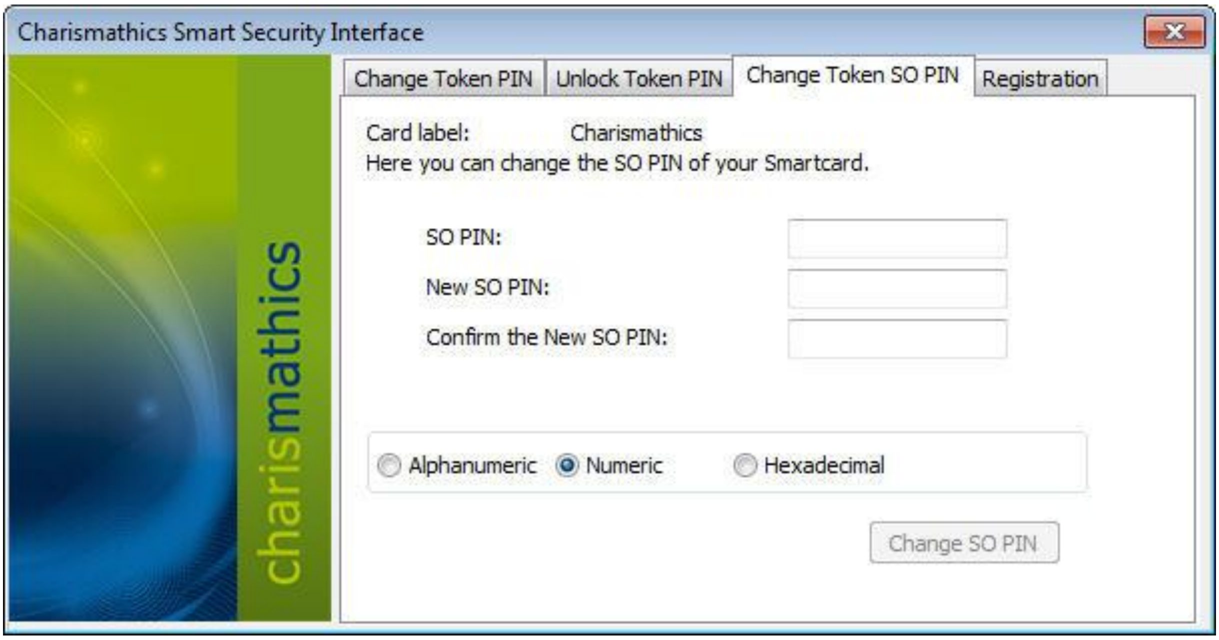
Confirm the New PIN:

○ Alphanumeric ● Numeric ○ Hexadecimal

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.

4.3 Change Token SO PIN



Charismathics Smart Security Interface

Change Token PIN | Unlock Token PIN | Change Token SO PIN | Registration

Card label: Charismathics

Here you can change the SO PIN of your Smartcard.

SO PIN:

New SO PIN:

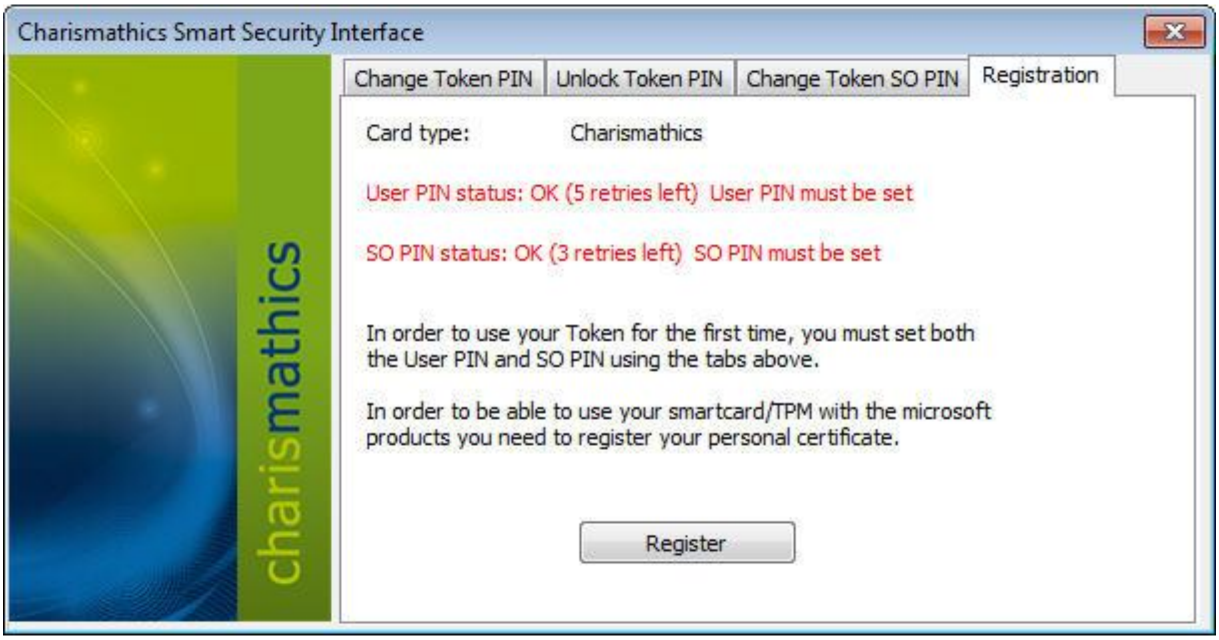
Confirm the New SO PIN:

○ Alphanumeric ● Numeric ○ Hexadecimal

To change the Token SO PIN, enter the SO PIN followed by the new SO PIN, which must be entered a second time as confirmation. The minimum and maximum length of the SO PIN dependends on the card OS.

