Charismathics Smart Security Interface for Mac OS X Version 5.0

User Manual

October 30, 2012

charismathics

Table of Contents

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	• Smart card login into Mac • Email security with Mail.app • Safari, Google Chrome • Email security with Entourage • Keychain (viewing of certificate and keys) • VPN • Adobe Acrobat Digital Signing • Centrify Mac Smart card login to AD.
	libcmP11.dylib	• Email security with Thunderbird • SSL-Authentication with smart card in Firefox

2.2 Supported Smart Cards

CSSI for Mac 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 2.0
- 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
- Oberthur 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.

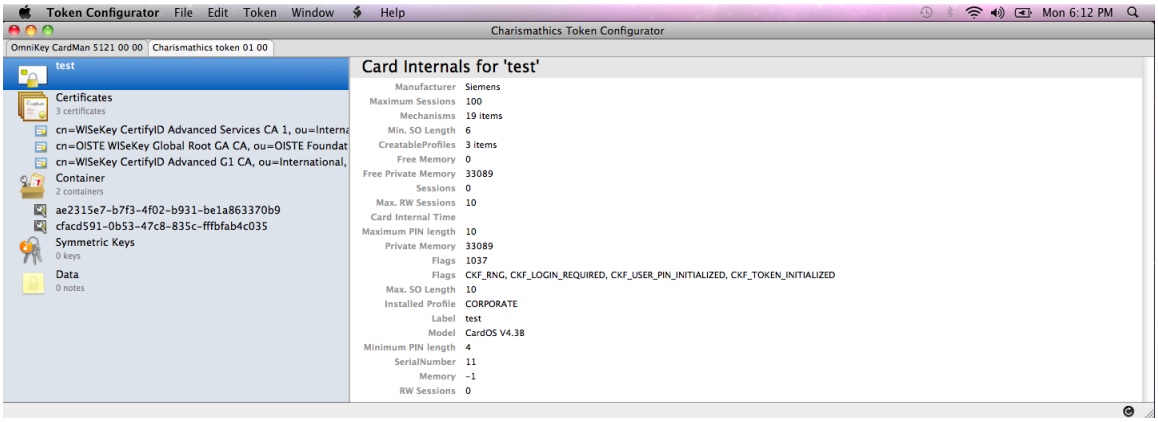
Note: After changing the contents of the smart card, you need to remove and reinsert the smart card to see the changes in other applications. This also applies when you perform Create Profile, Generate Key and Imports functions.

3.1 User Interface

After opening Token Configurator you will see the following interface:

Token Configurator with no card reader or token inserted

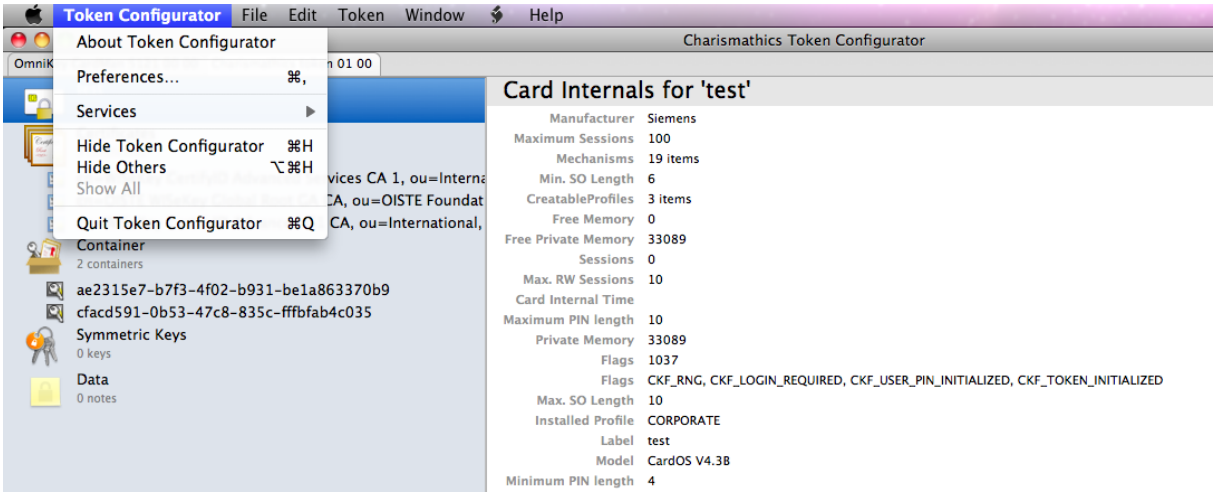
Token Configurator with smart card, smart card reader or token inserted



