

## Charismathics Smart Security Interface for Mac OS X Version 5.0

**User Manual** 

October 30, 2012

charismathics

## **Table of Contents**

1	Introdu	action
2	Suppor	rted Hardware and Software Applications4
	2.1	Supported Applications4
	2.2	Supported Smart Cards4
	2.3	Supported Smart Card Readers7
3	Admini	stration Tool: Token Configurator8
	3.1	User Interface
	3.1.1	Token Configurator Menu10
	3.1.2	File Menu12
	3.1.3	Edit Menu13
	3.1.4	Token Menu13
	3.1.5	Window Menu19
4	User To	col: Charismathics Smart Security Interface Utility20
4	4.1	Change PIN20
4	4.2	Unlock PIN21
4	4.3	Change Token SO PIN21
5	Config	uration of Applications supporting Charismathics PKCS#11 Library22
!	5.1	Configuring Firefox22
ļ	5.2	Configuring Thunderbird23
6	Configu	uration of Applications supporting Charismathics tokend24
(	6.1	Configuring Mail24
(	6.2	Configuring Entourage24

# **1** Introduction

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

**CSSI** for Mac 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
- AET profile
- PIV profile
- IAS ECC profile
- CNS profile
- FineId profile

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

#### ScardUtility.app

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

Installed in the following location: /Applications/Charismathics/

#### libcmP11.dylib

- Information on how to use this library and configuring its supported applications is explained in Chapter 5 Configuration of Applications supported by libcmP11.dylib.
- Installed in the following location: /Applications/Charismathics/

#### CSSI.tokend

- Information on how to use this module and configuring its supported applications is explained in Chapter 6 Configuration of Applications supported by CSSI.tokend.
- Installed in the following location: /Library/Security/tokend/

**CSTC** - **Charismathics Security token configurator** for Mac is not included in CSSI User edition tool and has to be purchased separately. It is comprised of the following modules:

#### Token Configurator.app

- Information on how to use this tool is described in Chapter 3 Administration Tool: Token Configurator.
- Installed in the following location: /Applications/Charismathics/

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

- Smart card login to Mac
- SSL- Authentication by smart card (Mozilla Firefox, Safari, Google Chrome)
- Email security with cards using Thunderbird
- Email Security with Office mac 2011
- Centrify Smart card login to Active Directory Domain
- Adobe Acrobat
- Email security with cards using Mail.app and Entourage
- VPN

## **2** Supported Hardware/Software Applications

## 2.1 Supported Applications

CSSI for Mac supports the following applications:

Client OS	Component	Applications/Usage
Mac OS X 10.5.6 and higher	CSSI.tokend	<ul> <li>Smart card login into Mac</li> <li>Email security with Mail.app</li> <li>Safari, Google Chrome</li> <li>Email security with Entourage</li> <li>Keychain (viewing of certificate and keys)</li> <li>VPN</li> <li>Adobe Acrobat Digital Signing</li> <li>Centrify Mac Smart card login to AD.</li> </ul>
	libcmP11.dylib	<ul> <li>Email security with Thunderbird</li> <li>SSL-Authentication with smart card in Firefox</li> </ul>

## 2.2 Supported Smart Cards

CSSI for Mac is tested with the following smart cards:

ACOS A-Trust Card

ACOS A04

ACOS EMV A03

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 2.0
- 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
- NetKey PKS/2000/E4

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
- Derthur ID One V5.2a Dual
- Oberthur CosmopolIC 64K V5.2 Fast ATR (1)
- SIPRNet token

## 2.3 Supported Smart Card Readers

Please make sure your PC/SC smart card reader has been installed according to the producer's specifications and is fully operational.

The following smart card readers have been tested for CSSI Mac:

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

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

*Note:* PC/SC-drivers are supported. If RSA 2048 bit key shall be used, then the smart card reader must support the extended APDU.

## **3** Administration Tool: Token Configurator

**Token Configurator** 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 smart card, 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 Token Configurator you will see the following interface:

#### Token Configurator with no card reader or token inserted



#### Token Configurator with smart card, smart card reader or token inserted



- The top tabs display the smart card readers that are connected to the system. Smart card readers and virtual USB token readers are displayed in the same window. Once a token has been inserted, an additional tab will be displayed. Selecting the tab will display the information of the token.
- The left panel contains the Label, Certificates, Container, Symmetric Keys and Data icons. Selecting the icon displays the parameters and its associated values on the left panel.

