FUJITSU

THE POSSIBILITIES ARE INFINITE

Fujitsu mPollux DigiSign Client

Appendices

Fujitsu mPollux DigiSign Client Version 3.0

March 2010

Second Edition November 2009

Table of Contents

APPENDIX A: SETTING UP THE WINDOWS DOMAIN LOGON

To set up the windows domain logon:

1. Check that you are using Windows XP (or newer) server
2. Check that you are using active directory (AD)
3. Check that the CA service is available
4. Check that the Web enrollment procedure is available
5. Check that the Web enrollment station has suitable user rights for enrolling certificates
6. Check that the DigiSign Client CSP is installed on the Web enrollment station
7. Check that the smart card type for the DigiSign Client CSP has been added to the enrollment station
8. Check that the smart card type for the DigiSign Client CSP has been added to the end user's workstation
9. Store the smart card login enabling certificate on the chip card
10. Add the corresponding enterprise level CA's certificate to the domain active directory

For more information on how to set up a Microsoft Windows server, see http://msdn.microsoft.com.

APPENDIX B: TECHNICAL CHARACTERISTICS

The mPollux DigiSign Client 3.0 is compliant with the following platforms, features and standards:

1. Computing platforms

- Microsoft Windows XP
- Microsoft Windows 2003 32/64-bit
- Microsoft Windows Vista 32/64-bit
- Microsoft Windows 7 32/64 bit
- Microsoft Windows 2008 and 2008R2, 32/64 bit
- SUSE Enterprise Desktop 10.3 SP1
- Linux Red Hat Enterprise 5
- Ubuntu 7.10
- Mac OS X 10.4 (Tiger), x86
- Mac OS X 10.5 (Leopard), x86

2. Reader driver interfaces

- PC/SC

3. Smart Card operating systems

- MIOCOS v1.1 and newer for Atmel
- MIOCOS v2.3 for Fujitsu FRAM
- SetCOS 4.3.1, 4.3.2 and 4.4.1
- SetCOS for Java with EID applet
- Aventra MyEID Applet for JCOP
- Oberthur FINEID Applet

5. Interface standards

- CryptoAPI v2.0
- PKCS#11 v2.0

6. Other interfaces

- DigiSign Toolkit (DLL)
- Http interface to signature component
- Personal signer (ActiveX component)

7. Authentication methods

- Manual and automated PIN

8. Supported cryptographic algorithms

- RSA with key generation
- MD5, SHA (several variants)
- RC-2, DES, 3-DES, AES

APPENDIX C: TECHNICAL ARCHITECTURE

Client components and how to use them

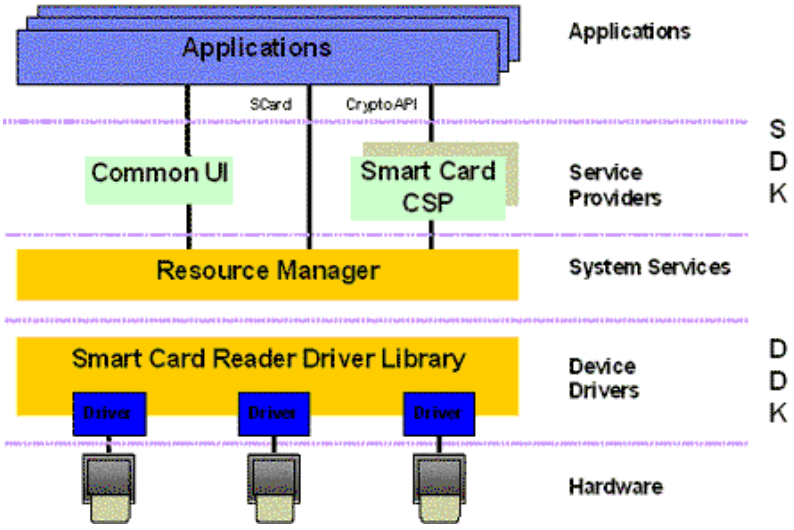
The mPollux DigiSign Client comprises three components:

- Microsoft CryptoAPI compliant CSP
- PKCS#11 interface (RSA Laboratories, Public Key Cryptography Standards)
- Integrated Certificate Loader and DigiSign Client Manager

1.1 DIGISIGN CLIENT CSP INTERFACE

CSP (Cryptographic Service Provider) is an interface that forms part of Microsoft's cryptographic computing interface CryptoAPI (or CAPI). It offers the possibility to add new cryptographic devices and algorithms.

The DigiSign Client CSP interface offers a suitable and simple solution for initializing, personalizing and using smart cards.



The cryptography system semantics of the CryptoAPI define the key containers accessed through CSP. These containers hold the cryptographic keys and certificates.

In addition, Microsoft Windows has its own separate certificate memory, which is the major certificate memory in Windows. This means that the smart card certificates are located in two places.

Windows based applications usually cannot use certificates that are located inside CSP; CryptoAPI does not automatically add CSP certificates to the certificate storage. An integrated certificate loader and management tool is therefore required when using the CSP interface.

The DigiSign Client package includes a Certificate Loader for managing certificates. This tool enables the loading of CSP located certificates into the Windows certificate memory in order to ensure that the certificates are available for use.

The user interface of Certificate Loader is located on the task bar, as described in chapter 1.1.

The following icons are used to inform the user of the current status (the first icon on the upper left corner in the following figures):

Waiting for a smart card to be inserted into the reader:

Reading smart card data content:

The card is ready to use:

1.2 DIGISIGN CLIENT PKCS#11 INTERFACE

Cryptoki (Cryptographic Token Interface) is another commonly used cryptographic interface. It is defined by RSA Laboratories in accordance with Public Key Cryptographic Standard number 11 (PKCS#11). This standard is designed for any cryptographic computing device and therefore differs from CSP. The interface is not integrated with Microsoft Windows' own certificate system.

PKCS#11 interface provides the same compliancy with smart cards, smart card data content profiles and computer platforms as CSP, including card personalization and management features.

The smart card can be used with both DigiSign Client interfaces (CSP and PKCS#1). These interfaces may be used simultaneously, which offers good compliancy with many computer applications, such as VPNs, browsers etc.

1.3 WHAT IS 'AUTOMATED AUTHENTICATION'?

DigiSign Client architecture is designed based on the rules of smart card access condition management. The DigiSign client software therefore includes a mechanism called 'Automatic Authentication'.

Automatic authentication guarantees that

- the user PIN query is handled easily and securely.
- several PIN code and certificate combinations can be stored on one smart card. DigiSign automatically selects or lets the user choose the required combination.
- information on a web authentication is shared with all of the applications.

In practice, this means that the user is authenticated only when the smart card demands it.

APPENDIX D: DIGISIGN REGISTRY VALUES

[HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\DigiSign Client]

Unless otherwise stated, the default value is '0'.