- 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



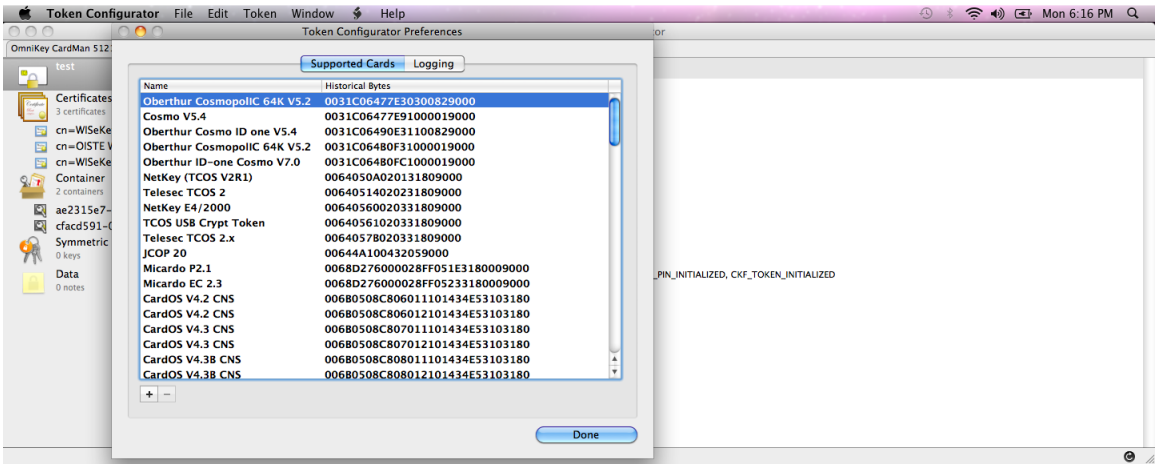
- **About Token Configurator**

  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.

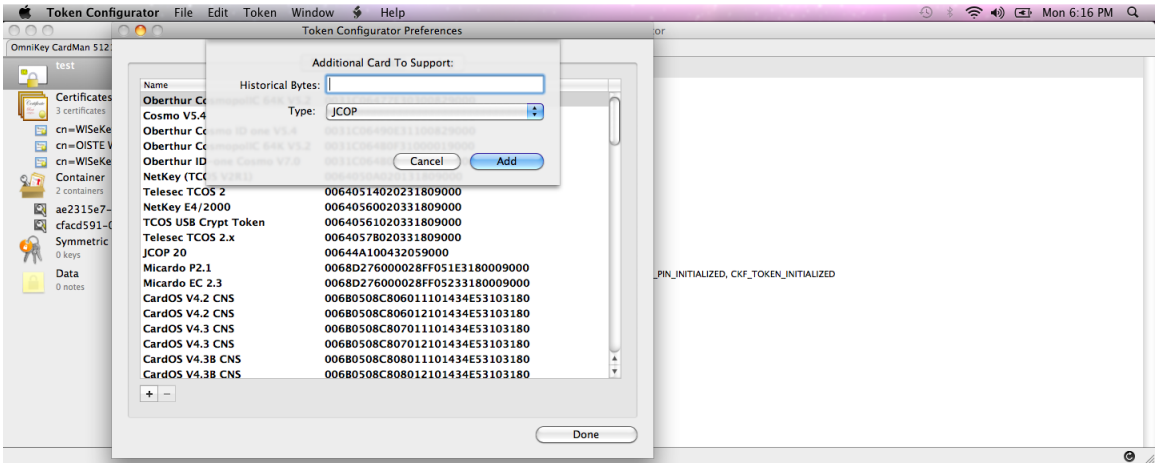
Viewing supported cards: To view the list of supported cards just go to **Token Configurator - Preferences – Supported Cards**.



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**.

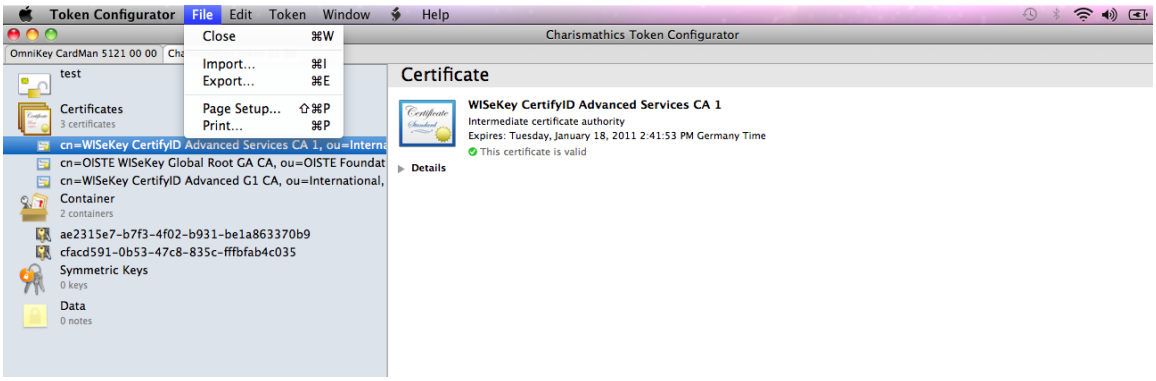


The newly added card can now be viewed on the Supported Cards list.