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

4.4 Registration



Card type: Charismathics

User PIN status: OK (5 retries left) User PIN must be set

SO PIN status: OK (3 retries left) SO PIN must be set

In order to use your Token for the first time, you must set both the User PIN and SO PIN using the tabs above.

In order to be able to use your smartcard/TPM with the microsoft products you need to register your personal certificate.

Registration page display the number of retry left for User PIN and SO PIN.

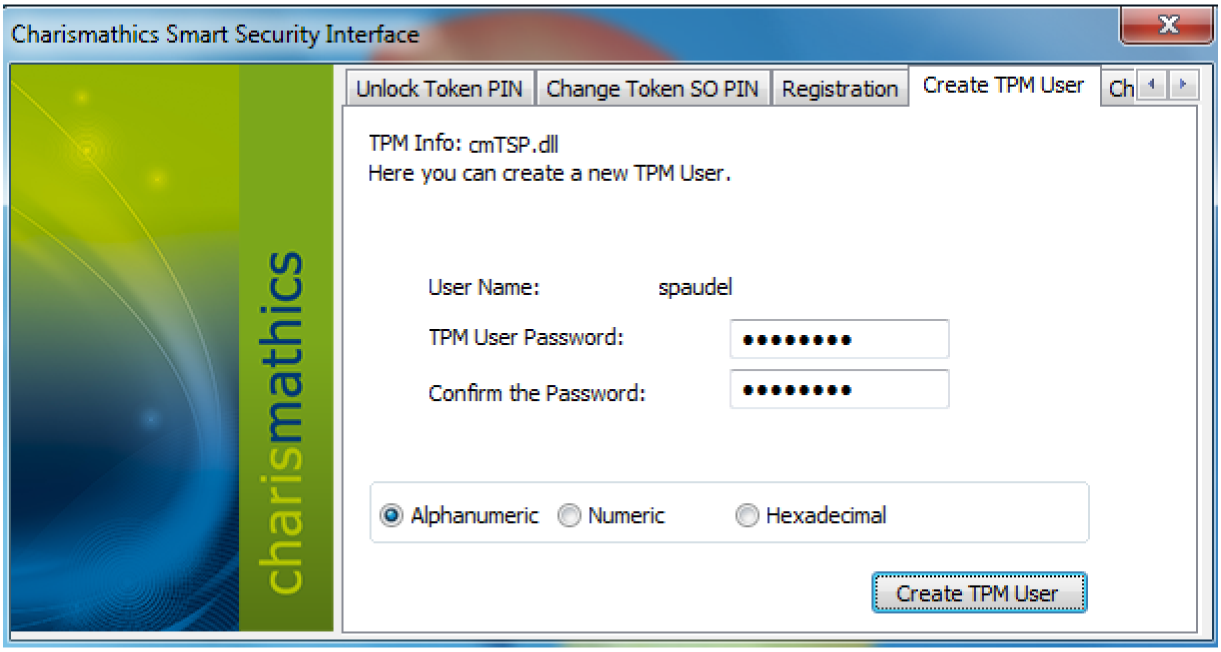
Your smart card may contain multiple certificates and keys. These certificates must be registered once, so that applications can use these. Certificates propagation is done automatically once the card is inserted into the smart card reader. If in case automatic certificate propagation does not work, simply clicking on Register button as shown in the screen shot above will do the job.

Important: The registration need to be done only once for each card.

4.5 Create TPM User (Optional)

All TPM operations have a number of prerequisites:

- TPM hardware has to be present
- TSS module has to be installed
- TPM Ownership must have been taken, e.g. with CSSI – Security token configurator tool.



TPM Info: cmTSP.dll
Here you can create a new TPM User.

