



County of Los Angeles
Department of Mental Health

Contract Providers Transition Project
(CPTP)

Electronic Data Interchange (EDI)
SECURITY AND ACCESS

Version 1.3

August 2008

DOCUMENT REVISION HISTORY

| Version | Release Date | Revised by | Comments/Indicate Sections Revised |
|----------------|---------------------|-------------------|---|
| Revised v 1.3 | 08/15/2008 | Calvin Phan | Added Section 6 |

Table of Contents

| | | |
|----------|--|-----------|
| 1 | EDI SECURITY AND ACCESS OVERVIEW | 1 |
| 2 | HOW TO IMPORT A DIGITAL CERTIFICATE INTO INTERNET EXPLORER | 1 |
| 3 | HOW TO IMPORT A DIGITAL CERTIFICATE INTO NETSCAPE NAVIGATOR..... | 5 |
| 4 | TEST YOUR CERTIFICATE | 12 |
| 4.1 | NETSCAPE NAVIGATOR USERS | 12 |
| 4.2 | INTERNET EXPLORER USERS | 14 |
| 5 | HOW TO REMOVE YOUR DIGITAL CERTIFICATE..... | 16 |
| 5.1 | INTERNET EXPLORER USERS | 16 |
| 5.2 | NETSCAPE NAVIGATOR USERS | 18 |
| 6 | HOW TO CHECK THE EXPIRATION DATE OF THE DIGITAL CERTIFICATE | 21 |

1 EDI Security and Access Overview

The security and controls required to transmit Personal Health Information (PHI) over the internet are defined by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 under the Privacy and Security standards. DMH and its trading partners are covered entities under HIPAA and must adhere to these standards for all electronic data exchanged (EDI) over the internet or County intranet. In order to provide secure data exchange, DMH has established security and access controls for all EDI transmissions.

As part of the EDI certification process, DMH will issue each trading partner a special code that will be installed by the trading partner. The special code is referred to as a Digital Certificate. The Digital Certificate will be used to verify that the trading partner is actually the organization authorized to send EDI transactions to DMH. Without the correct information, EDI information will not be transmitted.

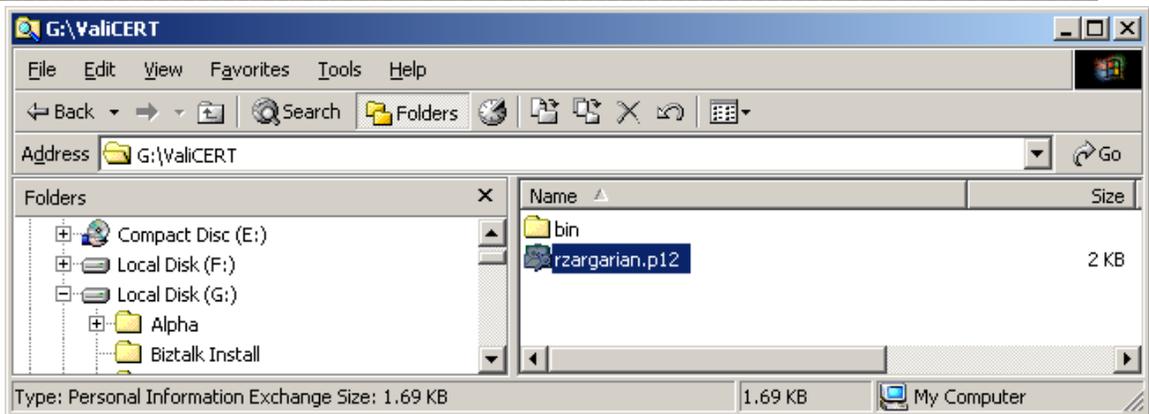
The EDI data is also coded (referred to as encrypted) to provide another level of security. The encrypted data will only be understood by trading partners with the correct validation or decoding tools. To begin testing, each trading partner will be issued a Test Digital Certificate. Once the trading partner is ready to send Production EDI transactions, a Production Digital Certificate will be issued.