- **Quit Token Configurator**

  Quits the Token Configurator application.

3.1.2 File Menu



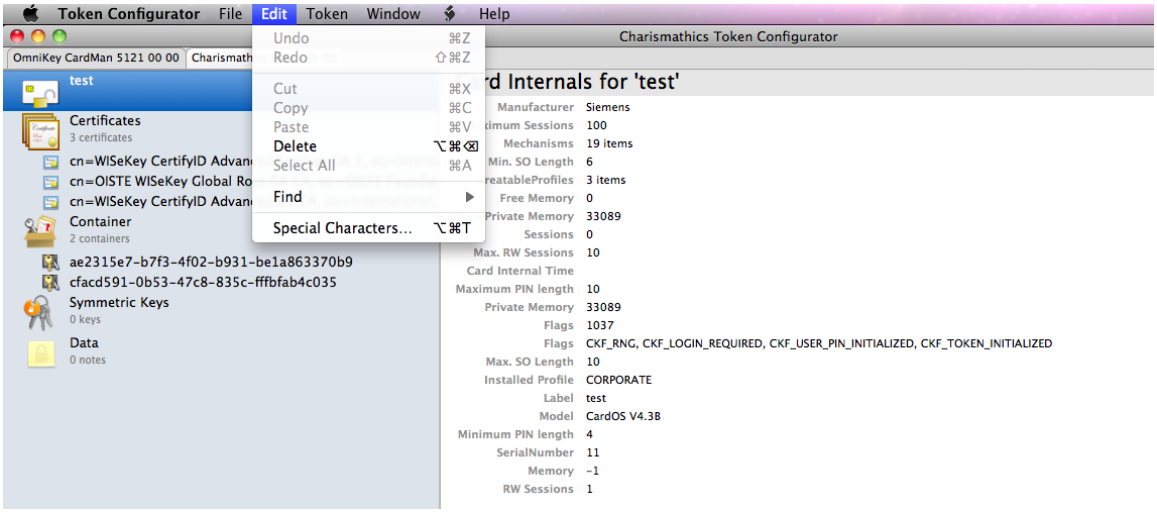
- **Import**

  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.