User Name: spaudel

TPM User Password: ●●●●●●●●●

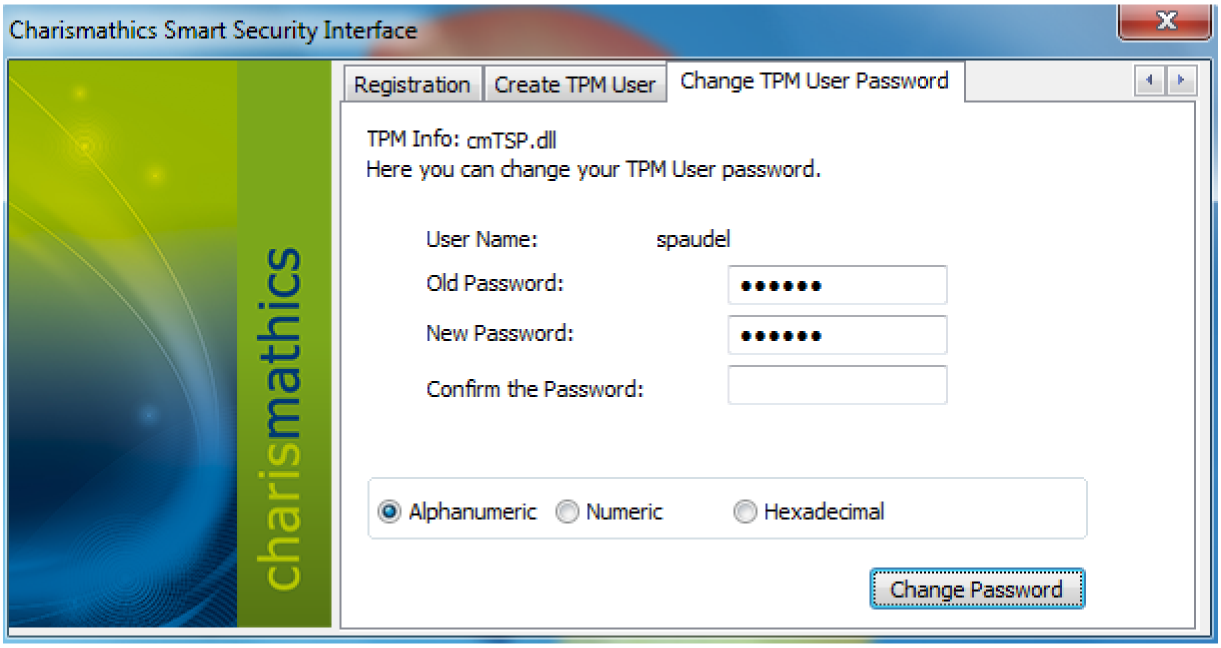
Confirm the Password: ●●●●●●●●●

● Alphanumeric ○ Numeric ○ Hexadecimal

Creating a TPM User only works on systems where a TPM User for the current user does not yet exist

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

4.6 Change TPM Password (Optional)



TPM Info: cmTSP.dll
Here you can change your TPM User password.

User Name: spaudel

Old Password: ●●●●●●

New Password: ●●●●●●

Confirm the Password:

● Alphanumeric ○ Numeric ○ Hexadecimal

Changing a TPM User only works on systems where a TPM User for the current user has been created.

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

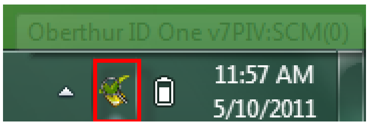
5 Register Tool

This tool is installed only for Windows XP. For Vista and above, certificate propagation is done automatically using the system services.

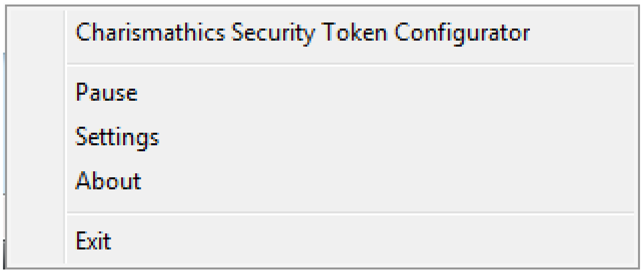
Under windows XP, to make certificates accessible for Microsoft Windows applications like Internet Explorer or Outlook Express, register tool is required to propagate the certificates from your smart card in the windows certificate store. The settings for this registration are configured in this Register 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 Charismathics Security Token Configurator or the Charismathics Smart Security Interface Utility to pause the Register Tool, to configure Settings, to read information or to terminate the Register Tool, which is now explained.

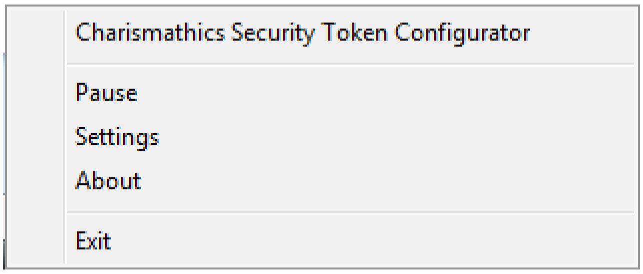


5.1 Start CSSI security token configurator and Start CSSI Utility

The context menu of the system tray icon offers the choice of starting either the user edition (Charismathics Smart Security Interface Utility) and the Charismathics Security Token Configurator. Refer to chapters 3 and chapter 4 regarding these tools.

5.2 Pause/ Continue

If automatic registration of the certificates on the token is not desired, you can pause the Register Tool. Select Pause from the context menu of the system tray icon to temporarily stop automatic registration. Once paused, you can select Continue from the same menu.