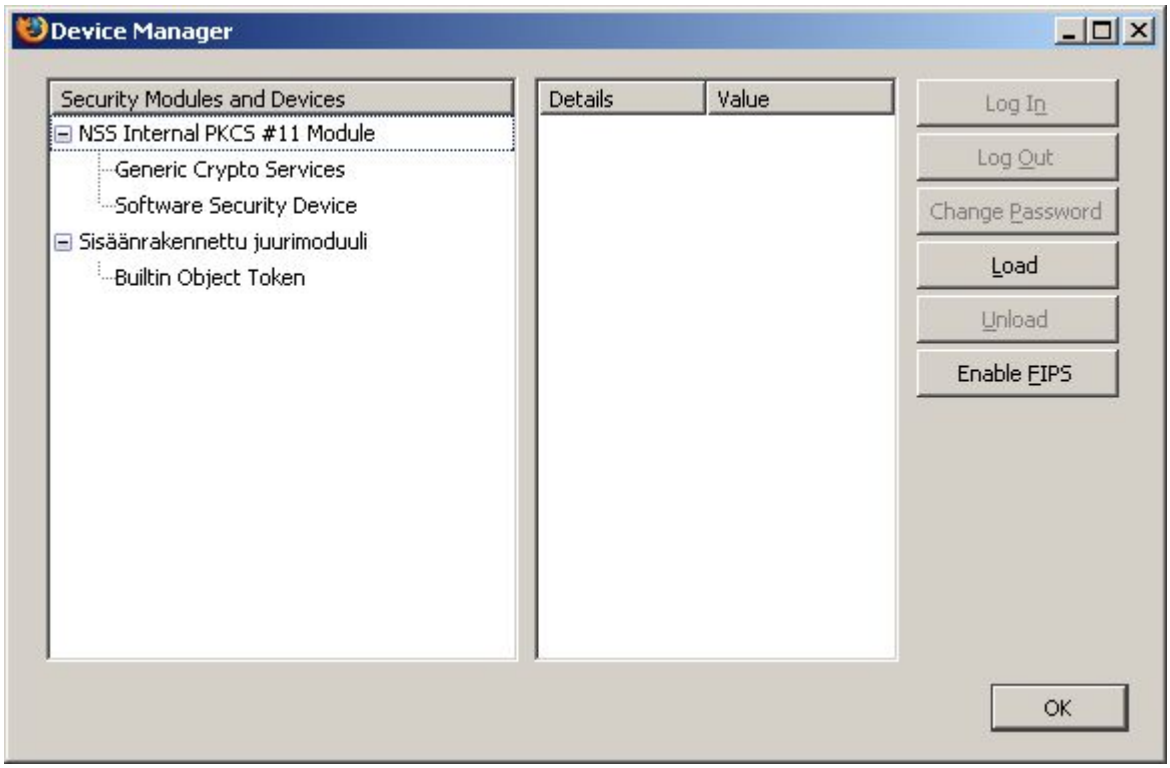
Type	Value and explanation
SmartCardCacheKeep	if set to '1', the smart card cache is not removed from the hard disk
SmartCardCachePath	location of smart card cache
disableNonRepPurpose	Microsoft certificate option: by default, the non repudiation certificate purpose is set to 'none'
doNotUseSmartCardCache	smart card cache is used by default
pkcs15crt	if set to '0', the new keys are saved on the card without CRT components
keyGenCheatMode	CSP option: if set to '1', the new keys are never generated for the card during enrollment
closeBrowsers	if set to '1', all web browsers that have used DigiSign Client will be closed
excludeReader	if set, the reader is excluded from the smart card reader list
safeMode	if set to '1', the presence of the smart card is checked regularly to ensure that removal of the card is detected Do not use this option if the card reader detects removal actions with the default settings
addCertFriendlyName	if set to '1', friendly names are added to the certificates
acceptEmptyPIN	if set to '1', empty PINs are accepted
closeBrowserExcludeReader	if defined, this reader is excluded when the card is removed from the reader. See 'closeBrowsers'.
SmartCardSNCache	if set to '1', the card data is cached in a file named with the card serial number
userLevel	DigiSign Manager modes: '0' (default) - advanced features are hidden '1' - advanced features are displayed '2' – as '1', but with object deletion feature
disableCryptokiAutoLogin	if set to '0', the cryptoki-interface is flagged to indicate that login is not required. When the PIN is required, cryptoki opens a PIN query dialog.

APPENDIX E: DIGISIGN CONFIGURATION FOR MOZILLA FIREFOX AND MOZILLA THUNDERBIRD IN WINDOWS

Using DigiSign with Mozilla Firefox 2.0 or Mozilla Thunderbird requires the following configuration. The screenshots may differ from what you see on screen, depending on your software version.

Firefox

1. Select ‘Options…’ from the Tools menu
2. Select the Advanced tab at the top of the dialog that appears
3. Select Encryption (Firefox) or Certificates (Thunderbird)
4. Select Security devices. The following window opens:



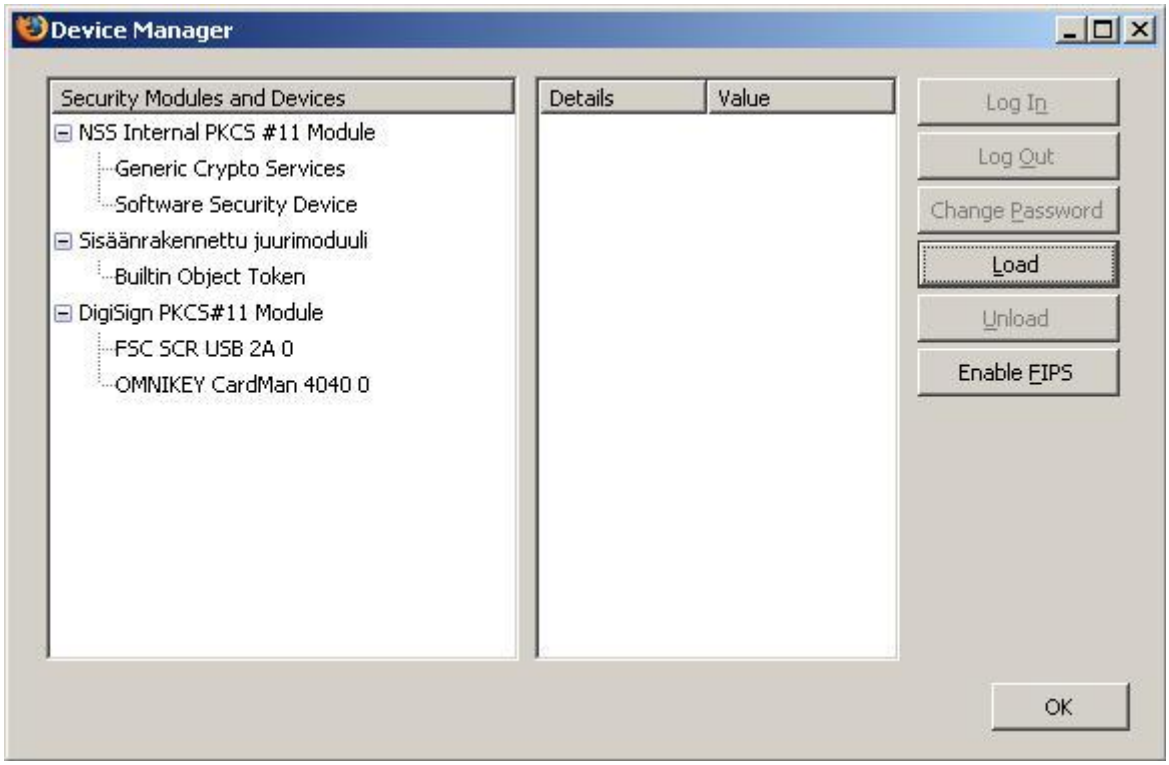
5. Click ‘Load’ on the right hand side, and the following dialog box opens:

6. Change the Module name to ‘DigiSign PKCS#11 Module. Click ‘Browse’ and select the Cryptoki.dll file in your DigiSign installation folder (default is ‘C:\Program Files\Fujitsu Services\mPollux DigiSign Client’). Click ‘OK’.