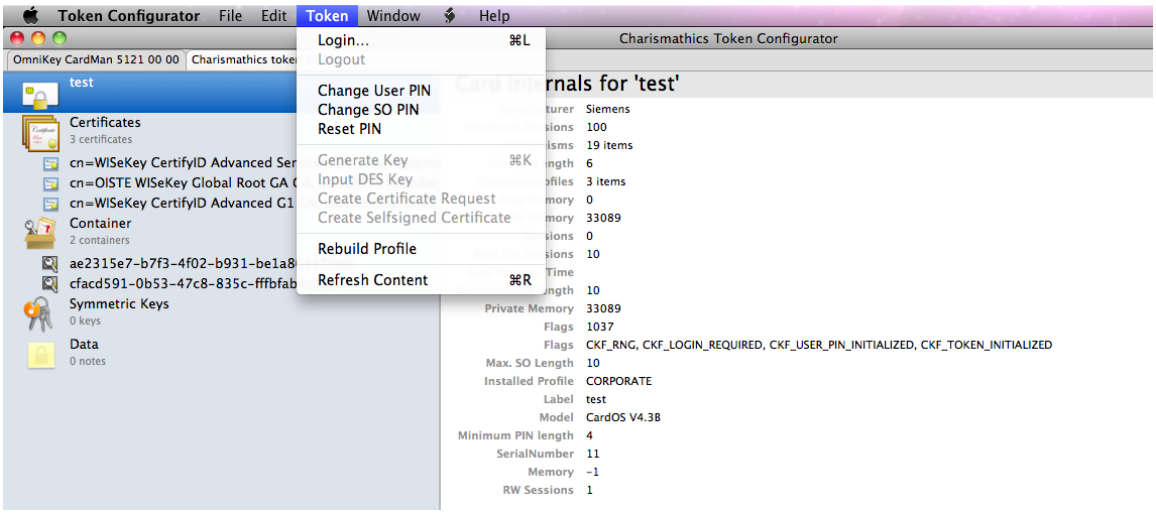
3.1.3 Edit Menu



- **Delete**

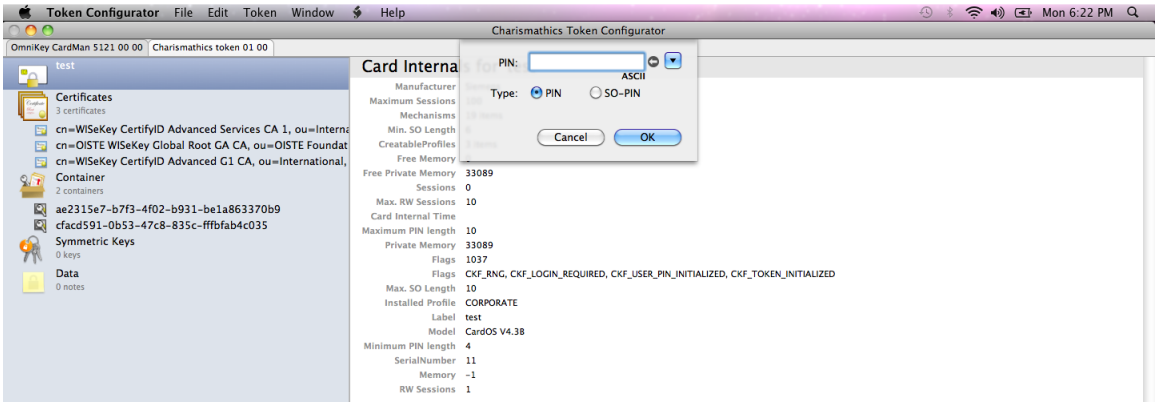
  Allows you to delete a certificate or key. To do this, just highlight the certificate or key and go to Edit - Delete.

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.



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.

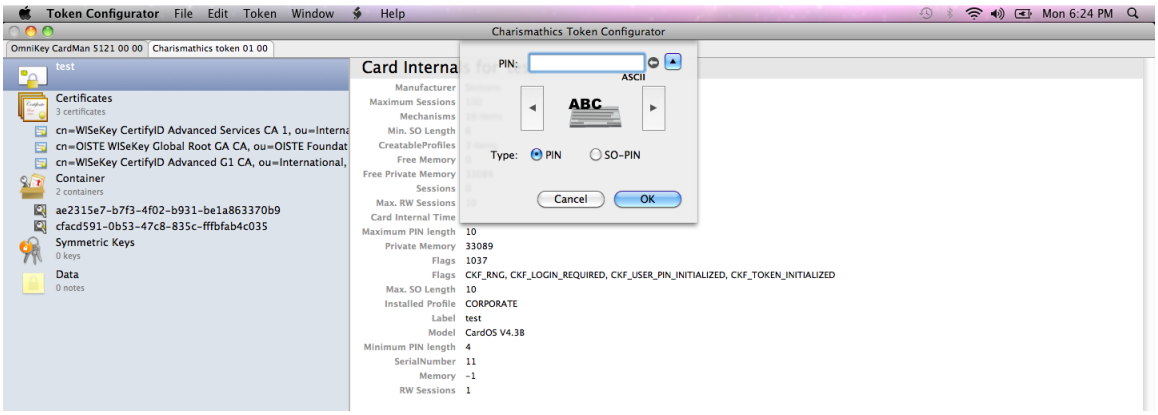
- **Hex**
  The PIN has to be entered in a hexadecimal format. Two digits will be converted to one character of the PIN, e.g 61 to 'a', 62 to 'b', 63 to 'c' …
  For each digit the valid values are characters '0'-'9' and 'a'-'f'.

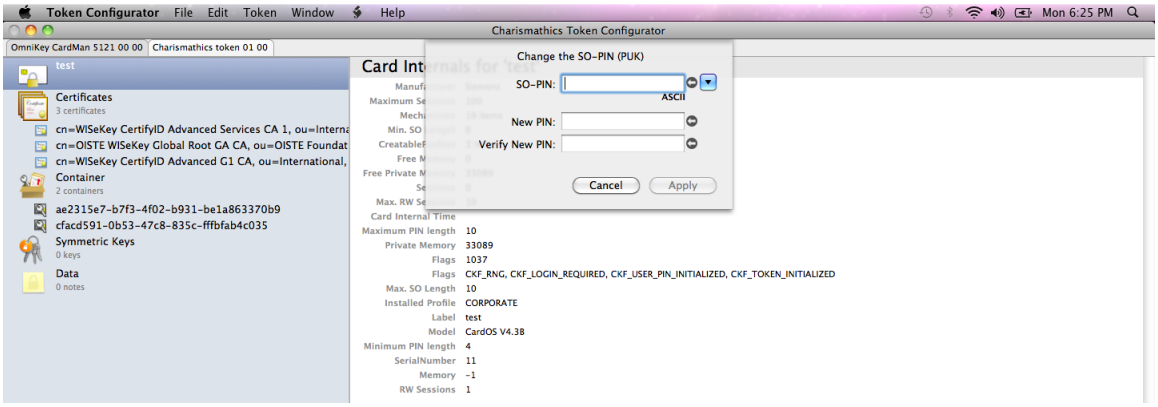
- **PINPAD**
  This option is only available when a reader with a pinpad is connected and authentication to the inserted token is possible via secure PIN entry. When this option is selected, the edit text for the PIN will be disabled and the user must input the PIN from the corresponding Secure PIN Entry (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.