### 3.1.1 Token Configurator Menu

<b>É</b>	Token Configurator File Edit	Token Window	🐓 Help	
Θ 🕚	About Token Configurator			Charismathics Token Configurator
OmniK	Preferences ೫,	n 01 00	Card Interna	Is for 'test'
-	Services		Manufacturer	
	Hide Token Configurator 第H Hide Others 乙第H Show All	vices CA 1, ou=Interna IA, ou=OISTE Foundat		19 items 6
2	Quit Token Configurator #Q Container 2 containers	CA, ou=International,	Free Memory Free Private Memory Sessions	33089 0
2 2 2			Max. RW Sessions Card Internal Time Maximum PIN length Private Memory	10 33089
	Data O notes		Flags Max. SO Length Installed Profile	CORPORATE
			Label Model Minimum PIN length	CardOS V4.3B

#### About Token Configurator

Shows a window that contains further information about the Token Configurator application.

#### Preferences

This gives you the option to view and add smart cards with new ATR value.

**Viewing supported cards:** To view the list of supported cards just go to **Token Configurator -Preferences – Supported Cards**.

00	O O Token Configurator Preferences	or
test Certificates certificates certificates certificates certificates certificates certificates certificates certificates certificates certificates certificates certificates con-Wiseke Container container	Token Configurator Preferences           Supported Cards         Logging           Name         Historical bytes           Oberrithur Cosmopolic G4K V52.20         0031C06477E3000829000           Oberrithur Cosmopolic G4K V52.20         0031C064781000019000           Oberrithur Cosmopolic G4K V52.20         0031C06480F31000019000           Oberrithur Cosmopolic G4K V52.20         0031C06480F31000019000           Nettkey (TCOS V2AI)         0064051020331809000           Telesec TCOS 2.2         0064051020331809000           Telesec TCOS 2.x         00640578020331809000           Telesec TCOS 2.x         006640578020331809000           COP 20         00644100432059000           Micardo F2.1         0068057600028FF05233180009000           GardOS V4.2 CMS         00680508C80011011434E53103180           CardOS V4.3 CMS         00680508C800121011434E53103180           CardOS V4.3 CMS         00680508C800121011434E53103180           CardOS V4.3 CMS         00680508C8080121011344E53103180           CardOS V4.3 CMS         00680508C8080121011344E53103180           CardOS V4.3 CMS         00680508C8080121011344E53103180           CardOS V4.3 CMS         00680508C8080121011344E53103180           CardOS V4.3 CMS         00680508C8080211011344E53103180	

**Adding supported cards:** Token Configurator can be used to associate smart card operating systems with new ATRs.

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

- 1. Go to SmartCard Admin Preferences Supported Cards Tab.
- 2. Click on the "+" sign found in the lower left corner.
- 3. Enter the **Historical Bytes**.
- 4. Select the **Type** of the smart card operating system on the drop-down list.
- 5. Click on Add.



The newly added card can now be viewed on the Supported Cards list.

Quit Token Configurator

Quits the Token Configurator application.

### 3.1.2 File Menu



Import

Allows you to import RSA keys and certificates from an .cer, .pfx or .p12 file. You may also drag the file from the finder to the left content list of the token.

Export

Allows you to export certificates in to your computer.

### 3.1.3 Edit Menu

🗯 Token Configu	<b>ırator</b> File	Edit Token Window	<b>9</b>	Help	
9 🔿 🌕		Undo	жZ		Charismathics Token Configurator
OmniKey CardMan 5121 00	00 Charismath	Redo	ΩដΩ		
e o test		Cut	жx	d Internal	s for 'test'
		Сору	жC	Manufacturer	Siemens
Certificates		Paste	жV	cimum Sessions	100
3 certificates		Delete	<b>~</b> #α	Mechanisms	19 items
🛐 cn=WISeKey C	ertifyID Advan	Select All	жA	Min. SO Length	6
🔁 cn=OISTE WISe	Key Global Ro			reatableProfiles	3 items
📴 cn=WISeKey C	ertifyID Advan	Find	•	Free Memory	0
0 🥱 Container		Special Characters	∵жт	Private Memory	
2 containers		special characters		Sessions	
🔣 ae2315e7-b7f	3-4f02-b931-	be1a863370b9		lax. RW Sessions	10
-0-0	3-47c8-835c-			rd Internal Time	
Symmetric Key				mum PIN length	
0 keys	3			Private Memory	
A. 4.				Flags	
Data 0 notes					CKF_RNG, CKF_LOGIN_REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED
0 notes				Max. SO Length Installed Profile	
				Label	
					CardOS V4.3B
			Mini	mum PIN length	
			MITH	SerialNumber	
				Memory	
				RW Sessions	
				365510115	1

#### Delete

Allows you to delete a certificate or key. To do this, just highlight the certificate or key and go to Edit - Delete.