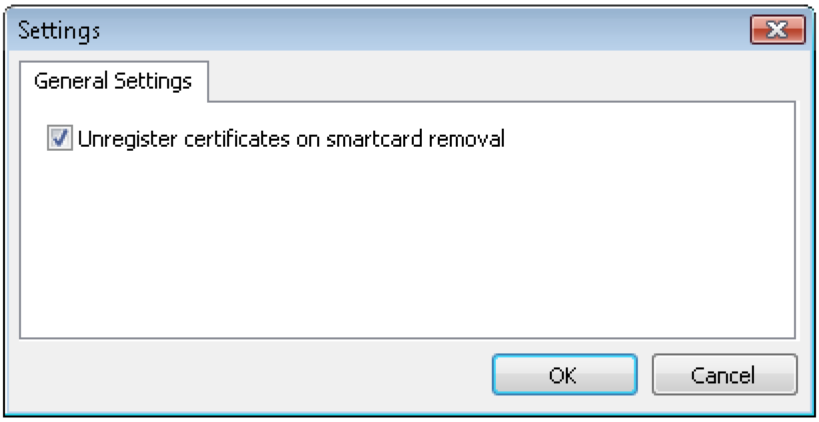
In addition to adding the certificates to the user store, they can also be added to the machine store. Set the registry value at:

[HKEY_LOCAL_MACHINE\SOFTWARE\charismathics\smart security interface]
To store certificates in the machine store, set "CSP_RegisterMachineStore"=hex:01.

Revert the value to hex:00 to disable storing the certificates in the machine store.

5.3 Settings

The default functionality of the Register Tool is to register certificates automatically as soon as a token is inserted. Once the token is removed the certificates can be unregistered automatically. If this is desired, you can configure this using "Settings”.



☑ Unregister certificates on smartcard removal

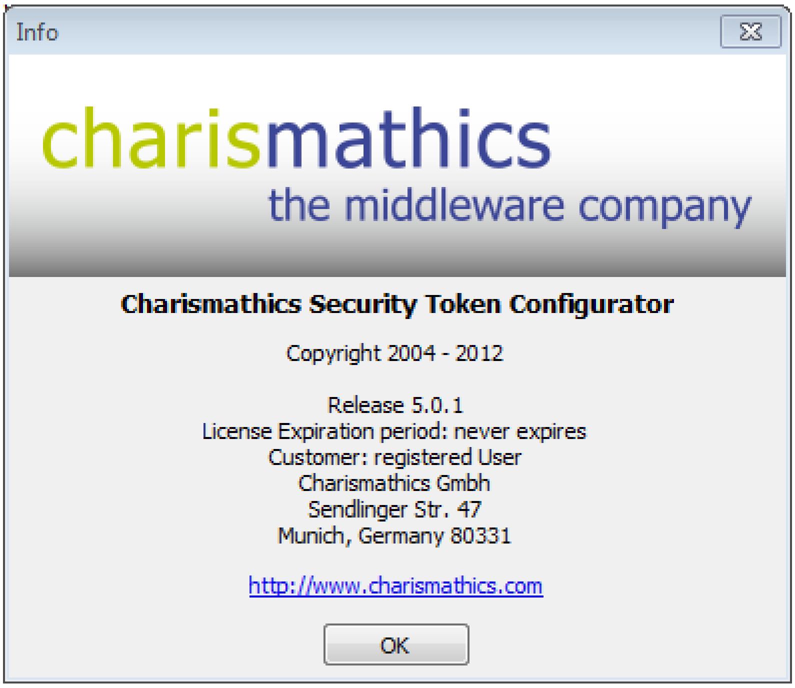
An alternate way of accessing this option is modifying the registry entry in

[HKEY_LOCAL_MACHINE\SOFTWARE\charismathics\smart security interface]
To deactivate automatic unregistering, use: "CSP_DeactivateUnregister"=hex:00.

To activate automatic unregistering, use: "CSP_DeactivateUnregister"=hex:01.

5.4 About

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



Charismathics Security Token Configurator

Copyright 2004 - 2012

Release 5.0.1
License Expiration period: never expires
Customer: registered User
Charismathics Gmbh
Sendlinger Str. 47
Munich, Germany 80331