7. Confirm the installation of the security module by clicking ‘OK’.

8. Click on ‘OK’ to close the alert message.

9. You should now see the DigiSign PKCS#11 Module, with your smart card reader under it. Click ‘OK’ to close the window.

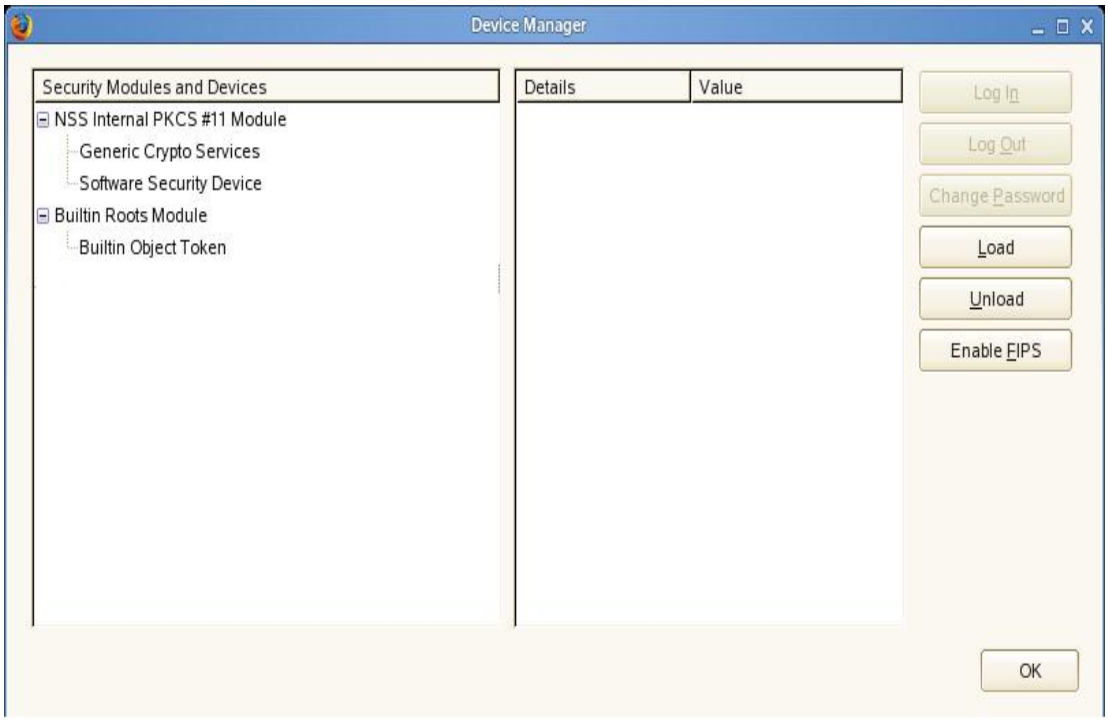


APPENDIX F: DIGISIGN CONFIGURATION FOR MOZILLA FIREFOX 2.0 AND MOZILLA THUNDERBIRD IN LINUX

Firefox

Modify the Mozilla Firefox web-browser to use the DigiSign PKCS#11 module. The screenshots may differ from what you see on screen, depending on your software version.

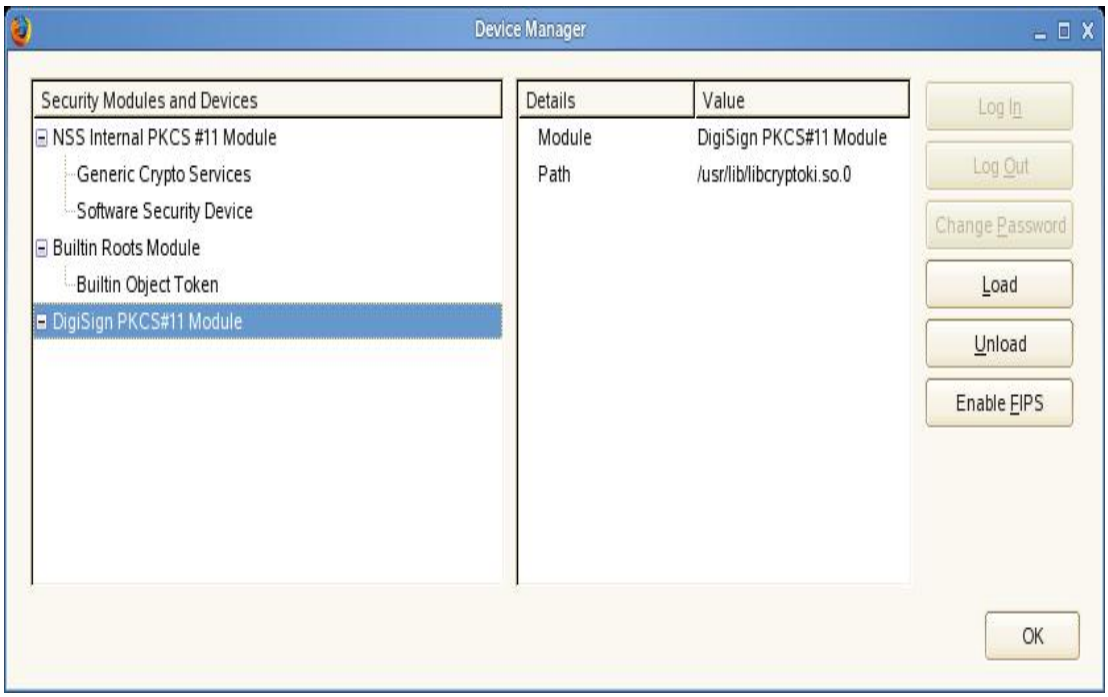
1. Select ‘Preferences’ from the Edit menu
2. Select the Advanced tab at the top of the window that appears
3. Select the Encryption tab.
4. Select Security devices. The following window opens:



5. In this Device Manager window, load a new DigiSign PKCS#11 module by clicking the Load button.

6. The following dialog opens. Enter a new name for the module (for example DigiSign PKCS#11 Module). Click browse to select the correct module, which is libcryptoki.so.0. The correct path is `/usr/lib/`libcryptoki.so.0

7. Once the selected libcryptoki.so.0 module has been loaded, click the 'OK' button to close the dialog. The libcryptoki.so.0 module has then been added successfully.

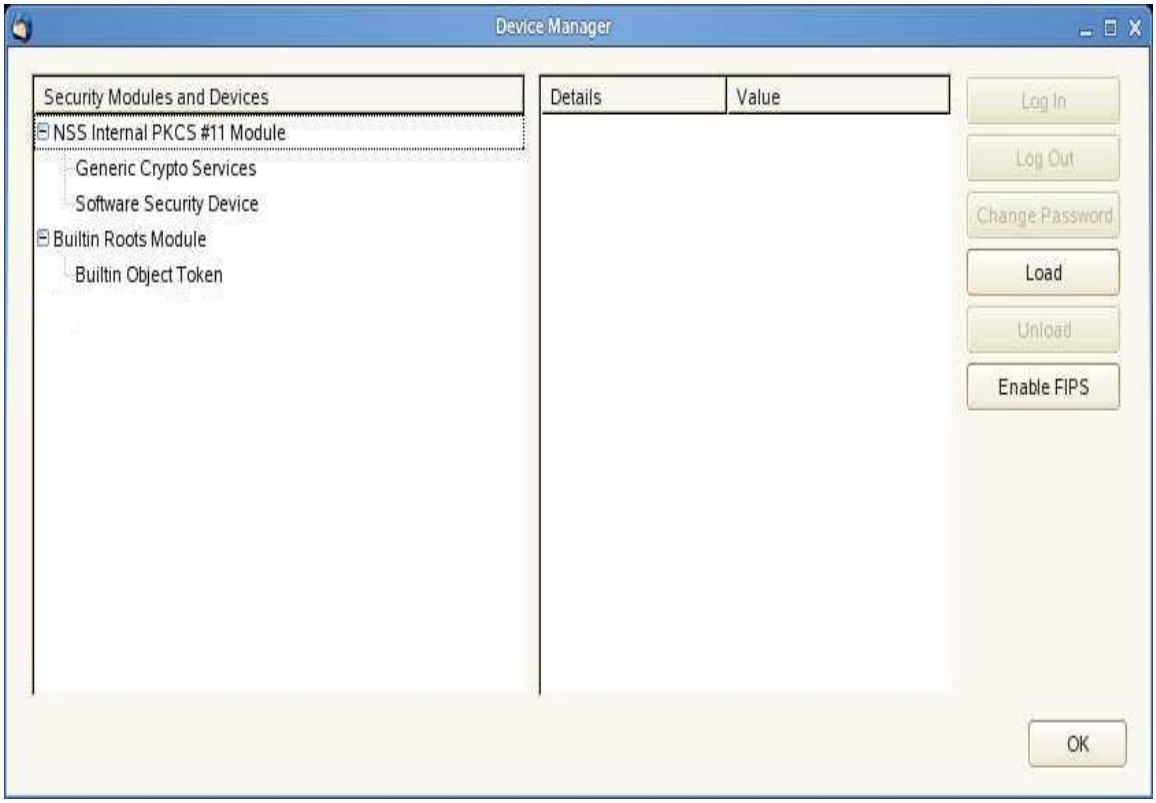


Thunderbird

Modify the Thunderbird e-mail client to use the DigiSign PKCS#11 module. The screenshots may differ from what you see on screen, depending on your software version.

