Charismathics Smart Security Interface ©

User Manual V 5.0 for LINUX

charismathics

Contents

1 Introduction

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

CSSI for Linux provides modules that are needed in order to integrate different smart cards and USB tokens into your applications. The functionality ranges from administration of the card to modules supporting the operating system to use token.

The following file structures (profiles) are supported:

- Charismathics corporate profile
- PKCS#15 profile
- FINEID profile
- PIV Profile
- IAS ECC Profile
- CNS Profile
- AET Profile
- IAS ECC Profile

CSSI for Linux – User Edition is comprised of the following modules:

- **SCARDUTILITY – User tool**

Information on how to use this tool is described in Chapter 4 Smart Security Interface Utility.

- **libcmP11.so – PKCS11 Library for Linux**

Information on how to use this library and configuring its supported applications is explained in Chapter 5 Configuration of Applications supported by libcmP11.so.

CSTC – Charismathics Security Token Configurator for Linux is not included in CSSI User edition tool and has to be purchased separately. It is comprised of the following modules:

- **SCMANAGER – CSTC tool**

Information on how to use this tool is described in Chapter 3 Administration Tool: Charismathics Security Token Configurator.

CSSI for Linux enables you to use additional applications and services that use this standard interface. In particular the following applications can be augmented by CSSI:

Smartcard login to Linux

SSL – Authentication by smartcard (Mozilla Firefox)

Email security with cards using Thunderbird

Adobe Acrobat

VPN

2 Supported Hardware

2.1 Supported Smart Cards

CSSI for Linux is tested with the following smart cards:

- 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
- 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.

CSSI PIV for Mac is tested with the following PIV / CAC cards:

- 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

2.2 Supported Smartcard 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 in Linux has been tested with the following card readers:

- Omnikey Cardman 3621 USB
- Omnikey Cardman 3821 USB
- SCM SCR 3310 USB
- SCM SCR 3311 USB
- SCM SCR 532 serial/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.**