### 3.1.4 Token Menu



#### Login

**PIN** means "Personal Identification Number". It is a unique personal code or password which is often used to authenticate the user and gain access to various systems such as credit and debit cards, bank, and computer accounts. One common example are Automatic Teller Machines (ATMs). When the user entered the correct PIN, the user is granted access to the system.

🗯 T	oken Configurator File Edit Token Window	🐓 Help	- · · · · · · · · · · · · · · · · · · ·
0 🔴 🔿			Charismathics Token Configurator
OmniKey	CardMan 5121 00 00 Charismathics token 01 00		
-	test	Card Interna	
Capture	Certificates	Manufacturer Maximum Sessions	Type: 🕑 PIN 🔘 SO-PIN
₩ <u>₩ </u>	3 certificates cn=WISeKey CertifyID Advanced Services CA 1, ou=Interna	Mechanisms Min. SO Length	
	cn=OISTE WISeKey Global Root GA CA, ou=OISTE Foundat cn=WISeKey CertifyID Advanced G1 CA, ou=International,	CreatableProfiles Free Memory	Cancel OK
2	Container 2 containers	Free Private Memory Sessions	
	ae2315e7-b7f3-4f02-b931-be1a863370b9 cfacd591-0b53-47c8-835c-fffbfab4c035	Max. RW Sessions Card Internal Time	-
<u>6</u>	Symmetric Keys	Maximum PIN length Private Memory	33089
	Data		CKF_RNG, CKF_LOGIN_REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED
	0 notes	Max. SO Length Installed Profile	CORPORATE
		Label Model	test CardOS V4.38
		Minimum PIN length SerialNumber	
		Memory RW Sessions	
		Memory RW Sessions	

Prior to operations on the token, the user is required to log in with his User PIN or SO-PIN. Once logged in, additional information becomes available, both within the left and the right panel. Failing to enter the correct User PIN three times in a row locks the card. See "Reset PIN" on how to clear the lock.

The hardware configuration and user settings determine the initial PIN entry method. To change the entry method, click on the drop down button and choose an entry method. Supported entry methods are:

#### ASCII

Every character is valid. However, the card may not support unusual characters.

Numeric

Each character of the PIN needs to be a number ('0'...'9'). This can be used to ensure PINPAD compatibility.

Hex

The PIN has to be entered in a hexadecimal format. Two digits will be converted to one character of the PIN, e.g 61 to 'a', 62 to 'b', 63 to 'c' ... For each digit the valid values are characters '0'-'9' and 'a'-'f'.

PINPAD

This option is only available when a reader with a pinpad is connected and authentication to the inserted 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 Secure PIN Entry (SPE) reader.

Logout

This item works analogous to the "Login" option.

• Change User PIN and Change SO 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 mistyping. All values are masked with **bullets** to provide privacy. The PIN entry method can be changed the same way as in the login dialog.