This document describes the process to install and remove the digital certificates that are used for testing EDI and also for production submission of EDI transactions. All digital certificates are currently set to expire in the year 2010 and must be renewed prior to that date.

2 How to import a Digital Certificate into Internet Explorer

These procedures are to be performed by the clients who received their Certificates from DMH authorized staff (EDI Certification Group).

Once you receive your client certificate, save it (*username.p12* file) in a local disk on the workstation.

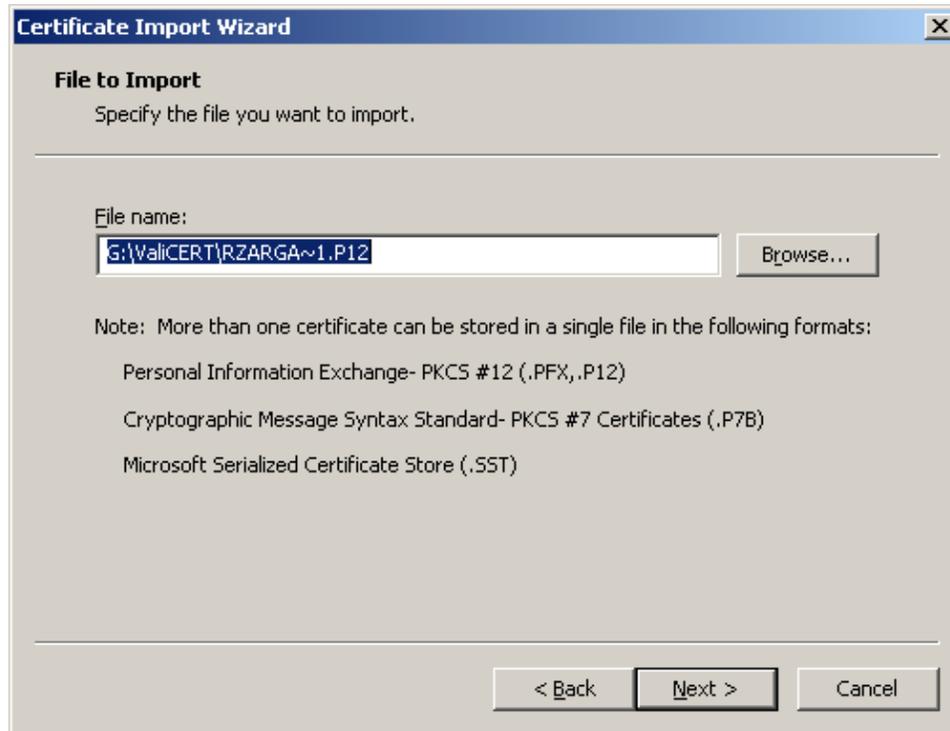


Open the Windows Explorer, navigate to where the file is saved and double click the file.

A Certificate Import Wizard will guide you. Click Next on the Welcome screen.