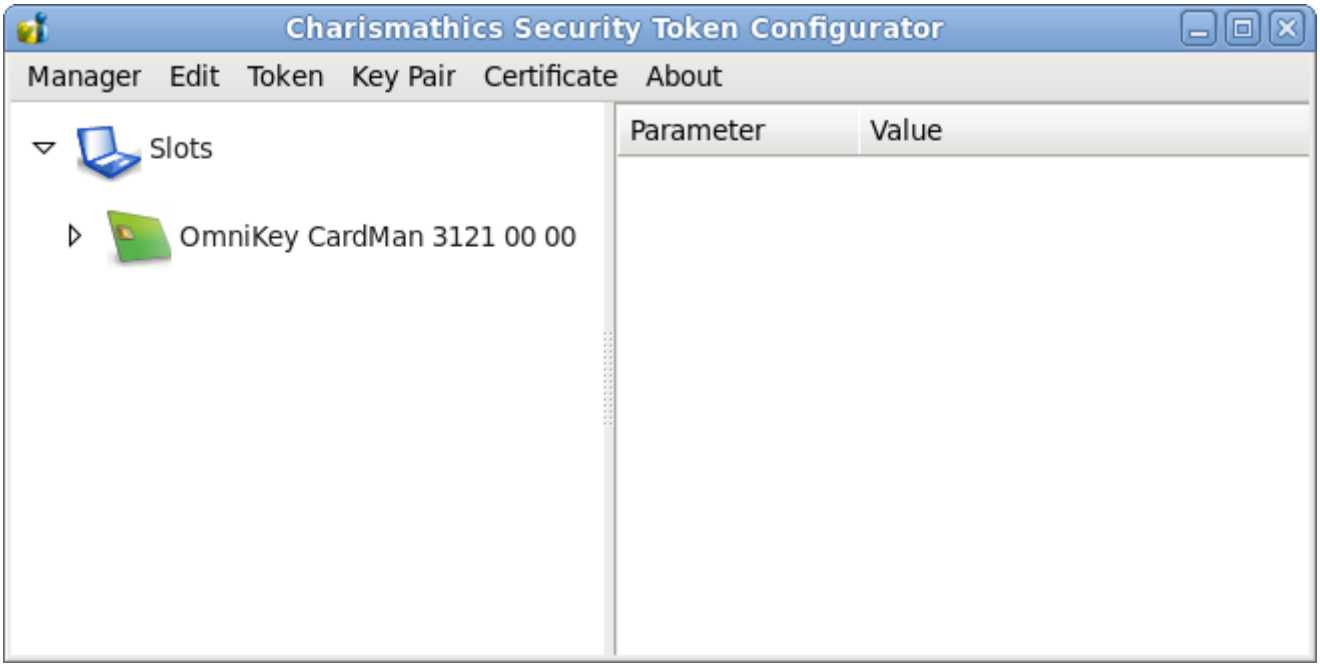
3 Administration Tool: CSTC

CSTC offers functions to manage smart card content: initialize smart cards, manage PINs, generate and manage keys and certificates.

Note: After changing the contents of the smartcard, you need to remove and reinsert the smart card to see the changes in other applications. This also applies when you perform Create Profile, Generate Key and Imports functions.

3.1 User Interface

After opening the CSTC tool you will see the interface you see below.