<b>* Token Configurator</b> File Edit Token Window	🐓 Help		) 🕴 🛜 🜒 💽 Mon 6:24 PM Q
		Charismathics Token Configurator	
OmniKey CardMan 5121 00 00 Charismathics token 01 00	Cand Internet	PIN:	
test	Card Interna	ASCII	
Certificates	Manufacturer Maximum Sessions		
3 certificates	Mechanisms		
cn=WISeKey CertifyID Advanced Services CA 1, ou=Interna			
cn=OISTE WISeKey Global Root GA CA, ou=OISTE Foundat	CreatableProfiles		
cn=WISeKey CertifyID Advanced G1 CA, ou=International,		Type: 💿 PIN 🔘 SO-PIN	
🟫 Container	Free Private Memory Sessions		
2 containers	Max, RW Sessions	Cancel OK	
ae2315e7-b7f3-4f02-b931-be1a863370b9	Card Internal Time		
Cfacd591-0b53-47c8-835c-fffbfab4c035		10	
Symmetric Keys 0 keys	Private Memory		
Data		1037 CKF_RNG, CKF_LOGIN_REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED	
0 notes	Max. SO Length	10	
	Installed Profile	CORPORATE	
	Model Minimum PIN length	CardOS V4.3B	
	SerialNumber		
	Memory		
	RW Sessions	1	
🖸 Takan Canfiguratan Kila Edit Takan Window	4 Halp		* <b>C</b> # 175 Mar 625 PM 0
Token Configurator File Edit Token Window	🐓 Help	Charismathics Token Configurator	) 🔅 🎅 ৰে) 💿 Mon 6:25 PM Q
	🐓 Help	Charismathics Token Configurator	) 🔅 🎅 📢 💽 Mon 6:25 PM Q
000	Server Help		) 🔅 🎅 4)) 🖅 Mon 6:25 PM Q
Omnikey CardMan 5121 00 00 Charismathics token 01 00		Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN:	) 🖇 🎅 🐠 (로) Mon 6:25 PM Q
OmniKey CardMan 5121 00 00 Charismathics token 01 00	Card Int	Charismathics Token Configurator Change the SO-PIN (PUK)	) 🔅 🎅 �) 💽 Mon 6:25 PM Q
Cominikey CardMan 5121 00 00 Charismathics token 01 00 test CardMan 5121 00 00 Charismathics token 01 00 test CardMan 5121 00 00 Charismathics token 01 00 test test test test test test test te	Card Int Manufi Maximum Se Mechi	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN:	) 🔅 🎅 4)) 💽 Mon 6:25 PM Q
Omnikey CardMan 5121 00 00       Charismathics token 01 00         Image: Certificates       3 conflicates         Image: CertifyID Advanced Services CA 1, ou=Internet	Card Int Manufi Maximum Se Mechi Min. SO	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: ASCII New PIN:	) 🔹 🎅 🐠 (프 Mon 6:25 PM) Q
Omikey CardMan \$121 00 00       Charismathics token 01 00         test       Certificates         3 certificates       Certificates         cn -WSEKey CertifyID Advanced Services CA 1, ou=Interm         cn -USTE WISEKey Clobal Root CA CA, ou=OISTE Foundat	Card Int Manufi Maximum Se Mechi Min. SO Creatable	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN:	) 🔅 중 4)) 🖅 Mon 6:25 PM Q
Ominikey cardMan 5121 00 00       Charismathics token 01 00         Test       Certificates         3 certificates       cruminate         cn = WiSeKey CertifyID Advanced Services CA 1, ou=International, cn=WiSeKey Clobal Root CA CA, ou=0ISTE Foundate         cn = WiSeKey CertifyID Advanced G1 CA, ou=International, cn=WiSeKey Clobal Root CA CA, ou=0ISTE Foundate	Card Int Manufi Maximum Se Mechi Min. SO	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: New PIN: Verify New PIN: Verify New PIN: C	) 🔅 🎅 4)) 💽 Man 6:25 PM Q
Omikey CardMan \$121 00 00       Charismathics token 01 00         test       Certificates         3 certificates       Certificates         cn -WSEKey CertifyID Advanced Services CA 1, ou=Interm         cn -USTE WISEKey Clobal Root CA CA, ou=OISTE Foundat	Card Int Manufi Maximum Se Mech Min. SO Creatable Free N Free Private M Se	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: ASCII New PIN:	) 🔹 🎓 🐠 (王) Mon 6:25 PM Q
Omikey CardMan 5121 00 00       Charismathics token 01 00         test       Certificates         a creinficates       creinficates         cr - WSEKey CertifyID Advanced Services CA 1, ou=Interm.         cr - OISTE WISEKey Clobal Root CA CA, ou=OISTE Foundat         cr - WISEKey CertifyID Advanced G1 CA, ou=International,         cr Container	Card Int Manufi Maximum Se Mech Min. SO Creatablef Free N Free Private M Se Max. RW Se	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: New PIN: Verify New PIN: Verify New PIN: C	) 🔌 🤝 🜒 🖅 Mon 6:25 PM Q
Omikey CardMan S121 00 00       Charismathics token 01 00         Test       Certificates         3 certificates       3 certificates         Cardinates       Containers         Containers       Certificates         CardInates	Card Int Manufi Maximum Se Mech Min. SO Creatablef Free Private N Free Private N Se Max. RW Se Card Internal Time	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: Ascil New PIN: Cancel Apply	) े रू ब) 💿 Mon 6:25 PM Q
Omilikey CardMan 5121 00 00       Charismathics token 01 00         Itest       Certificates         Cardificates       Control Contrective Control Control Control Control Cont	Card Int Manufi Maximum Se Mech Min. SO Creatablef Free N Free Private M Se Max. RW Se	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN:	) 🔹 🎓 🐠 (王) Mon 6:25 PM Q