http://www.charismathics.com

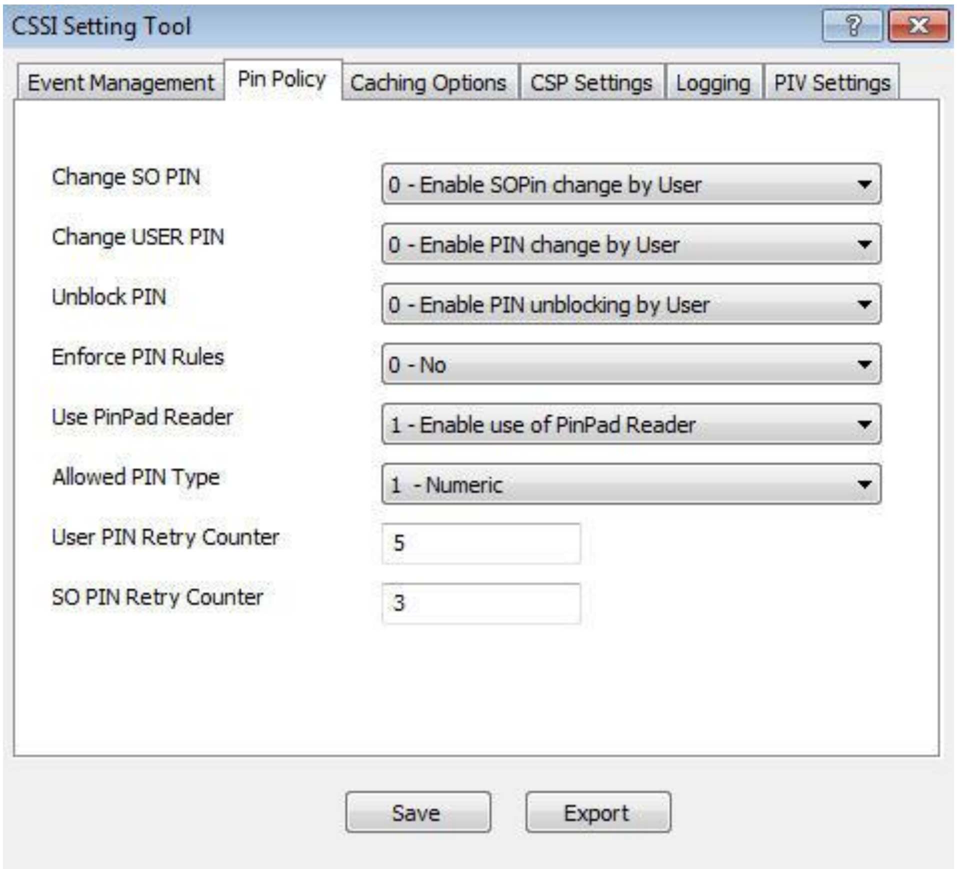
5.5 Exit

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

6 Charismathics Setting Tool

The Charismathics Setting Tool can be used to change the default registry entries.

This tool is installed under \Program Files\Charismathics\Smart Security Interface\CSSISetting.exe.



Change SO PIN: 0 - Enable SOPin change by User

Change USER PIN: 0 - Enable PIN change by User

Unblock PIN: 0 - Enable PIN unblocking by User

Enforce PIN Rules: 0 - No

Use PinPad Reader: 1 - Enable use of PinPad Reader

Allowed PIN Type: 1 - Numeric

User PIN Retry Counter: 5

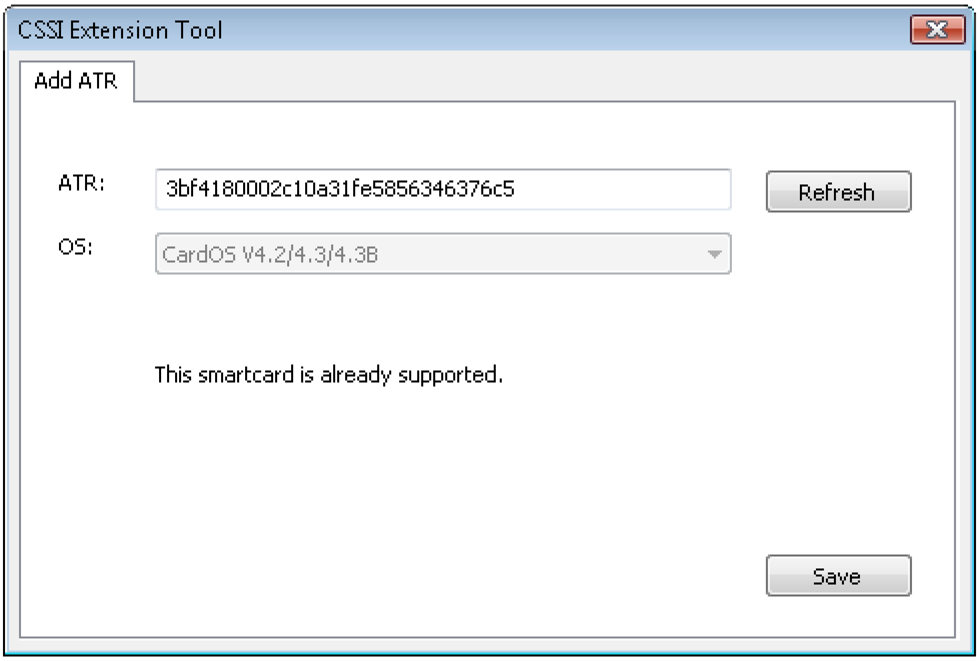
SO PIN Retry Counter: 3

This tool is installed as a part of Charismathics Security Token Configurator tool when running the setup package is custom mode. In order to open this tool from Menu option in Security token configurator tool, you need to open Security Token Configurator as an administrator and go to Menu – Manager – CSSI Setting Tool.

Note: This tool can be opened only with Administrator right.

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 cannot be guaranteed.



ATR: 3bf4180002c10a31fe5856346376c5

OS: CardOS V4.2/4.3/4.3B

This smartcard is already supported.

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 cannot be changed while the card is in the reader.
   b. If no OS is associated with the ATR, select the correct OS or a 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 Cryptographic Service Providers of CSSI

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** (in short cmCSP) has been added.

Using cmCSP enables a number of programs and functions that come with a Windows Operating System, like Outlook Express, Internet Explorer, network login and VPN-login to use smart-cards, USB tokens and TPM. They will be explained in the following.

Charismathics Smart Security Interface includes also a minidriver for any CardOS V4.x smart card.
The minidriver corresponds to the BaseCSP specification V6. For more information regarding the description of the minidriver requirements, please visit Microsoft website
http://www.microsoft.com/whdc/device/input/smartcard/sc-minidriver.mspx.