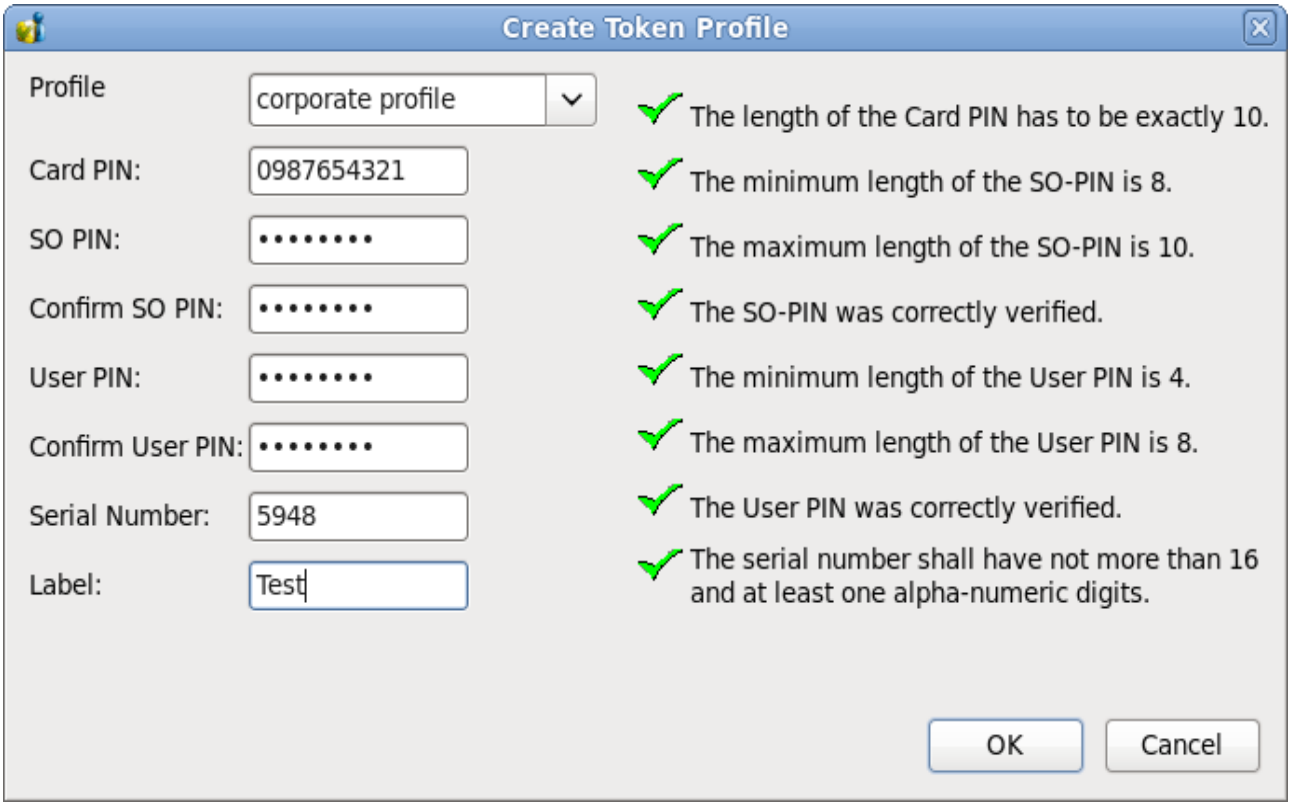


The left panel displays the list of smart card readers which are connected to the system. Hardware smart card readers and virtual USB token readers are displayed in the same window. Once a token has been inserted, the hierarchy is extended. Selecting an item in the hierarchy view displays its properties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

3.1.1 Token Configurator Menu

- "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 arrow-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.



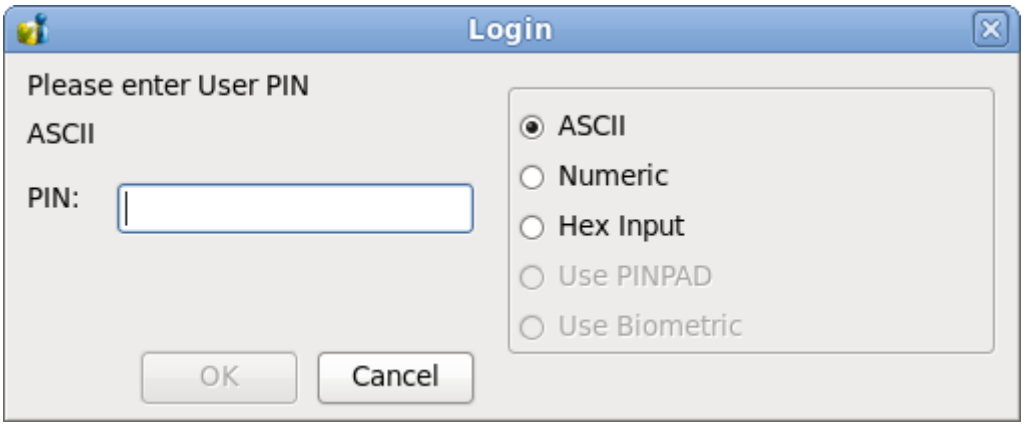
3.1.2 Edit menu/ Context menu

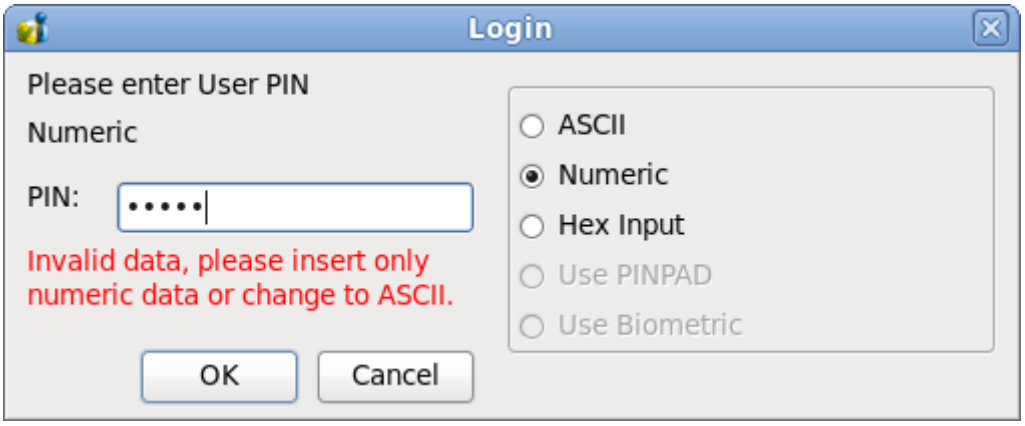
The content and availability of the "Edit" menu changes according to the item selected in the main hierarchy view. Most functions of the "Edit" menu are also accessible by right-clicking an item in the hierarchy.