Omikey CardMan 5121 00 00       Charismathics token 01 00         Test       Certificates         a certificates       Certificates         cn = USEKey Clobal Root CA CA, ou=OISTE Foundat         cn = OISTE WiSeKey Clobal Root CA CA, ou=International,         cn = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE For XI-2000         cr = Caratiners	Card Int Manuf Maximum S Min. 50 Creatable Free Private S Max. RW S Card Internal Time Maximum PIN length Private Memory Flags	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: SO-PIN: Verify New PIN: Cancel Apply 10 33089 1037	) 🔌 (국 4) (王) Mon 6:25 PM Q
Ominikey CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics 00         Image: CardMan 512 00	Card Int Manuf Maximum Se Mech Min. SO Creatable Free N Se Max. RW Se Card Internal Time Maximum PIN length Private Memory Flags	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: Asccl New PIN: Cancel Apply Cancel Apply 10 33069 1037 Ccf PAC, CKF, LOGIN, REQUIRED, CKF_USER, PIN_INITIALIZED, CKF_TOKEN_INITIALIZED	) े रू ब) उ Mon 6:25 PM Q
Omikey CardMan 5121 00 00       Charismathics token 01 00         Test       Certificates         a certificates       Certificates         cn = USEKey Clobal Root CA CA, ou=OISTE Foundat         cn = OISTE WiSeKey Clobal Root CA CA, ou=International,         cn = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE WiSeKey Clobal Root CA CA, ou=International,         cr = OISTE For XI-2000         cr = Caratiners	Card Int Manufi Maximum Se Mech Creatable Free Private Free Private Se Max RW Se Card Internal Time Maximum PIN length Private Memory Flags Max.SO Length	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN:	) 🔹 🎓 🐠 (王) Mon 6:25 PM Q
Ominikey CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics 00         Image: CardMan 512 00	Card Int Manuf Maximum Se Mech Min. SO Creatable Free N Se Max. RW Se Card Internal Time Maximum PIN length Private Memory Flags	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: Ascri New PIN: Cancel Apply Cancel Cancel Cancel Corport Canc	) 🔅
Ominikey CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics 00         Image: CardMan 512 00	Card Int Manuf Maximum Se Mech Min. SO Creatablef Free N Free Private N Se Max. RW Se Card Internal Time Maximum PN Length Private Memory Flags Hax So Length Installed Profile Label Model	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: SO-PIN: SO-PIN: SO-PIN: Cancel Apply Cancel Apply Cancel	) े रि क ब) (ट) Mon 6:25 PM Q
Ominikey CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics 00         Image: CardMan 510 00	Card Int Manuf Maximum Se Mech Min. SO Creatable Free Private Free Private M Se Max. RW Se Card Internal Time Maximum PIN length Private Memory Flags Max. SO Length Installed Profile Label Model Minimum PIN length	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: Ascil New PIN: Cancel Apply 10 3009 1037 CCF SNG, CKF, LOGIN, REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED 10 CORPORATE test Cardos V4.38 4	) 🔅 😤 4)) 🖅 Mon 6:25 PM Q
Ominikey CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 5121 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics token 01 00         Image: CardMan 512 00 00 00       Charismathics 00         Image: CardMan 510 00	Card Int Manuf Maximum S Mech Min. SO Creatable Free N Se Max. RW S Card Internal Time Maximum PN length Private Memory Flags Max. SO Length Installed Profile Label Minimum PIN length SerialNumber	Charismathics Token Configurator Change the SO-PIN (PUK) SO-PIN: SO-PIN: SO-PIN: SO-PIN: Verify New PIN: Cancel Apply Cancel Apply Cancel Canc	) 🔅 🎓 🌒 🖅 Mon 6:25 PM Q
Omikey CardMan 5121 00 00       Charismathics token 01 00         Test       Certificates         3 certificates       acrificates         acrificates       acrificates         cn=WiSeKey CertifyID Advanced Services CA 1, ou=Intern.         cn=0STE WiSeKey Clobal Root CA CA, ou=0ISTE Foundat         cn=WiSeKey CertifyID Advanced G1 CA, ou=International,         container         containers         ae2315e7-b713-4f02-b931-be1a863370b9         cf ac4591-0b53-47c8-835c-fffbfab4c035         Symmetric Keys         Data	Card Int Manuf Maximum Se Mech Min. SO Creatable Free Private Free Private M Se Max. RW Se Card Internal Time Maximum PIN length Private Memory Flags Max. SO Length Installed Profile Label Model Minimum PIN length	Charismathics Token Configurator           Change the SO-PIN (PUK)           SO-PIN:           New PIN:           Verify New PIN:         O           Cancel         Apply           10         33069           1037         CCr RMC, GKF, LOGIN, REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED           Corrors value           103         CardoS value           104         11           -1         -1	) े रि क ब) (ट) Mon 6:25 PM Q