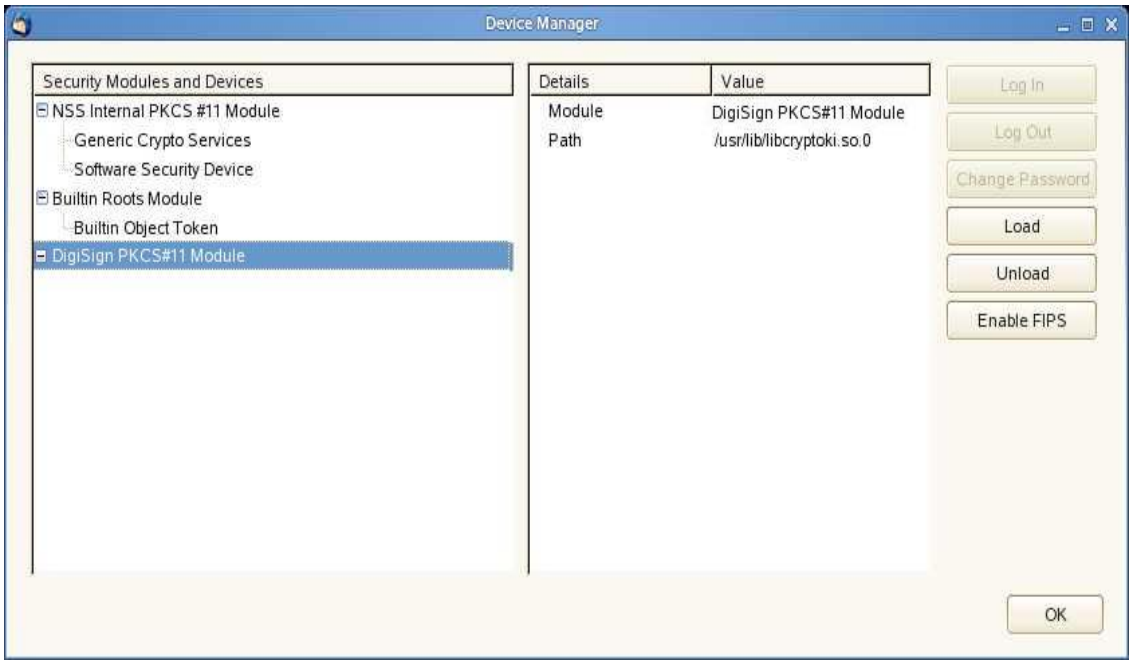
1. Select ‘Preferences’ from the Edit menu
2. When the Thunderbird preferences window opens, select Privacy and the Security tab. Then click the Security Devices button.

3. In the Device Manager window that appears, load a new DigiSign PKCS#11 module by clicking the Load button.

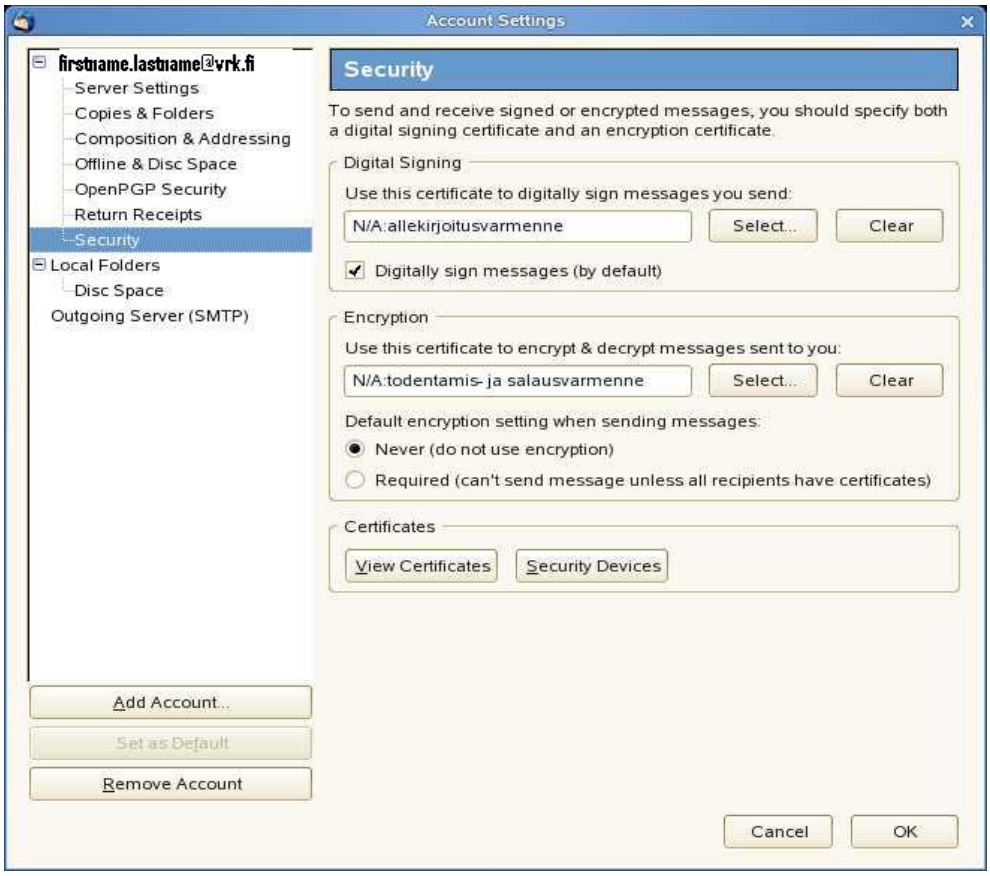


4. The following window opens. Enter a new name for the module (for example, DigiSign PKCS#11 Module). Click browse to select the correct module, which is libcryptoki.so.0. The correct path is `/usr/lib/`libcryptoki.so.0

5. Once the selected libcryptoki.so.0 module has been loaded, click the 'OK' button to close the dialog. The libcryptoki.so.0 module has then been added successfully.



6. To add the required Digital Signing and Encryption Certificates to the Thunderbird e-mail client, select Edit and then Account Settings from the drop-down list. When the Account Settings window opens, select *Security* and then add the Digital Signing and Encryption Certificates. Then click the 'OK' button. The Digital Signing and Encryption Certificates have then been added successfully.



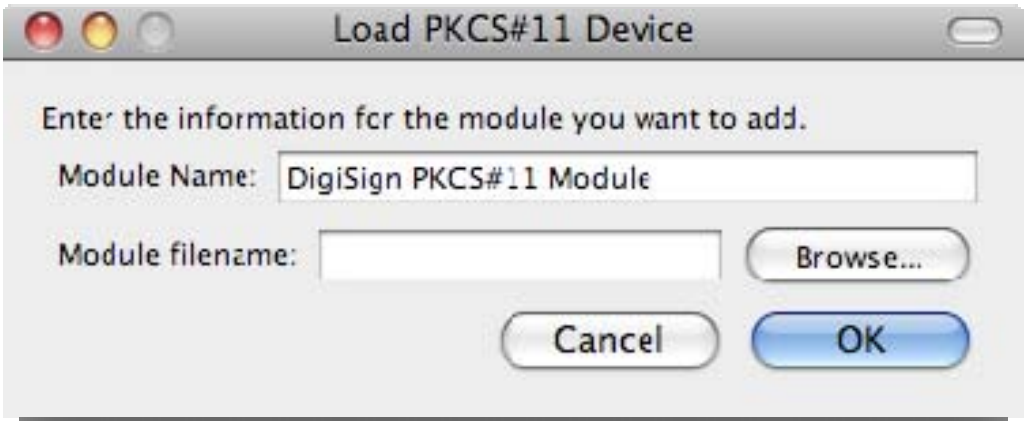
APPENDIX G: DIGISIGN CONFIGURATION FOR MOZILLA FIREFOX 2.0 AND MOZILLA THUNDERBIRD IN MACOS

Using Mac DigiSign with Mozilla Firefox 2.0 and Thunderbird 2.0 requires the following configuration. To update Firefox and Thunderbird to use the DigiSign PKCS#11 module, perform the following steps. The screenshots may differ from what you see on screen, depending on your software version.