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.





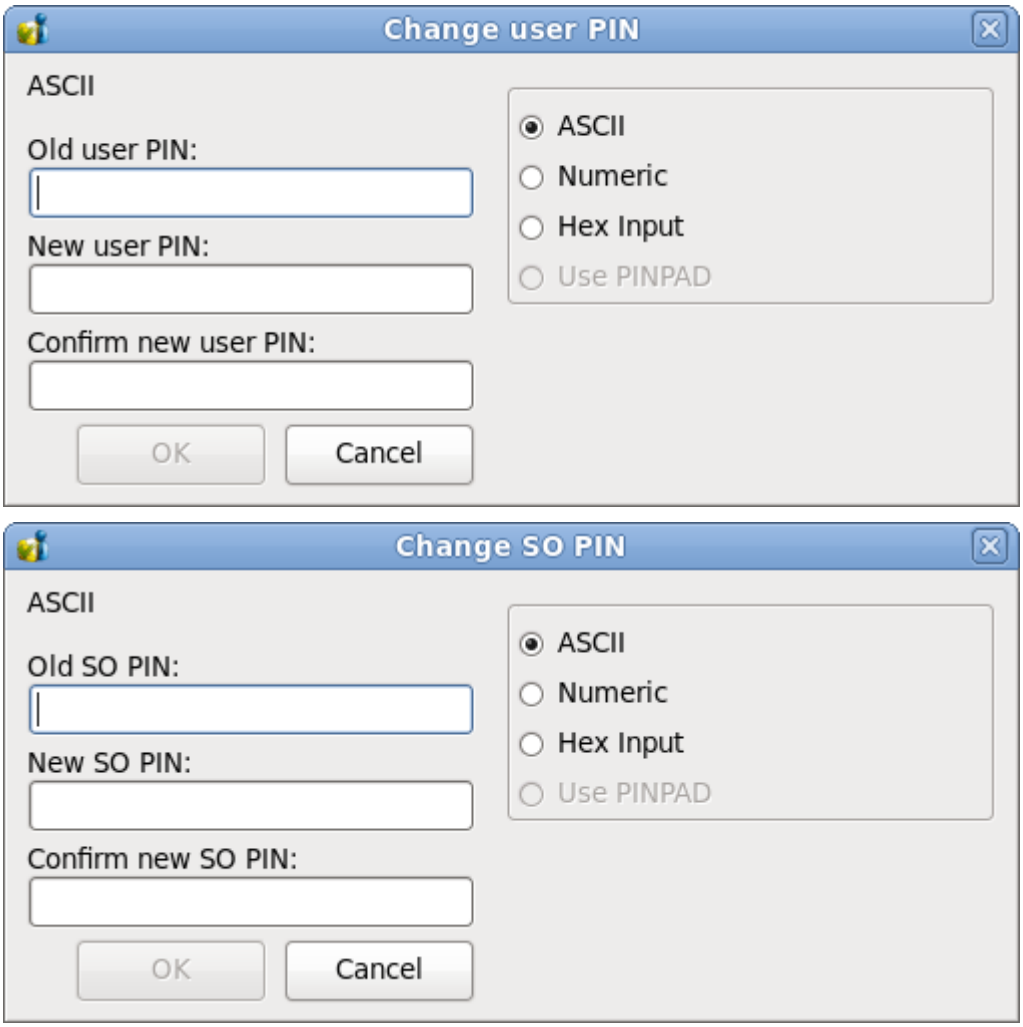
The hardware configuration and user settings determine the initial PIN entry method. Supported entry methods are:

- **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.