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 for Mac supports alphanumeric PINs and is not restricted to numeric digits in general.

The User PIN must be entered to write on the card (e.g. key generation, storing a certificate), delete objects or to use cryptographic functions (e.g. signing or decryption). Refer to the table below regarding the 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 or reset 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 required for unlocking the User PIN.

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

#### **Constraints for PIN lengths:**

PIN (default)	Charismathics Profile	PKCS#15 Profile	CNS Profile
User PIN (1111111)	4 - 8	4 - 8	4 - 8
SO PIN (111111111)	8 - 10	8 - 10	4 - 8

#### Reset PIN

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.

<b>(</b>	oken Configurator File Edit Token Window	🐓 Help	🕘 🕴 🛜 🜒 💽 Mon 6:25 PM 🔍
0 🔴 🤇			Charismathics Token Configurator
OmniKey	CardMan 5121 00 00 Charismathics token 01 00		
•	test	Card Int	Reset the PIN with the SO PIN
		Manufi	SO-PIN:
Confident	Certificates	Maximum Se	ASCII
	3 certificates	Mechi	New PIN:
<b>1</b>	cn=WISeKey CertifyID Advanced Services CA 1, ou=Interna	Min. SO	
- E	cn=OISTE WISeKey Global Root GA CA, ou=OISTE Foundat	CreatableF	Verify New PIN:
	cn=WISeKey CertifyID Advanced G1 CA, ou=International,	Free N	
2	Container	Free Private M	
	2 containers	Se	Cancel Apply
2	ae2315e7-b7f3-4f02-b931-be1a863370b9	Max. RW Se	
2	cfacd591-0b53-47c8-835c-fffbfab4c035	Card Internal Time Maximum PIN length	
<u> </u>	Symmetric Keys	Private Memory	
<b>9</b> 8	0 keys		017 33069 1918 1037
	Data		ngo 1057 r ngo cKr_RNG, CKF_LOGIN_REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED
	0 notes	Max, SO Length	
		Installed Profile	file CORPORATE
		Label	bel test
		Model	del CardOS V4.38
		Minimum PIN length	gth 4
		SerialNumber	per 11
		Memory	
		RW Sessions	ins 1

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 the Reset PIN option, if you know the SO PIN.

#### Generate Key

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 Token Configurator.

🗯 Token Configurator File Edit Token Window	🐓 Help 🕘 🖇 🎅 🐗 💽 Mon 6:26 PM	Q,
000	Charismathics Token Configurator	
OmniKey CardMan 5121 00 00 Charismathics token 01 00		
test	Card I Key Type: RSA Keypair	
Certificates 3 certificates	Maximum Maximum fast 512 bits secure	
cn=WISeKey CertifyID Advanced Services CA 1, ou=Interna cn=OISTE WISeKey Global Root GA CA, ou=OISTE Foundat	Min. Creata Label: MyPersonalKey	
cn=WISeKey CertifyID Advanced G1 CA, ou=International, Container 2 containers	Fre Free Privat Cancel Generate	
ae2315e7-b7f3-4f02-b931-be1a863370b9 cfacd591-0b53-47c8-835c-fffbfab4c035	Max. RV-sessions to Card Internal Time Maximum RPI length 10	
Symmetric Keys 0 keys	Private Menory 33089 Flags 1037	
Data 0 notes	Flags CKF_RNG, CKF_LOGIN_REQUIRED, CKF_USER_PIN_INITIALIZED, CKF_TOKEN_INITIALIZED Max. SO Length 10	
	Installed Profile CORPORATE Label test	
	Model CardOS V4.38 Minimum PIN length 4 SerialNumber 11	
	seriaikumeer 11 Memory -1 RW Sessions 1	

In principle there are two possibilities:

- 1. You can generate keys (key pairs comprising private and public keys and secret keys) with the ad-ministration tool of Charismathics Smart Security Interface.
- 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. Please refer to <u>Chapter 3.1.2 File Menu - Import</u> on how to Import keys.

Use of these functions requires that you are logged into the smart card: go to **Token - Login** and enter your User PIN.

The generation of a key pair (private and public key) is accessed from the **Token - Generate Key**. Once the generation process is finished, you can view these keys in the left panel under Container or Symmetric Keys.