Firefox

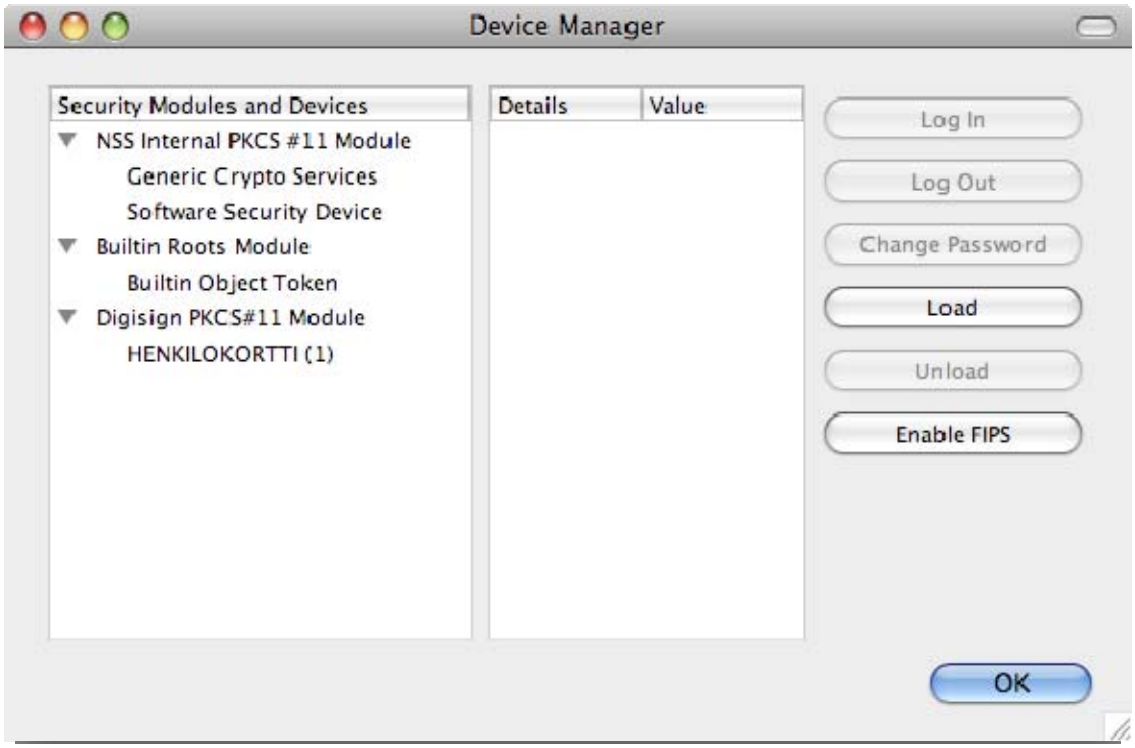
1. Select 'Preferences' from 'Firefox' menu or 'Thunderbird' menu (depending on which application you are updating)
2. Select 'Advanced' tab at the top of the window
3. Select 'Encryption' tab.
4. Select 'Security Devices'. You should see the following window:

5. In the Device Manager pop-up window, obtain a new DigiSign PKCS#11 module by clicking the button 'Load'. This opens a Load PKCS#11 Device pop-up window. In the window, enter a new module name (for example 'DigiSign PKCS#11 Module'), enter the path and name of the correct module (which is /Library/mPolluxDigiSign/lib/libcryptoki.1.dylib) and press 'OK'. Please note that using the Browse button may produce incorrect results.



6. The install program will ask for confirmation. Press ‘OK’.

The module has been added successfully.

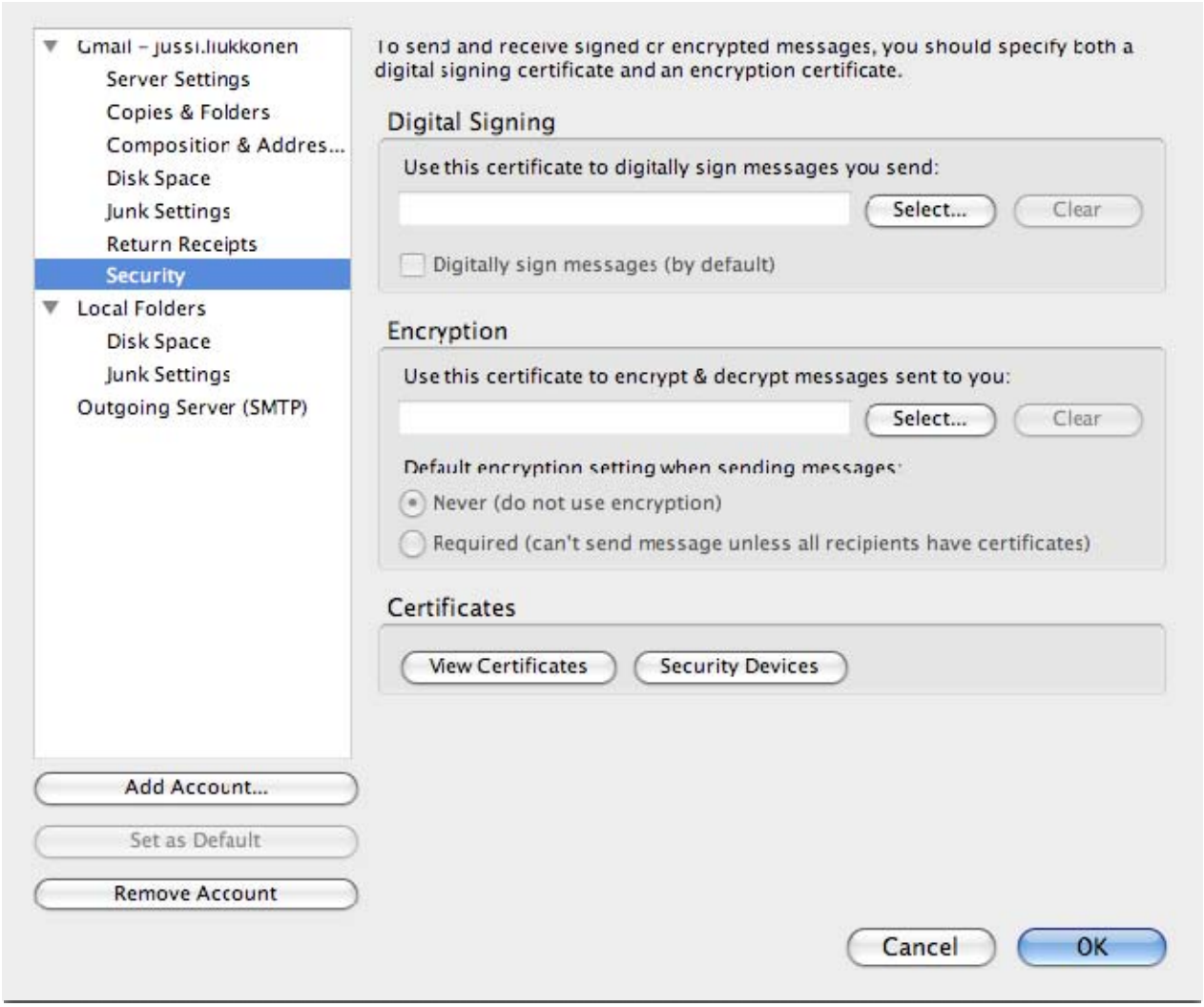


Selecting Certificate Authorities in Thunderbird in Mac.