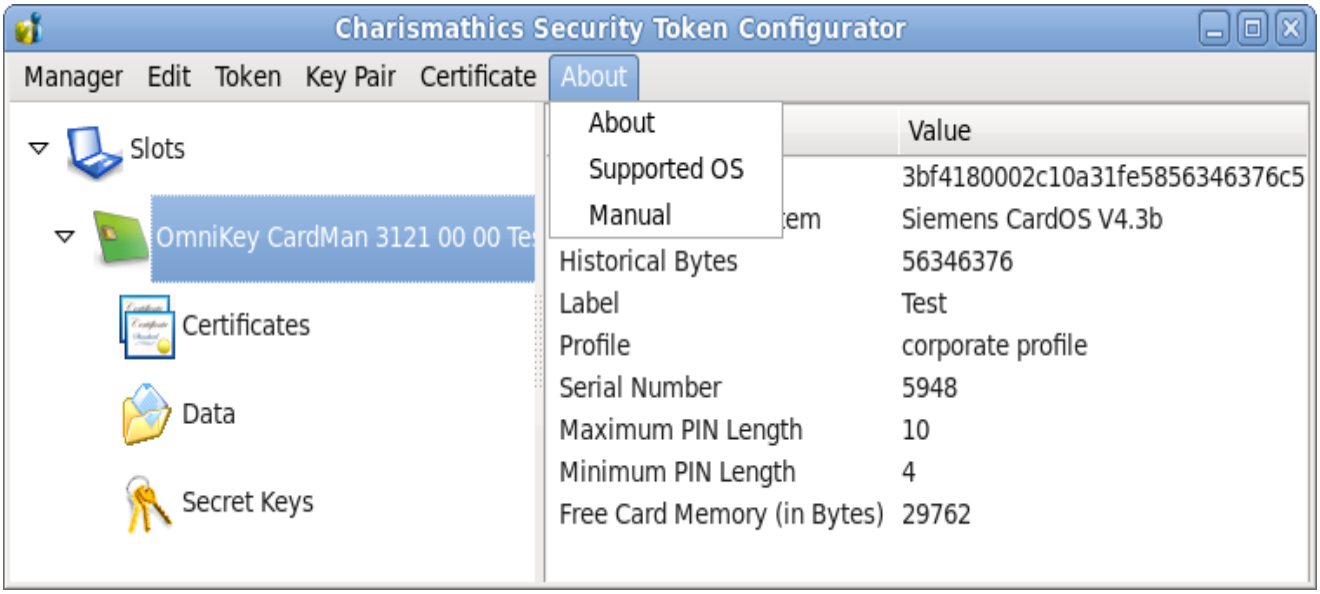
- "Logout": This item works analogous to the "Login" option.