#### Create Certificate Request and Create Selfsigned Certificate

In order to use the smart card for digital signatures or encryption you need a key pair, i.e private key and corresponding public key. The public key is made accessible to communication partners via a certificate. Certificates can be generated and managed by the Token Configurator. These options help you to manage certificates:

- Create Selfsigned Certificate The certificate is signed with your private key. This
  means it is not issued from a well-known Certificate Authority (CA) and each user of
  this certificate has to manually specify it is trusted.
- Create Certificate Request (Generate CSR) Well-known CAs are usually already preset as "trusted" certificate issuers on most operating systems, that means the certificate will be trusted without any further interaction.

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 by going to File - Import. Please refer to <u>Chapter 3.1.2 File Menu - Import</u> on how to Import certificates.

#### **Rebuild Profile**

It is possible to delete an existing profile on a card and set up a new profile with the **Card PIN**. 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.

00		Charismat	thics Token Configurator		
Container     Container     Container     Container     Container     Container     Container     Container     Symmetric Keys     Data     O notes	0 Card Maxim Cres Free Pri MaxC Card Maximu Pri	Profile: ( Label: Serial-Number: Card PIN:	CORPORATE Charismathics 123 0987654321		진 🤌 🎅 40) Œ Mon 6:29 PM C
	Minimu <del>m PIN Tength</del>	7cff250c7515211 -1	Cancel Apply		

**Smart card with profile**: If there is already a profile on the card and you want to create a new one, the existing profile will be deleted as a first step. To erase the profile, you need to enter the Card PIN used to initialize the card. The default Card PIN is "0987654321".

**Empty Smart Card**: During initialization, the **Card PIN**, the **SO PIN**, the **User PIN** and a Serial Number are required. Additionally a Label for the token can be assigned.

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.

## 3.1.5 Window Menu

00	Minimize		ЖM	ismathics Token Configurator	
niKey CardMan 5121 00 00 Charismathics token 01 00	Zoom				
test	Bring All	to Front		est'	
	√ Charisma	thics Token Configu	rator		
😤 🤪 3 certificates		Mechanisms	19 items		
cn=WISeKey CertifyID Advanced Services CA 1	1, ou=Interna	Min. SO Length	6		
cn=OISTE WISeKey Global Root GA CA, ou=OI	ISTE Foundat	CreatableProfiles	3 items		
cn=WISeKey CertifyID Advanced G1 CA, ou=Ir	nternational,	Free Memory	0		
Container		Free Private Memory			
2 containers		Sessions			
ae2315e7-b7f3-4f02-b931-be1a863370b9		Max. RW Sessions	10		
cfacd591-0b53-47c8-835c-fffbfab4c035		Card Internal Time			
Symmetric Keys		Maximum PIN length			
0 keys		Private Memory Flags			
Data		Flags		, CKF LOGIN REQUIRED, CKF USER PIN INITIALIZED, CKF TOKEN INITIALIZED	
0 notes		Max. SO Length		, CR_LOGIN_REQUIRED, CR_USER_FIN_INITIALIZED, CRF_TOKEN_INITIALIZED	
0 10(0)		Installed Profile		ATE	
		Label			
			CardOS V4	/// 3R	
		Minimum PIN length			
		SerialNumber			
		Memory			
		RW Sessions			

Minimize

Minimizes the Token Configurator window.

Zoom

Maximizes the Token Configurator window.

# **4** User Tool: Charismathics CSSI

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 by following the path: /Applications/Charismathics/ScardUtility.app

## 4.1 Change PIN

000	Charismathics Smart Security Interface Utility
	Change Token PIN Unlock Token PIN Change Token SO PIN
athice	Card label: citrix-test Here you can change the PIN of your Smartcard. Old PIN: New PIN: Confirm the New PIN:
chariemathics	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

	Change Token PIN	Unlock Token PIN	Change Token SO PIN
		x-test the PIN of your Sma	rtcard.
S	SO PIN:		
ic	New PIN:		
mat	Confirm the Ne	w PIN:	
charismathics	• Alphanumeric (	Numeric OF	lexadecimal
ha		(	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.

	Change Token PIN	Unlock Token PIN	Change Token SO PIN
athics		w SO PIN:	Smartcard.
charismathics	• Alphanumeric (	) Numeric O F	Hexadecimal Change SO PIN

4.3 Change Token SO PIN

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 is dependent on the card OS.