Smart card vendors can write card mini drivers to present a consistent interface to their smart card type to the Microsoft® Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface. These card mini drivers plug in to Windows® operating system code.

Note: Here, you will not find a description how to configure your Microsoft environment for the use of smart cards or USB tokens. 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 Server.

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

8.1 General Proceedings

In order to use a Microsoft product in connection with the CSP for the first time on a certain computer the certificates on the token must have been registered. Please refer to chapter 5 “ ” and 3.9.9 “Function "Register Certificate"” if you want to learn more about how to register your certificate.

The token must contain keys and certificates. There are several different possibilities to obtain these.

- Generating a key pair and corresponding certificate directly on the smart card with the functions of standard browsers, like Internet Explorer or Netscape. Thereby the token is accessed using the modules of **Charismathics Smart Security Interface**, i.e. correspondingly by cmCSP or cmP11.
  Import of existing keys and certificates on the smart card which were generated by other CAs or trust centers.
- Generation of key pair and corresponding self-signed certificate directly on the smart card by the Charismathics Security Token Configurator tool. Please note that the use of self signed certificates makes sense only in environments without 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.

The programs must be configured to work with your keys and certificates. Some programs require root-certificates to be installed in certain directories, others require registering the certificate.

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

8.2 Smart Card Login to a Windows 2003/2008 Domain

The following is a brief outline of the steps involved in setting up smart card or USB token login.

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

8.3 SSL- Authentication with Smart Card over the Internet Explorer

To use certificates stored on hardware tokens for SSL connections, the certificate must have been registered with the Windows Certificate Store. This can be done using either the CSTC or user edition of CSSI and the Register Tool (refer to chapter 6 "Register Tool" or in section 4.8 "Register Certificate").

8.4 Outlook Express with Electronic Signature & Encryption

Electronic signing and encryption requires the certificates to be registered the same as for SSL connections. Once this is done, the desired certificate for signing and encryption can be chosen from "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 for instance uses the red "signet" symbol in the right corner of the email window

In order for Outlook Express to automatically recognize the right key and corresponding certificate, the certificate should lie in the address book, i.e. the certificate should be imported into the "Digital IDs". 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 the certificate must be registered with the Charismathics Security Token Configurator tool (refer to chapter 6 "Register Tool" and 3.9.9 Function "Register Certificate"").

9 PKCS#11-Module of CSSI

The use of software that supports PKCS#11 is enabled by the **Charismathics Smart Security Interface-PKCS#11** (abbreviated cmP11)**.** The matter of applications and functionalities with tokens like network login, SSL, email security with Netscape and other producers are explained briefly**.**

Note: There is no description on how to configure each environment to use cmP11. If your application is not covered here, please consult the corresponding documentation that comes with the application.

Important: The PKCS#11 module is a DLL by the name "cmP11.dll" and is installed in the system directory. Usually this is C:\Windows\system32.

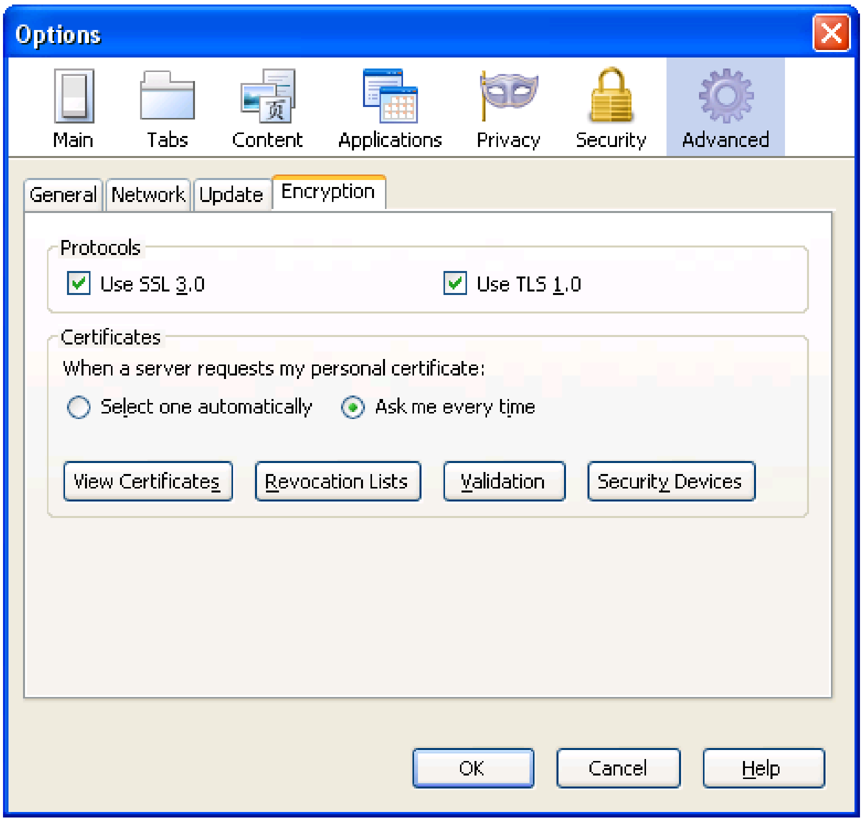
Remark: Despite strict measures for the quality of PKCS#11 modules by the different manufacturers, charismathics gmbh cannot guarantee the compatibility with each PKCS#11 Module of a third party manufacturer.