- “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 Info Menu

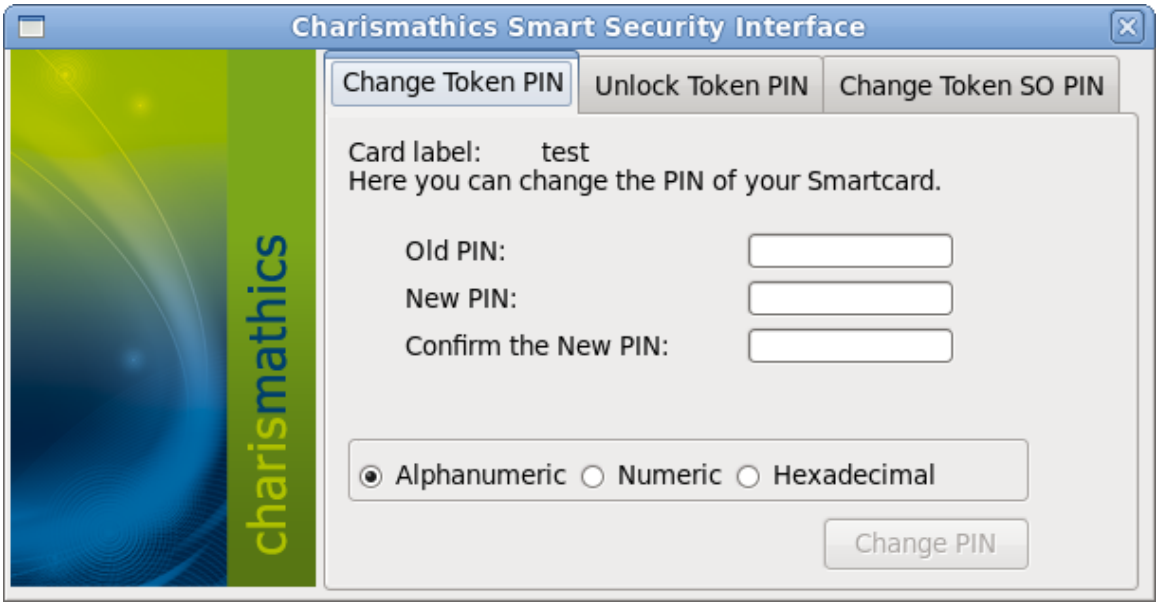


- "About": Displays general version information about the CSTC edition.
- "Supported OS": Displays the list of smart card operating systems supported by CSSI. This list includes only the predefined associations. Additional associations can be created with the CSSI Extension Tool.
- "Manual": This manual.

4 User Tool: CSSI Utility

This tool exposes all relevant functions if you acquired **Charismathics Smart Security Interface** in the user edition. Insert your smart card in the reader and open **Charismathics Smart Security Interface Utility.**

4.1 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.

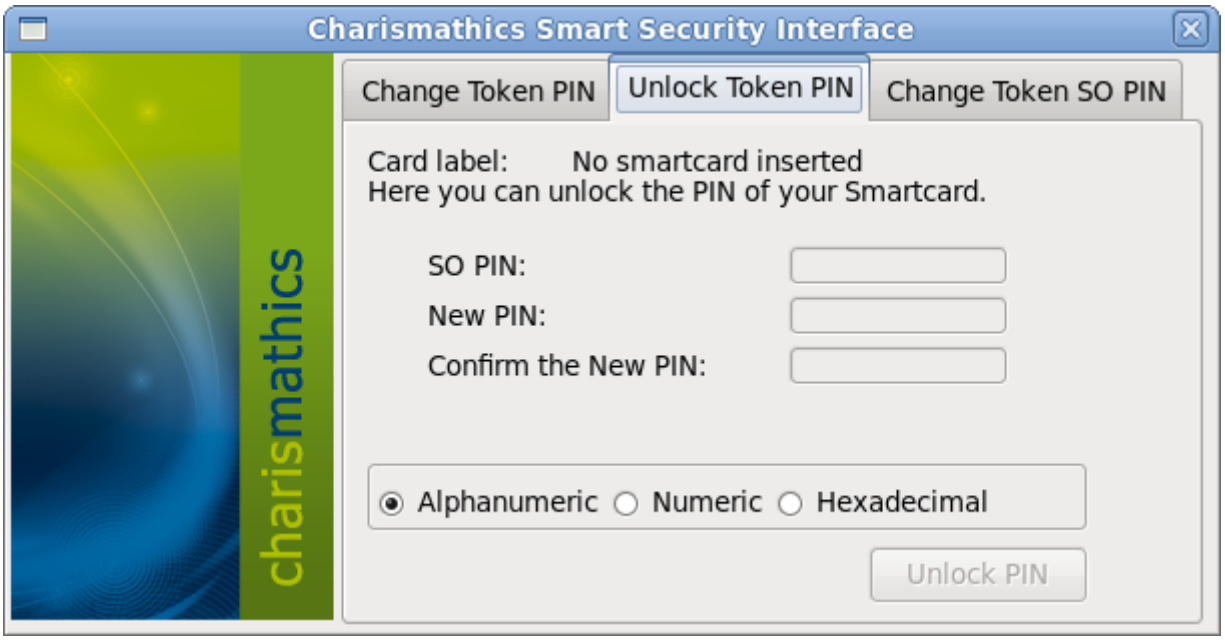
Click on the button "Change PIN", and you receive a window with the confirmation.