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

# **5** Configuring Application with PKCS#11

## 6.1 Configuring Firefox

Note:

- a) Make sure to have a card reader connected before configuring FireFox and Thunderbird.
- b) Some version of the Firefox "Browse" button 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 to follow the instructions below.
- 1. Open Mozilla Firefox.
- 2. Go to Firefox (toolbar) Preferences.
- 3. Go to Advanced tab Encryption tab.
- 4. Click Security Device. The Device Manager window will open.
- 5. Click on Load.
- 6. Leave the Module Name's default value which is "New PKCS#11 Module".
- Browse the path of libcmP11.dylib to the Module filename. The file path should be /Application/Charismathics/libcmP11.dylib
- 8. Click OK.
- 9. A Confirm dialog will prompt. Just click OK.
- 10. An Alert window will prompt "A new security module has been installed". This means that you have successfully loaded the libcmP11.dylib module. Just press OK and you are done.

0	C	0			Device N	lanager		0
	Se T	NSS Inter Gener	lules and Devices nal PKCS #11 Mo ic Crypto Service	odule s	Details	Value		Log In Log Out
	•	Builtin Ru Builtir	<u>.</u>	Ale			been installer	e Password Load Inload Ible FIPS
								ОК

## 6.2 Configuring Thunderbird

Configuring libcmP11.dylib in Thunderbird is just the same as Firefox. Please refer to  $\underline{4.1}$ Configuring Firefox.

# 7 Configuring Applications with tokend

## 7.1 Configuring Mail

**Prerequisites**: When Mail.app is launched, a token needs to be inserted that has a valid certificate for one of the email accounts and its corresponding private key. After launching Mail.app, it will not search again for certificates.

- 1. Open Mail.
- 2. Click New Message.
- 3. Click on the Sign and Encrypt button for signing and encrypting emails.

<b>(</b>	Mail	File	Edit	View	Mailbox	Message	Format	Window	Help
00	0								Ir
$\bigcirc$	)			$\bigcirc$		(	≪∽ →		<u>/</u>
Get Ma	il			Delete	Junk	Reply F	Reply All Forw	ard New M	essage
0	0				New Messa	age			$\bigcirc$
I				$\mathbb{D}$		Ð			>>>
Send	Chat	Attack	n Addi	ress Fo	nts Colors	Save As Dr	aft	Photo Brow	ser
	Т	o:							
	С	<b>c</b> :							
	Subjec	:t:						-	
≣▼									*
									_
1									

## 7.2 Configuring Entourage

- 1. Open Entourage.
- 2. Go to Entourage Account Settings.
- 3. Double click on your email account.
- 4. In the Edit Account dialog, select Mail Security tab.
- 5. In the Digital Signing area, click the Select button.
- 6. Select your Digital Signing certificate from the list.

🛒 Entoura	<b>ge</b> File	Edit	View	Message	Format	Tools	Window	Help	\$
000	Accour	nts		οĹ			Ed	it Accour	nt
New Delete			Make	Default		Acco	unt Settings	Options	Mail Security
Mail		Digital Signing Signing a message by using a certificate (digital ID) helps the recipient verify the authenticity of the message.							
	,				Signin	g certificat	e: <no< th=""><th>certificate</th><th>selected&gt; Select</th></no<>	certificate	selected> Select
	000	)		Cho	ose An Ide	ntity			
			sign me:	the certificat ssages from n-DEVSERVER	this accour		u will use t	o digitall	y in signed messages il ID) to send
			Show	Certificate	) I En	crypt outgo	Cancel		OK Select okments by default
		Γ			<u>Learn abo</u>	<u>ut diqital siq</u>	ining and encr	<u>yption</u>	(Cancel) OK

- 7. Click Choose.
- 8. Select your Encryption certificate from the list.
- 9. Click Choose.
- 10. Once you have selected your certificates, set the following options:
  - Select "Digitally sign all outgoing messages by default"
  - Select "Send digitally signed messages as clear text" This ensures that recipients can read your signed messages. It is important if your recipient is using a web-based or mobile mail client.
  - Select "Include my signing and encryption certificates in signed messages" This option includes your public encryption key so that someone else can use it to send you encrypted messages.

Edit Account
Account Settings Options Mail Security
Digital Signing
Signing a message by using a certificate (digital ID) helps the recipient verify the authenticity of the message.
Signing certificate: charismathics Select
Signing algorithm: SHA-1 (more compatible)
Digitally sign outgoing messages by default
Send digitally signed messages as clear text
☑ Include my signing and encryption certificates in signed messages
Encryption
Other people use your encryption certificate (digital ID) to send encrypted messages to you.
Encryption certificate: <no certificate="" selected=""> Select</no>
Encryption algorithm: 3DES (more compatible)
Encrypt outgoing messages and attachments by default
Learn about digital signing and encryption
Cancel OK