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.

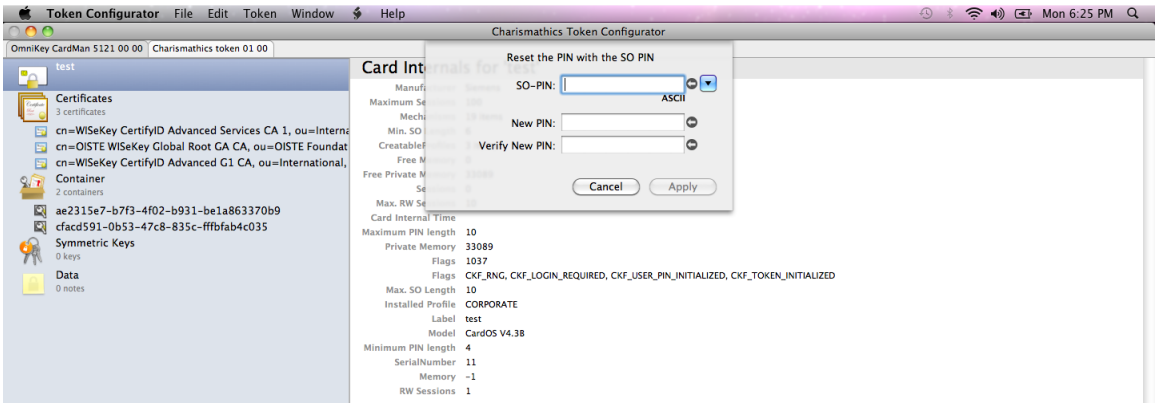
IMPORTANT: After ten consecutive wrong inputs the SO PIN will be locked.

Constraints for PIN lengths:

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

- **Reset PIN**

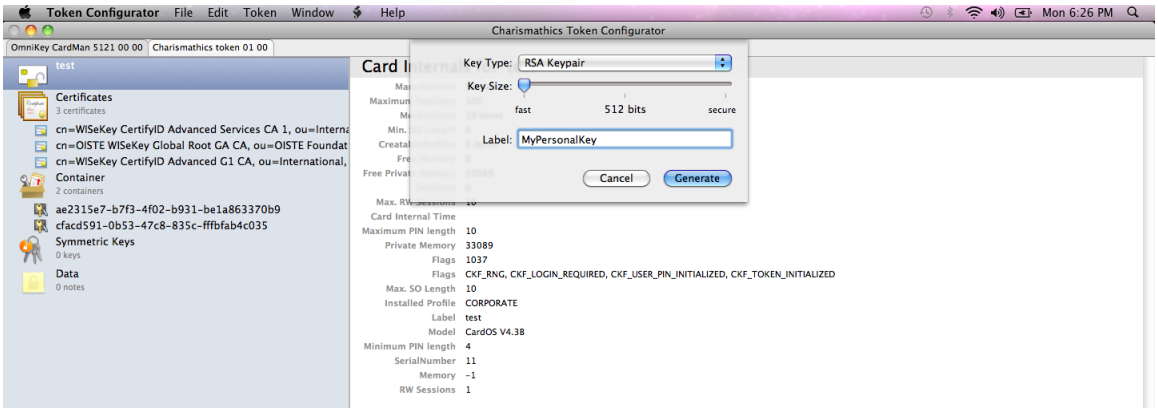
As a security measure a token will be locked if a user enters a wrong PIN three times in a row. This provides security since an unauthorized person could otherwise check all possible PINs by trial and error if you lost your smart card or USB token, or it has been stolen.



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.



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.

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. Please refer to Chapter 3.1.2 File Menu - Import 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:

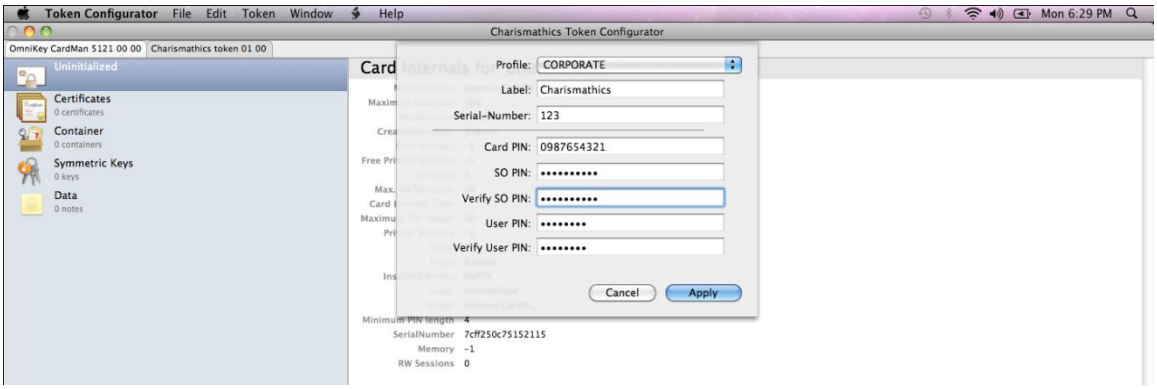
- Create Selfsigned Certificate - The certificate is signed with your private key. This means it is not issued from a well-known Certificate Authority (CA) and each user of this certificate has to manually specify it is trusted.

- 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 Chapter 3.1.2 File Menu - Import 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.

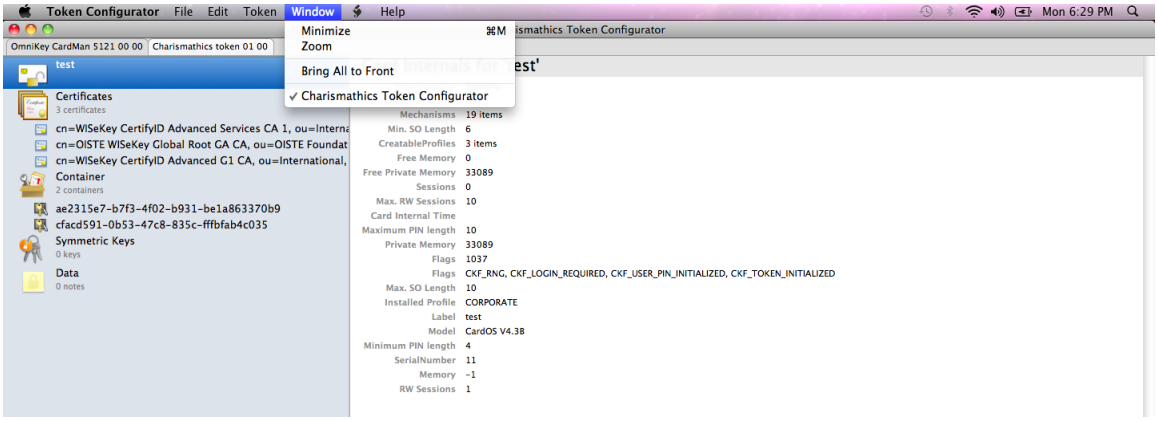


Smart card with profile: If there is already a profile on the card and you want to create a new one, the existing profile will be deleted as a first step. To erase the profile, you need to enter the Card PIN used to initialize the card. The default Card PIN is "0987654321".

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



- **Minimize**

  Minimizes the Token Configurator window.

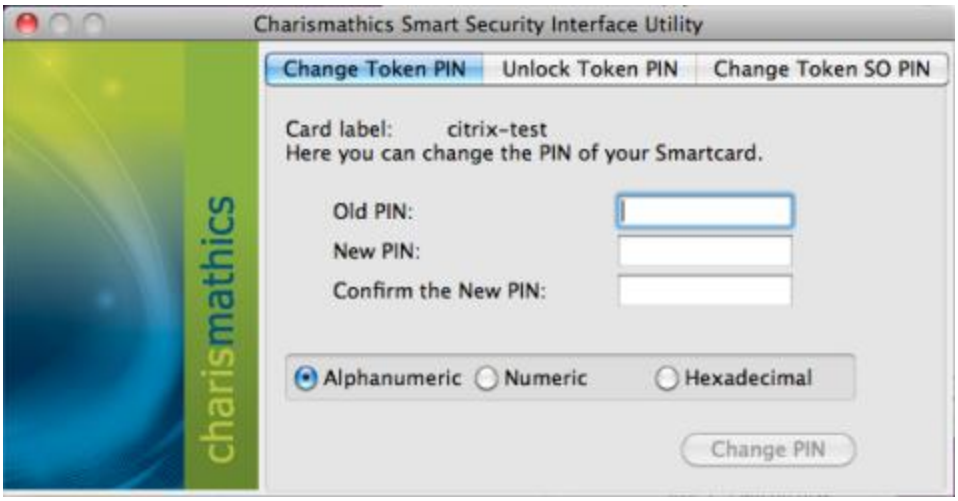
- **Zoom**

  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



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.

