

# Charismathics Smart Security Interface © User Manual V 5.0 for LINUX



#### Contents

1		Introduction	3
2		Supported Hardware	5
	2.1	Supported Smart Cards	5
	2.2	Supported Smartcard Readers	2
3		Administration Tool: Charismathics Security Token Configurator	11
	3.1	User Interface	11
	3.1.1	Token Configurator Menu	11
	3.1.2	Edit menu/ Context menu	12
	3.1.3	Token menu	12
	3.1.4	Info Menu	15
4		User Tool: Charismathics Smart Security Interface Utility	16
	4.1	Change PIN	16
	4.2	Unlock PIN	16
	4.3	Change Token SO PIN	17
5		Configuration of Applications supporting Charismathics PKCS#11	18
	5.1	Configuring Firefox	18
	5.2	Configuring Thunderbird	19
6		Information / Export Restrictions	20

## **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 <u>Chapter 4 Smart Security Interface</u> <u>Utility.</u>

#### libcmP11.so – PKCS11 Library for Linux

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

**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 <u>Chapter 3 Administration Tool:</u> <u>Charismathics Security Token Configurator</u>. **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.

👔 Charismathics Security Token Configurator 📃 🗆 🗵					
Manager Edit Token Key Pair Certificate About					
	Parameter	Value			
Description of the second seco					

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.

1		Create T	oken Profile 🛛 🗙
Profile	corporate profile	~	$\checkmark$ The length of the Card PIN has to be exactly 10.
Card PIN:	0987654321		The minimum length of the SO-PIN is 8.
SO PIN:	•••••		✓ The maximum length of the SO-PIN is 10.
Confirm SO PIN:	•••••		The SO-PIN was correctly verified.
User PIN:	•••••		The minimum length of the User PIN is 4.
Confirm User PIN	:•••••		The maximum length of the User PIN is 8.
Serial Number:	5948		The User PIN was correctly verified.
Label:	Test		The serial number shall have not more than 16 and at least one alpha-numeric digits.
			OK Cancel

#### 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"  $\rightarrow$  "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.

🛃 Lo	Login 🗙		
Please enter User PIN ASCII	ASCII		
DINI:	○ Numeric		
FIN.	<ul> <li>Hex Input</li> </ul>		
	O Use PINPAD		
	🔿 Use Biometric		
OK Cancel			

Lo	gin 🛛 🗙
Please enter User PIN	
Numeric	O ASCII
	<ul> <li>Numeric</li> </ul>
PIN	○ Hex Input
Invalid data, please insert only numeric data or change to ASCII	O Use PINPAD
hamene data of change to Aben.	🔿 Use Biometric
OK Cancel	

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"

👔 Change	user PIN 🗙
ASCII Old user PIN: New user PIN: Confirm new user PIN: OK Cancel	<ul> <li>ASCII</li> <li>Numeric</li> <li>Hex Input</li> <li>Use PINPAD</li> </ul>
👔 Change	so PIN
ASCII Old SO PIN: New SO PIN: Confirm new SO PIN: Confirm new SO PIN: Confirm new SO PIN:	<ul> <li>ASCII</li> <li>Numeric</li> <li>Hex Input</li> <li>Use PINPAD</li> </ul>

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

👔 Charismathics Security Token Configurator 📃						
Manager Edit Token Key Pair Certificate	About					
V Slots	About		Value			
	Supported OS		3bf4180002c10a31fe5856346376c5			
OmniKey CardMan 3121 00 00 Te	Manual	em	Siemens CardOS V4.3b			
	Historical Bytes		56346376			
Certificates	Label		Test			
Certificates	Profile		corporate profile			
Data	Serial Number		5948			
Data	Maximum PIN Length		10			
General Keye	Minimum PIN Length		4			
Secret Keys	Free Card Memory	(in Bytes)	29762			

- "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 Util-***ity.* 

## 4.1 Change PIN

Charismathics Smart Security Interface				
	Change Token PIN	Unlock Token PIN	Change Token SO PIN	
smathics	Card label: tes Here you can chan Old PIN: New PIN: Confirm the N	ew PIN:	martcard.	
ari	● Alphanumeric ○ Numeric ○ Hexadecimal			
			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.

Ch Ch	Charismathics Smart Security Interface					
	Change Token PIN	Unlock Token PIN	Change Token SO PIN			
mathics	Card label: No smartcard inserted Here you can unlock the PIN of your Smartcard. SO PIN:					
charis	<ul> <li>Alphanumeric</li> </ul>	○ Numeric ○ Hex	adecimal Unlock PIN			

Charismathics Smart Security Interface				
	Change Token PIN	Unlock Token PIN	Change Token SO PIN	
smathics	Card label: tes Here you can chan SO PIN: New SO PIN: Confirm the N	t ge the SO PIN of you ew SO PIN:	ur Smartcard.	
ari	<ul> <li>Alphanumeric O Numeric O Hexadecimal</li> </ul>			
G-			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.

Firefox Preferences						
ूरी General	Tabs	Content	Applications	Privacy	Security	لن Advanced
General	Network	Update	Encryption			
Protoc ⊻ Us Certifi	Protocols ☑ Use SSL <u>3</u> .0 Certificates					
Whe	When a server requests my personal certificate:					
⊖ Se	<ul> <li>Select one automatically          <ul> <li>Ask me every time</li> </ul> </li> </ul>					
View	View Certificates <u>R</u> evocation Lists <u>V</u> alidation Security Devices					
00 <u>H</u> e	Image: Book of the second					

Click Security Device. The Device Manager window will open.

🕹 Load PKCS#11 Device 🗕 🗆 🖂						
Enter the information for the module you want to add.						
Module Name: New PKCS#11 Module						
Module <u>fi</u> lename: <u>B</u> rowse						
Cancel Cancel						

- 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.

<mark>ک</mark> Dev	vice Manager		- 0 ×
Security Modules and Devi	Details	Value	Log I <u>n</u>
<ul> <li>▼NSS Internal PKCS #11 Module Generic Crypto Services Software Security Device</li> <li>▼Builtin Roots Module</li> </ul>	dule Status Description e Manufact HW Version FW Version Label Manufact Serial Nu HW Version FW Version	Not Logged In OmniKey Ca OnniKey Ca 0.1 0.1 test Siemens 1212 0.0 0.0	Log <u>O</u> ut
			Change <u>P</u> assword
Builtin Object Token ▼New PKCS#11 Module			Load
test			Unload
			Enable <u>F</u> IPS
			€ОК

## 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

#### © Copyright Charismathics GmbH 2002-2012

All rights reserved. Without the express prior written consent of Charismathics you must not distribute, edit or translate copyrighted material.

#### 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.