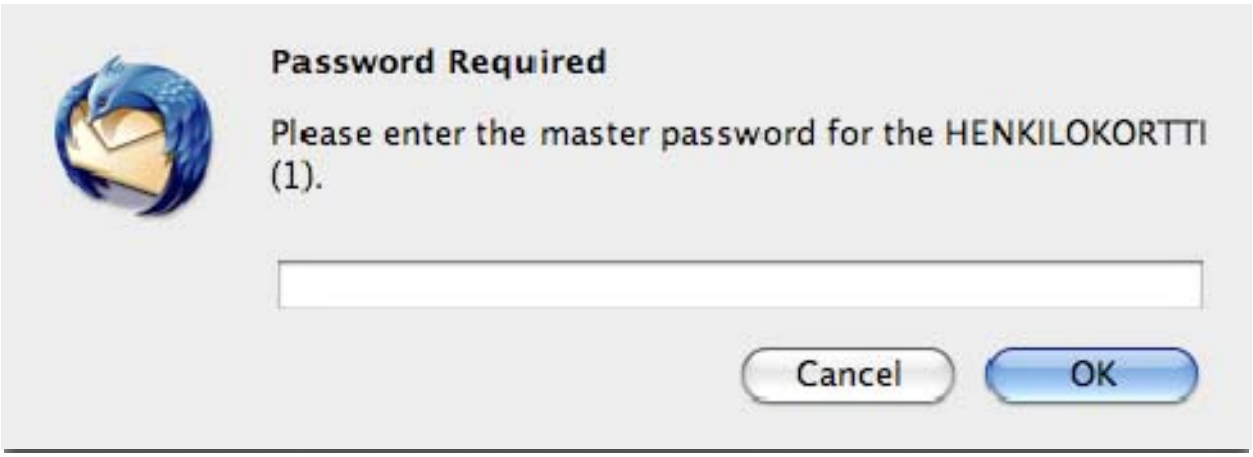
To select the certificate Authorities for Thunderbird e-mail client in Mac, do the following:

Ensure that your card is inserted in the reader before configuration.

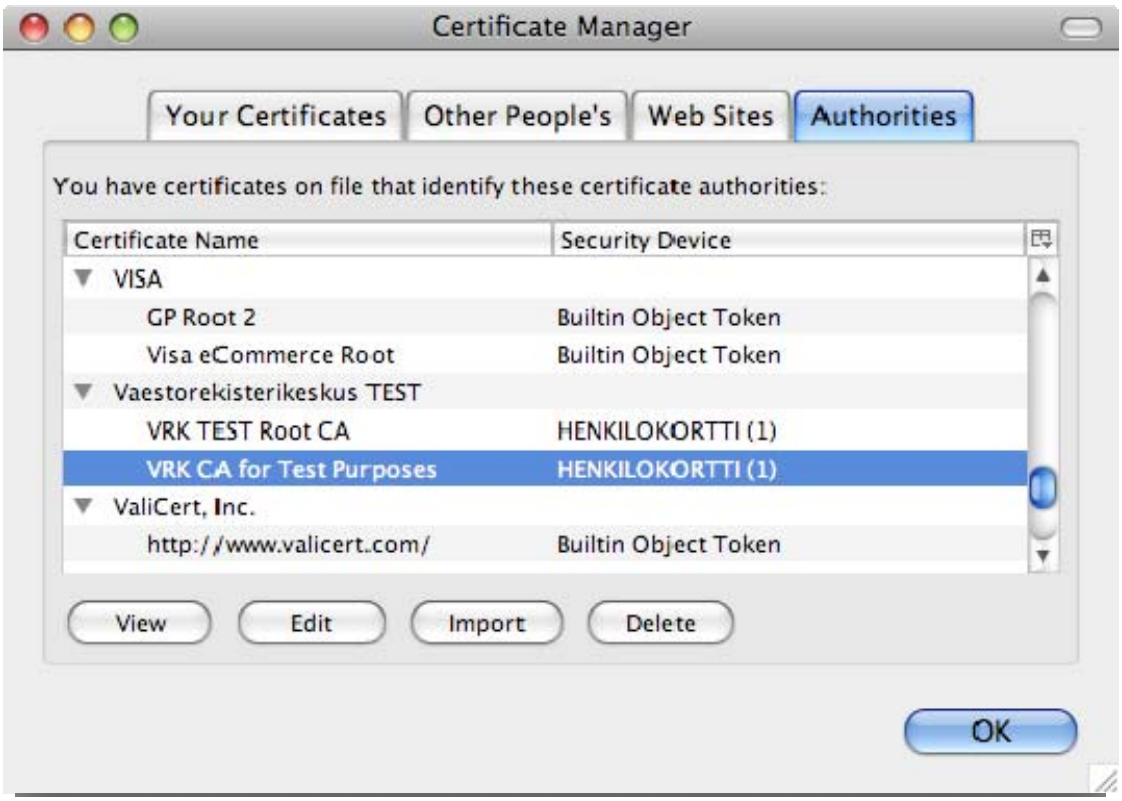
1. Select ‘Account Settings’ from the ‘Tools’ menu and, from there, select ‘Security’ (under correct account).



2. Select ‘View Certificates’. This requests the master password for the certificate on the card.



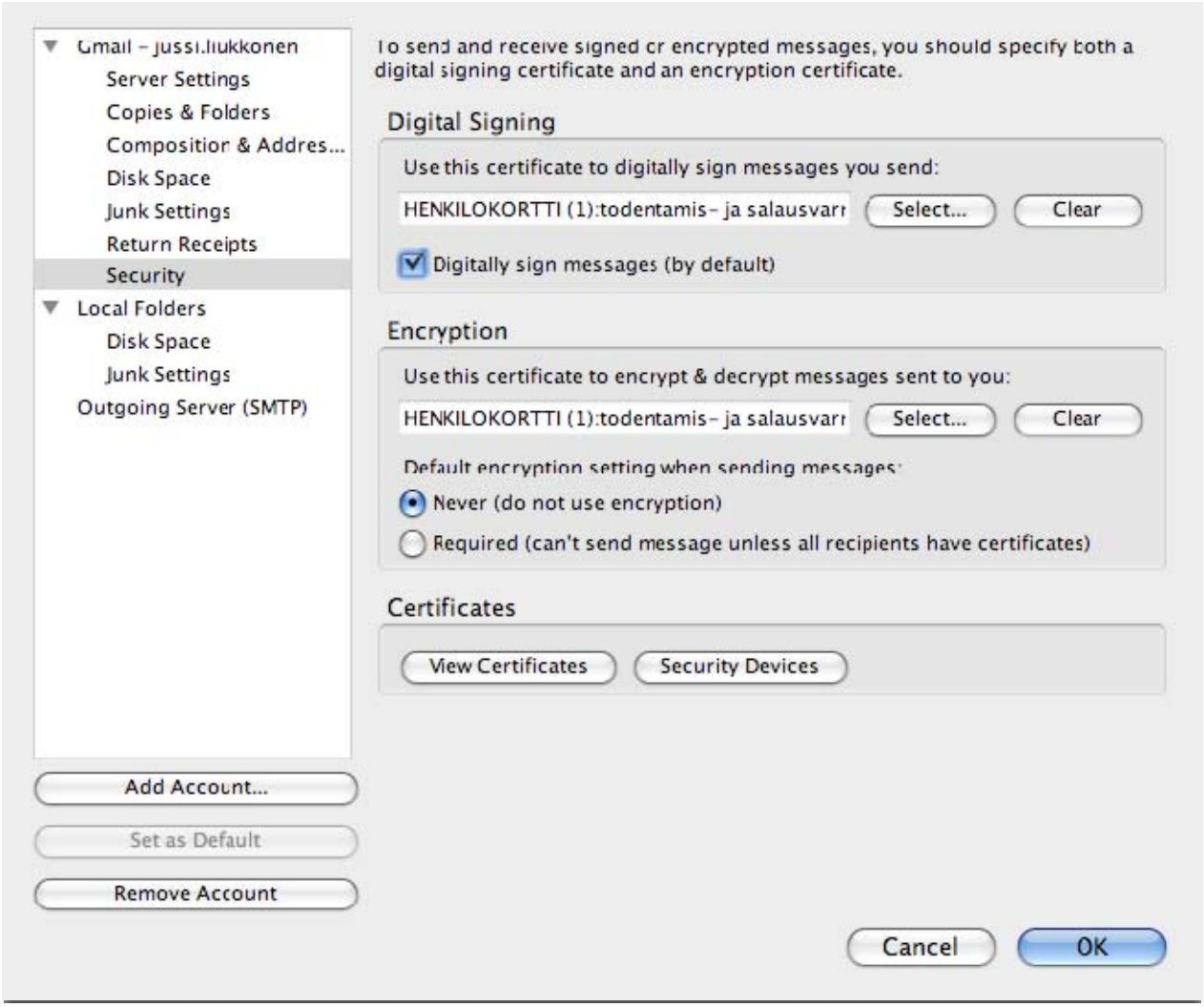
3. Enter the card's PIN code and press 'OK'. The Certificate Manager pop-up opens. Select the tab 'Authorities'.