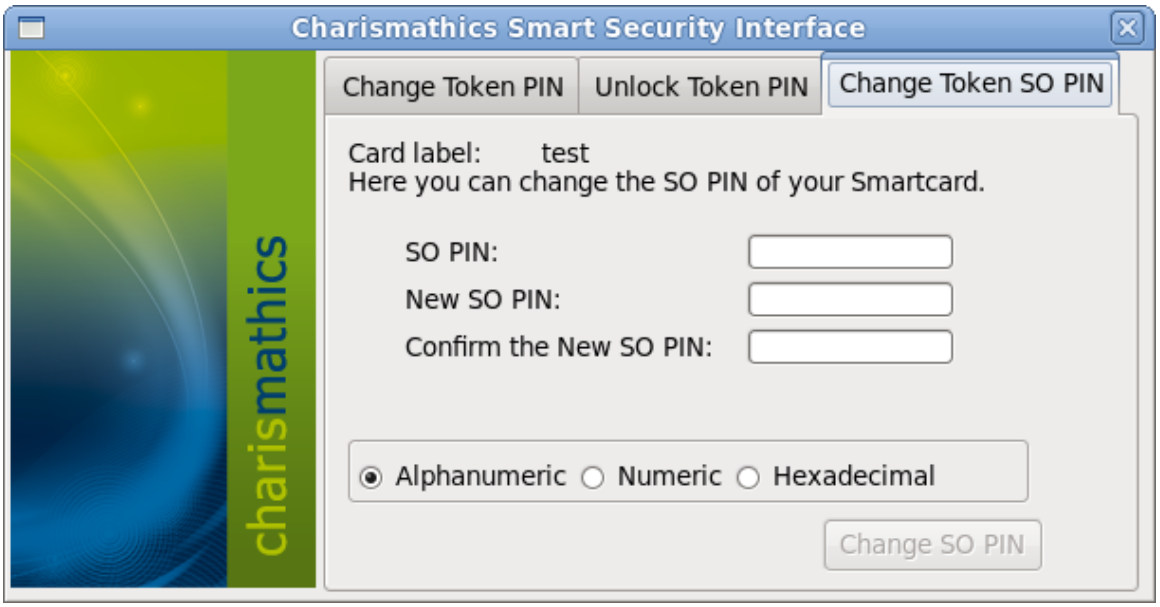
IMPORTANT: After three consecutive wrong inputs the User PIN will be locked. Please choose a PIN, which you can remember well, but which cannot be easily guessed. Avoid birthdays or simple sequences of numbers like 1234 or 1111.

4.2 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.


Charismathics Smart Security Interface
charismathics
Change Token PIN
Unlock Token PIN
Change Token SO PIN
Card label: No smartcard inserted
Here you can unlock the PIN of your Smartcard.
SO PIN:
New PIN:
Confirm the New PIN:
Alphanumeric
Numeric
Hexadecimal
Unlock PIN


Charismathics Smart Security Interface
charismathics
Change Token PIN
Unlock Token PIN
Change Token SO PIN
Card label: test
Here you can change the SO PIN of your Smartcard.
SO PIN:
New SO PIN:
Confirm the New SO PIN:
Alphanumeric
Numeric
Hexadecimal
Change SO PIN