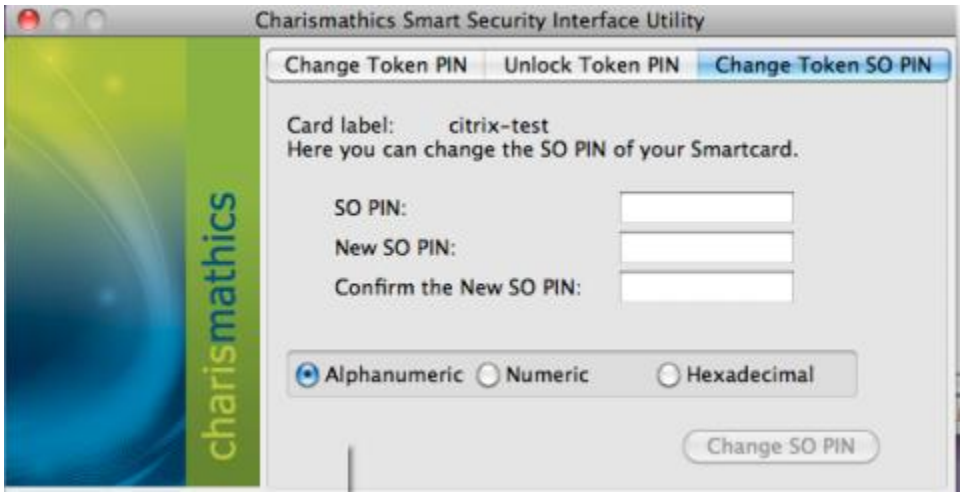
Click on the button "Change PIN", and you receive a window with the confirmation.

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.

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".
7. 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.

6.2 Configuring Thunderbird

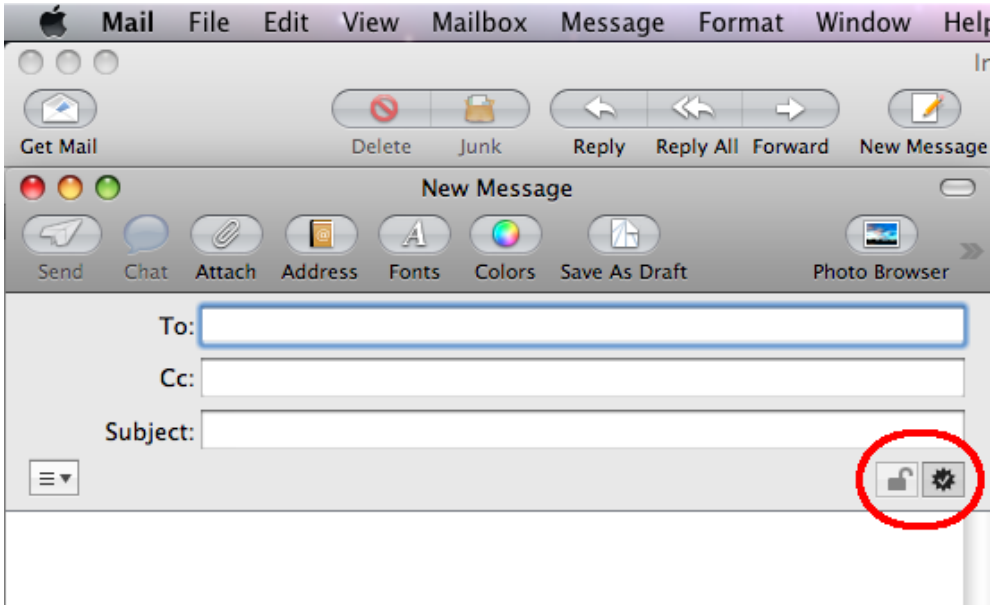
Configuring libcmP11.dylib in Thunderbird is just the same as Firefox. Please refer to **4.1 Configuring Firefox**.