4. Select the certificate 'Väestörekisterikeskus VRK Gov CA Citizen Qualified Certificate'.

5. Edit the CA certificate trust settings by clicking the 'Edit' button.

6. Select 'This certificate can identify mail users' and click the 'OK' button. 'Certificate Authorities' has been identified successfully.



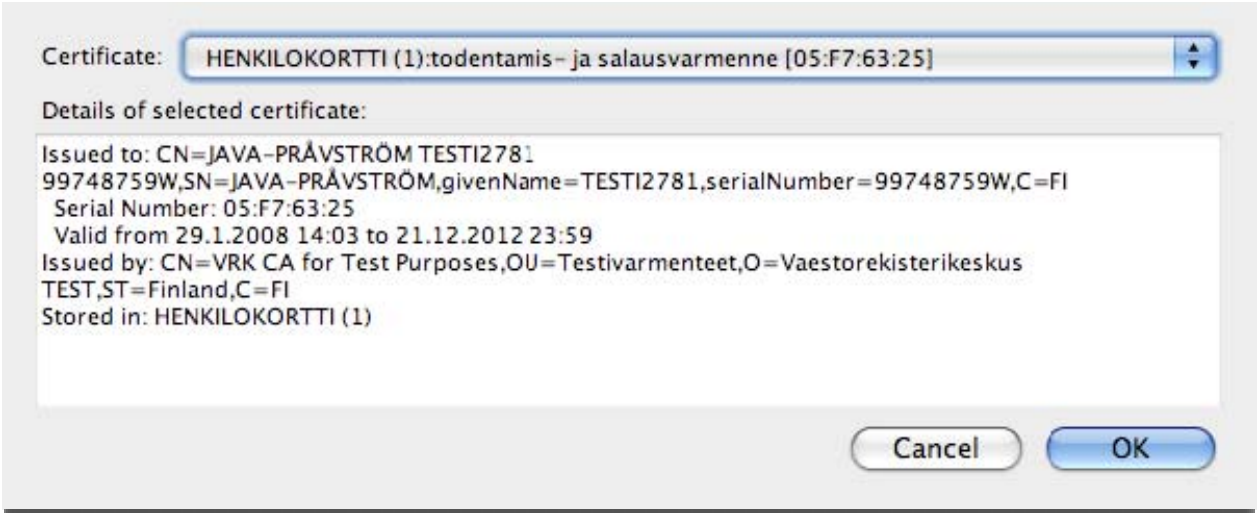
Selecting Digital Signing Certificate in Thunderbird in Mac.

To select a Digital Signing Certificate for a Thunderbird e-mail client, perform the following steps.

1. Select Account settings from the ‘Edit’ menu.

2. In the pop-up window Account settings, select ‘Security’.

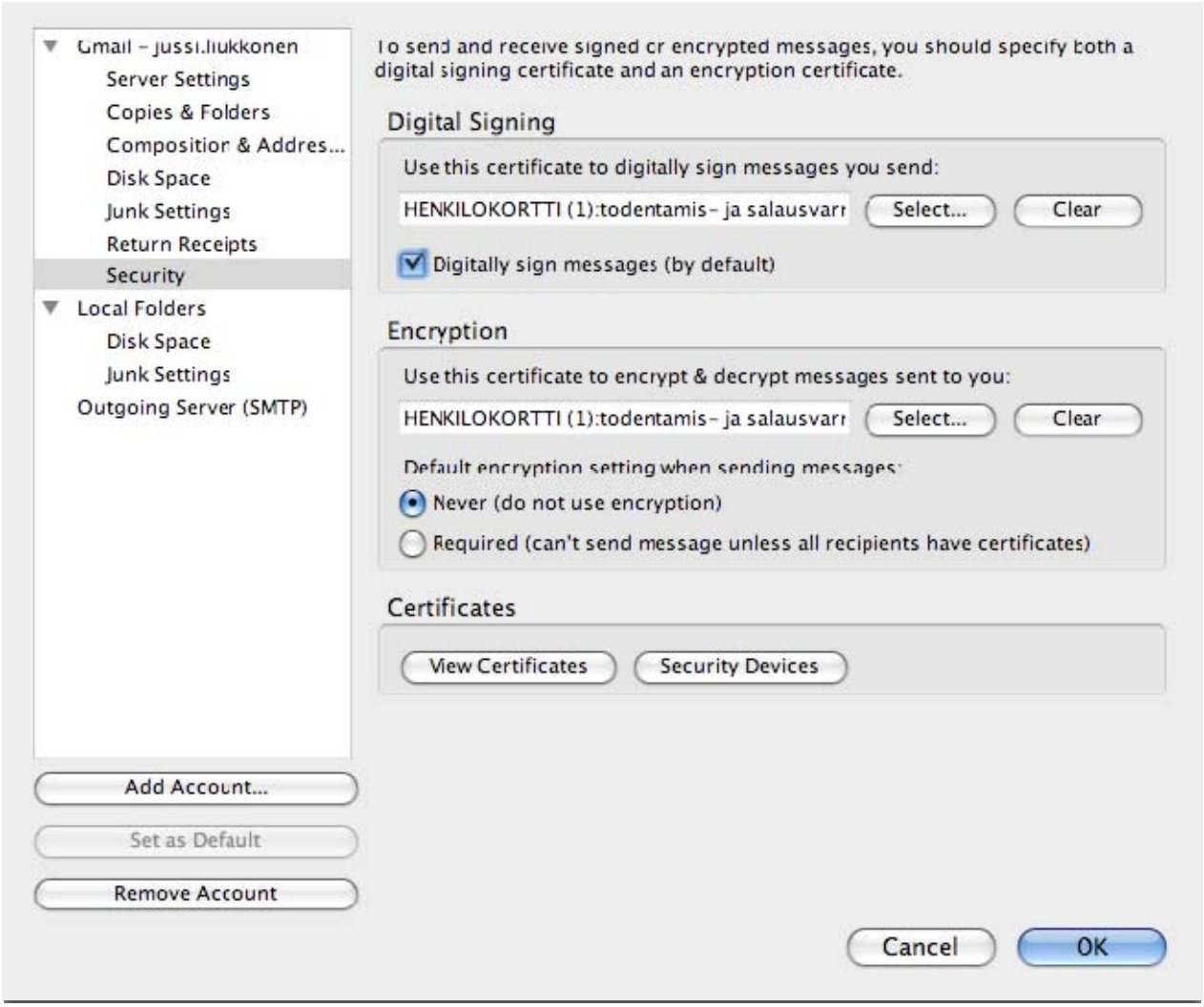
3. In the Digital Signing section, ‘Use this certificate to digitally sign messages you send’, click the ‘Select’ button and a pop-up window ‘Select Certificate’ will open.



4. Select the Digital Signing certificate and click the 'OK' button. Next, the application will ask whether this certificate should be used in encryption. Click 'Cancel'.

5. Check the 'Digitally sign messages (by default)' checkbox.

Now, the Digital Signing certificate has been added successfully and is in use.



Selecting an Encryption certificate in Thunderbird in Mac.

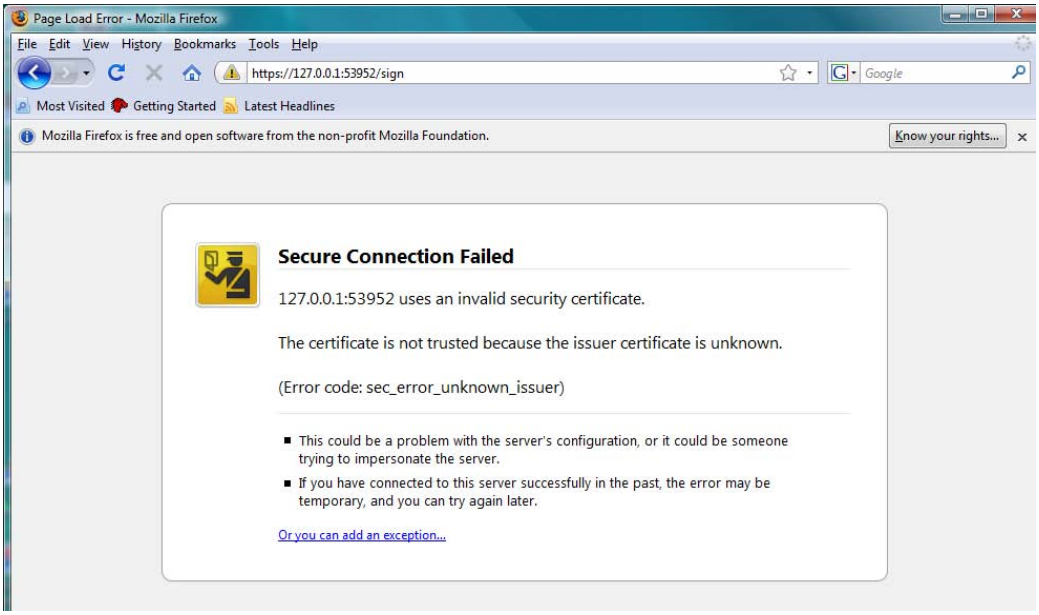
To select an Encryption certificate for a Thunderbird e-mail client, perform the following steps (similarly to selecting a Digital Signing certificate).