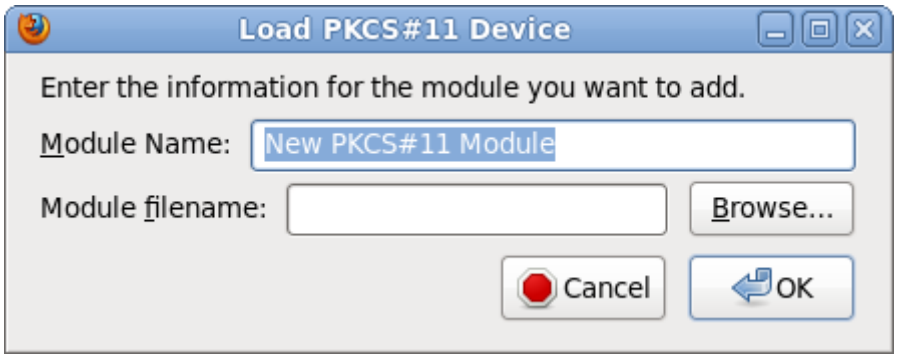
5 Configuration for support of PKCS#11

5.1 Configuring Firefox

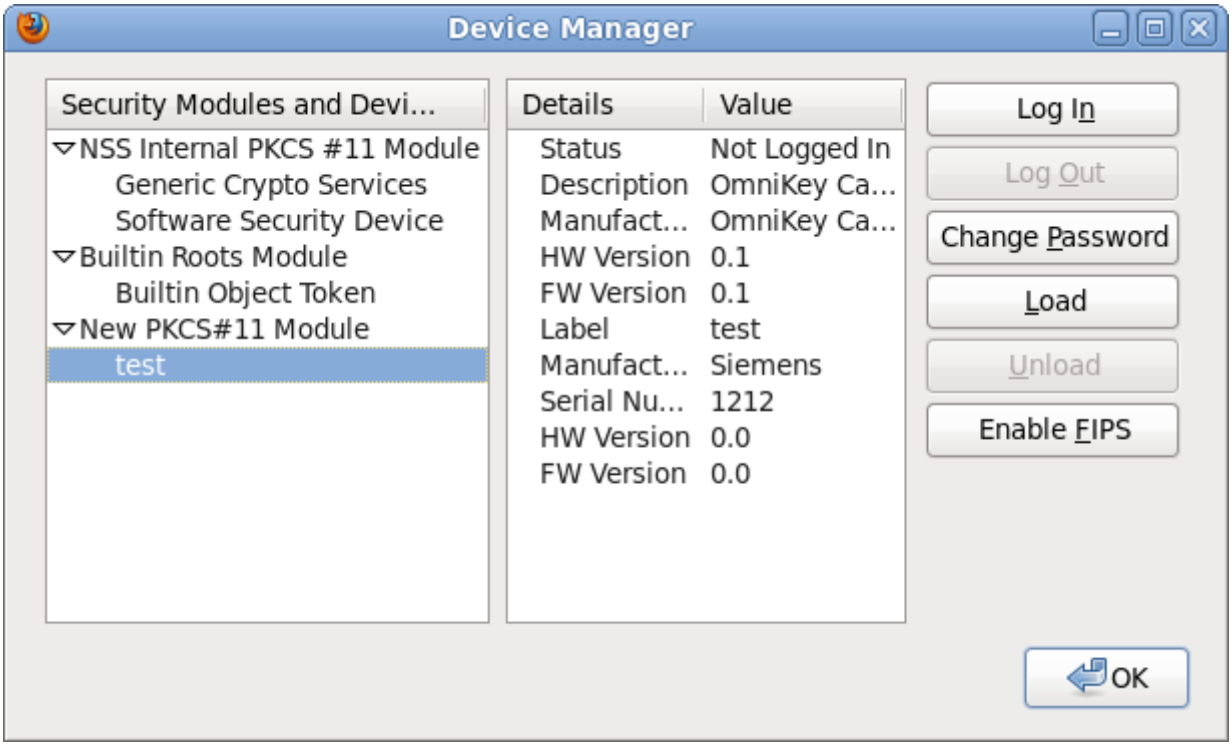
Note: Make sure to have a card reader connected before configuring Firefox and Thunderbird. It seems the "Browse" button in Firefox is not working correctly and gives a garbled path. It requires you to type manually the full path in the "path" field. To prevent mistyping, it is recommended following the instructions below:

- Open Mozilla Firefox.
- Go to Firefox (toolbar) – Preferences.
- Go to Advanced tab – Encryption tab.

- Click Security Device. The Device Manager window will open.



- Click on Load.
- Leave the Module Name's default value which is "New PKCS#11 Module".
- Enter the file path of libcmP11.so to the Module filename.
- Click OK.



5.2 Configuring Thunderbird

Configuring libcmP11.so in Thunderbird is just the same as Firefox. Please refer to 5.1 Configuring Firefox.

6 Information / Export Restrictions

Charismathics GmbH

47 Sendlinger St

80331 Munich

Germany

Manual Revision: November 26, 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.