7 Configuring Applications with tokend

7.1 Configuring Mail

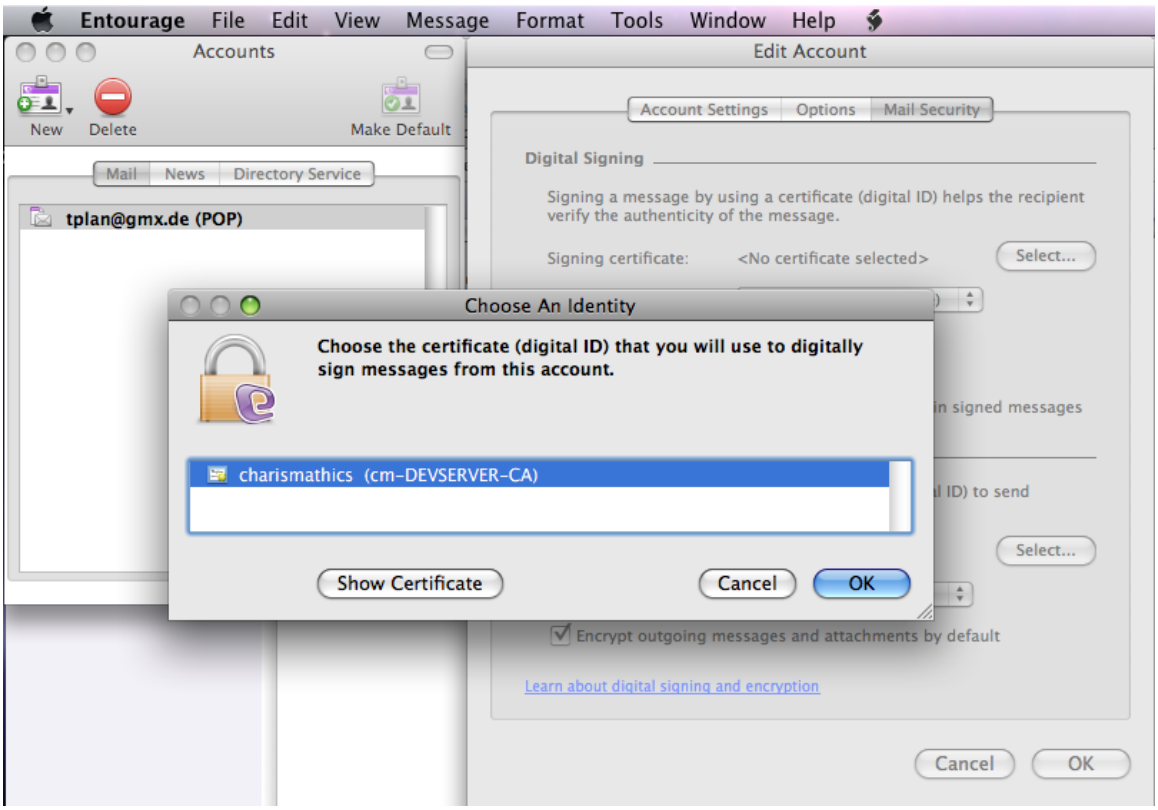
Prerequisites: When Mail.app is launched, a token needs to be inserted that has a valid certificate for one of the email accounts and its corresponding private key.
After launching Mail.app, it will not search again for certificates.

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



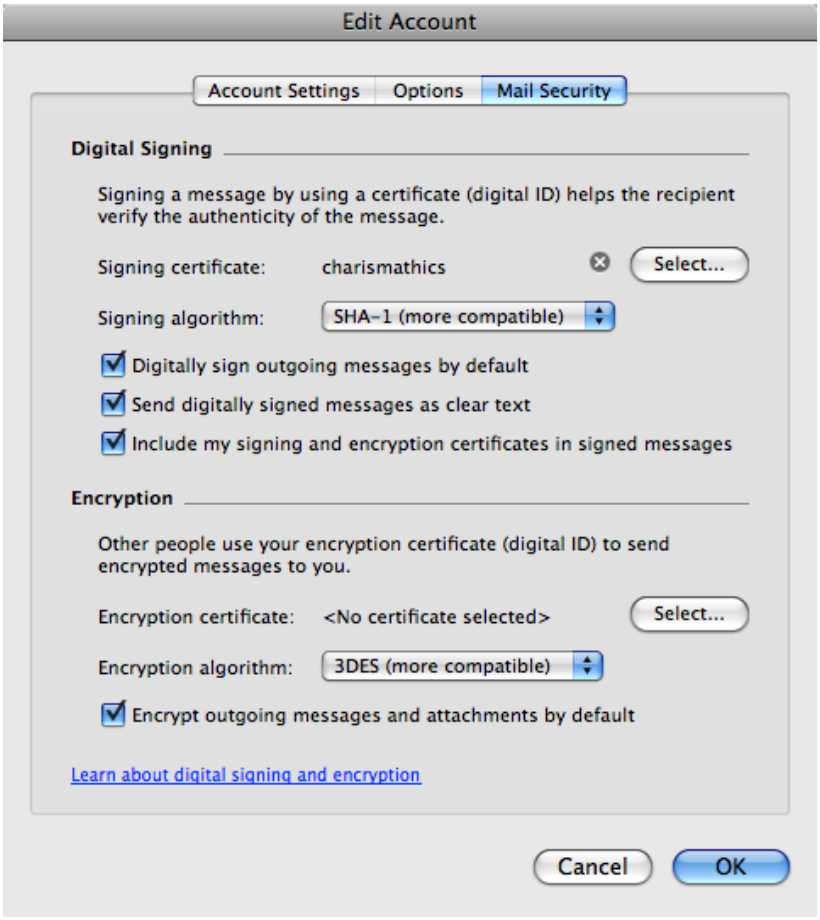
7.2 Configuring Entourage

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.



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...
Encryption algorithm:
3DES (more compatible)
Encrypt outgoing messages and attachments by default
Learn about digital signing and encryption
Cancel
OK