1. Select ‘Account Settings’ from the ‘Edit’ menu.
2. In the pop-up window Account settings, select ‘Security’.
3. In the Digital Signing section, ‘Use this certificate to encrypt & decrypt messages sent to you’, click the ‘Select’ button and a pop-up window 'Select Certificate' opens.
4. Select an Encryption certificate and click the ‘OK’ button.
5. Select the default encryption setting according to your preferences. If you select ‘Never’ you can still send encrypted mail, but this is not the default. If you choose ‘Required’, you will always send messages encrypted and in every case must have certificates for all recipients.

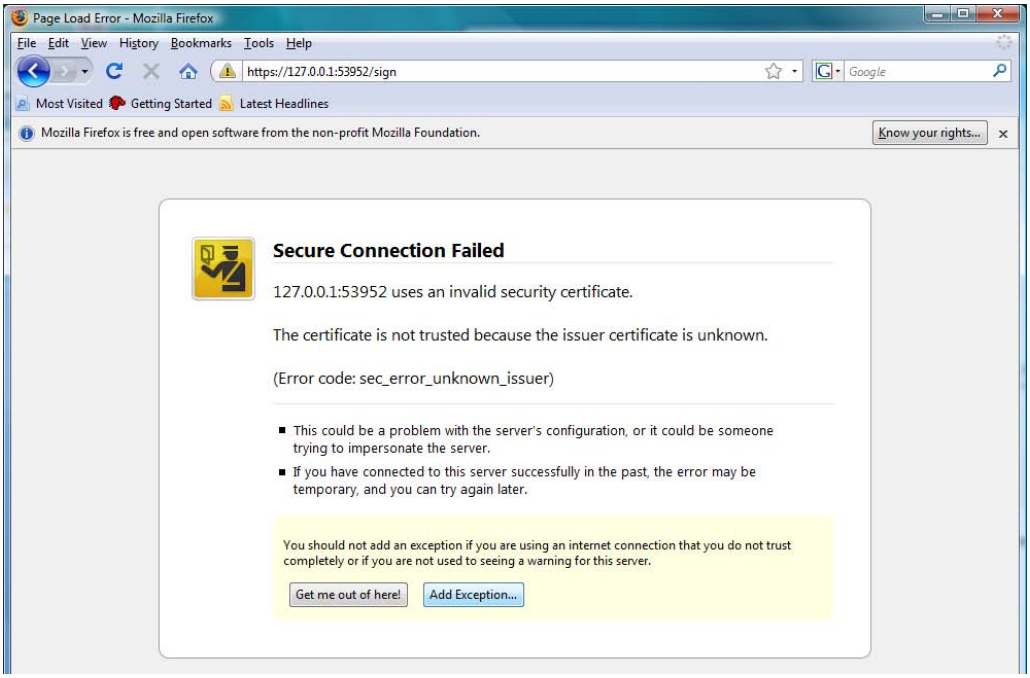
APPENDIX H: FIREFOX 3 CERTIFICATE EXCEPTION

To sign documents in Firefox with DigiSign you have to add certificate exception for the local signer component as follows:

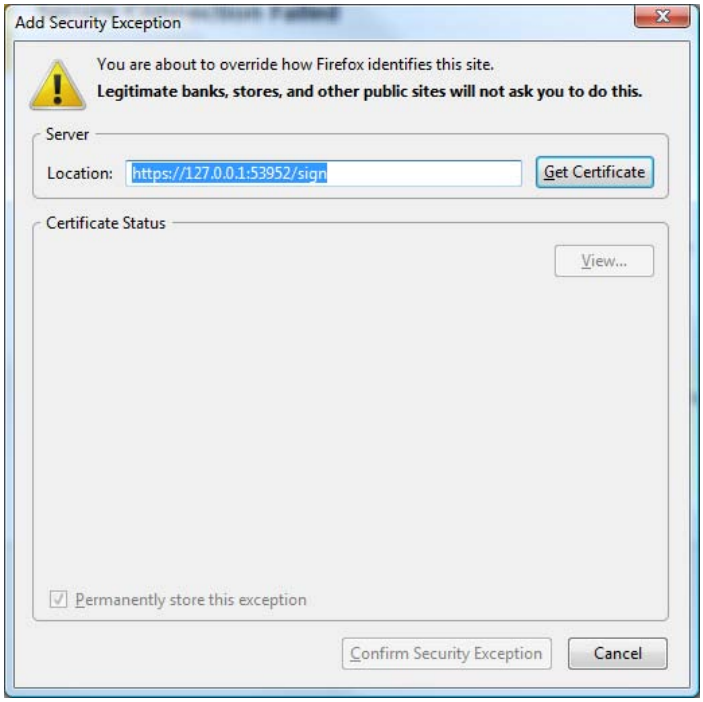
1. Browse to address https://127.0.0.1:53952/sign
2. You should obtain a window as shown below. Click on 'Or you can add an exception…'



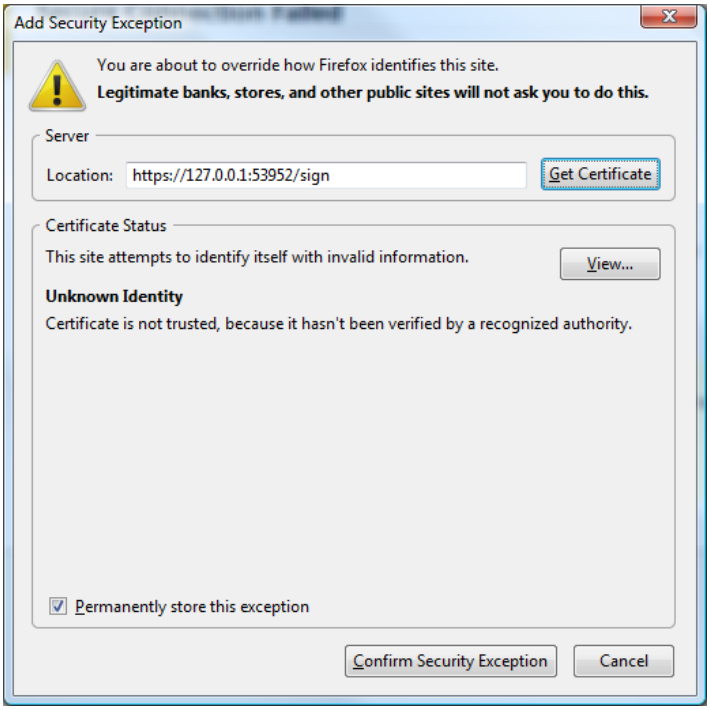
3. 3. Click 'Add Exception' button.



4. Click ‘Get Certificate’ button.



5. Click ‘Confirm Security Exception’



APPENDIX H: DIGISIGN TOOLKIT

DigiSign toolkit is an interface offering wide collection of functions for software developer.

Please notice that interface deliveries are not included in all releases.

If header and library files are present, they are located under *toolkit*-directory.

Toolkit includes following features:

- Functions to search user certificates
- Compute and verify signatures
- Authenticate against mPollux server
- Verify, change and unblock PIN codes
- Initialize and manage smart card data content
  - Add and remove keys, certificates and data objects
- Get callbacks of card insert and removal events
- Transmit CMP messages to different CA systems