9.1 Smart Card Login to a Novell eDirectory (formerly NDS)

This requires a very good understanding of the administration of Novell servers. To enable smart card or USB token login to an eDirectory you explicitly need the product NMAS and the corresponding Universal Smartcard Login Method.

9.2 SSL-Authenticatin with Smart Card Over Mozilla Firefox

Launch Firefox - Go to Tools – Options – Advanced – Encryption – Security Devices – Load.



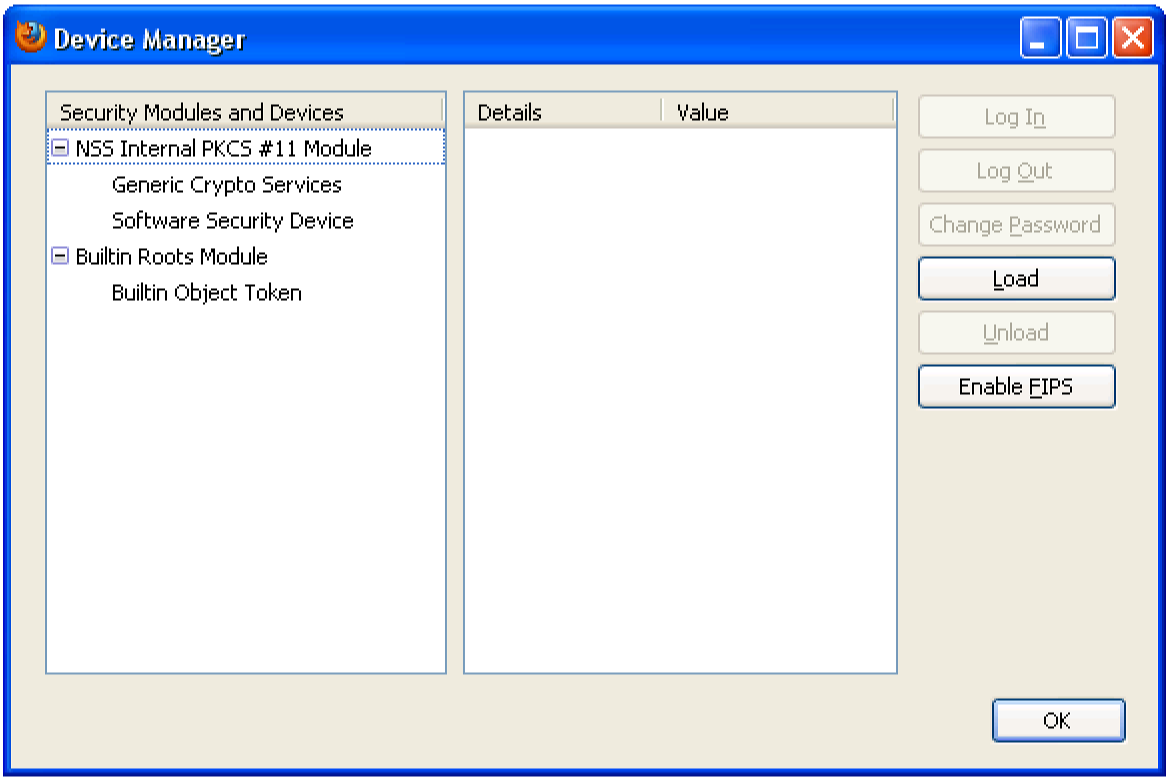
Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

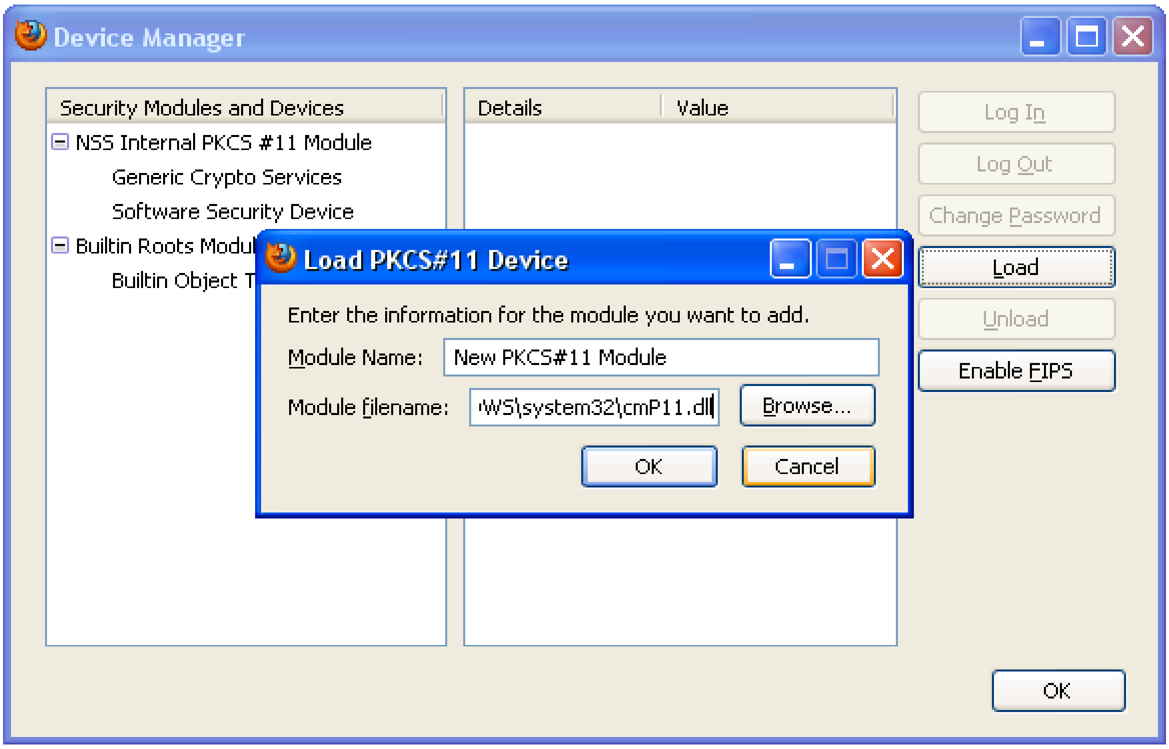
Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time



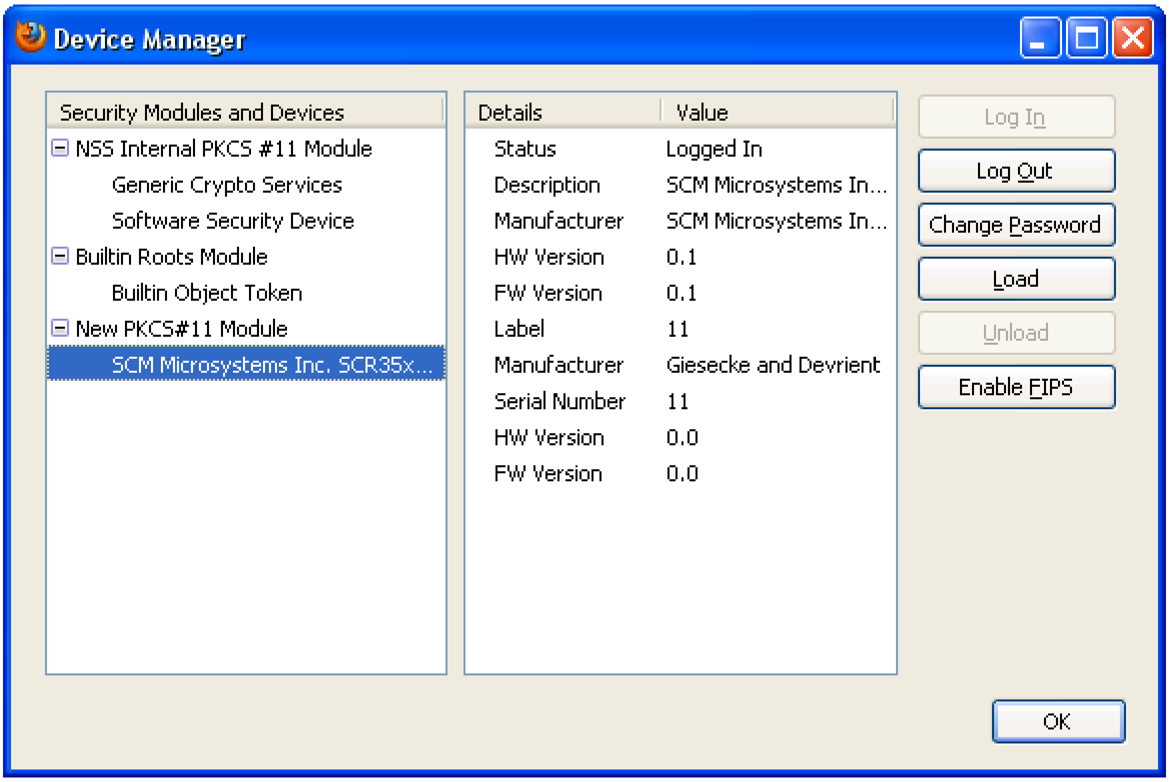
Click on Browse and locate cmP11.dll (cmP1164.dll for 64bit) and click on Open. Click on OK.



Enter the information for the module you want to add.

Module Name: New PKCS#11 Module

Module filename: ·WS\system32\cmP11.dll



Details	Value
Status	Logged In
Description	SCM Microsystems In...
Manufacturer	SCM Microsystems In...
HW Version	0.1
FW Version	0.1
Label	11
Manufacturer	Giesecke and Devrient
Serial Number	11
HW Version	0.0
FW Version	0.0

10 References

[PKCS#5] http://www.rsa.com/rsalabs/node.asp?id=2124

[PKCS#11] http://www.rsa.com/rsalabs/node.asp?id=2124

[MS_CA] HOW TO: Configure a Certificate Authority to Issue Smart Card Certificates in Windows http://www.petri.co.il/install_windows_server_2003_ca.htm

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

11 Information / Export Restrictions

Charismathics GmbH
47 Sendlinger St
80331 Munich
Germany

Manual Revision: November 20, 2012

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.