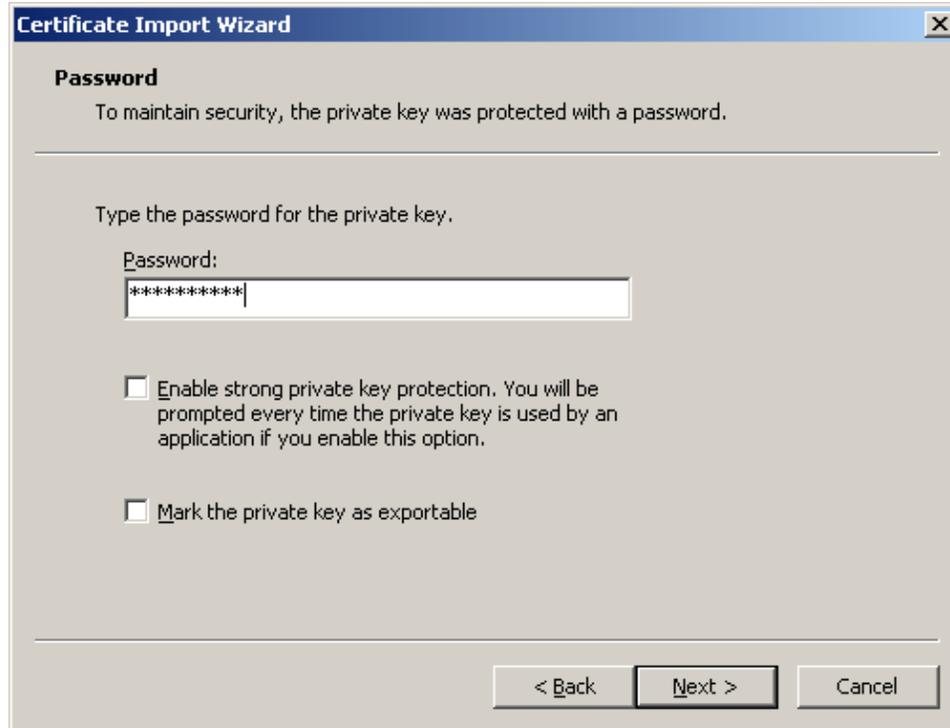


The wizard will fill in the field for the location of the file. Verify the path and click Next.



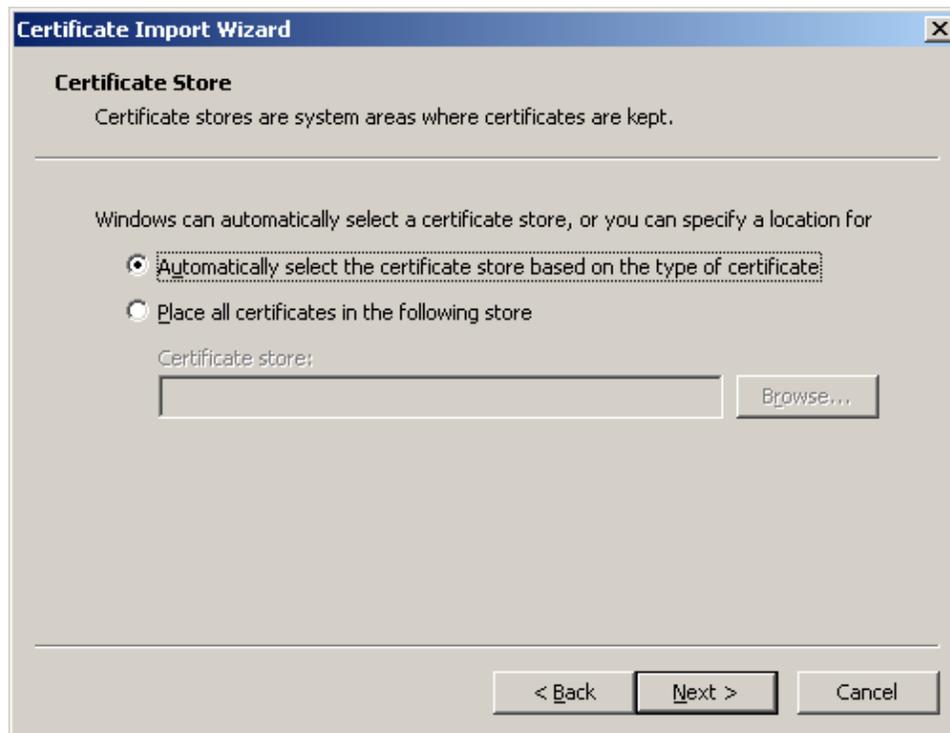
Enter the password that you have received along with your certificate file. Click Next.

DO NOT SELECT ANY OTHER OPTION ON THIS SCREEN.



Leave the default location for the certificate. Click Next.

DO NOT CHANGE ANYTHING ON THIS SCREEN.



The certificate will be installed. Click Finish to complete the installation.



A message will inform you that the certificate was imported. Click OK.

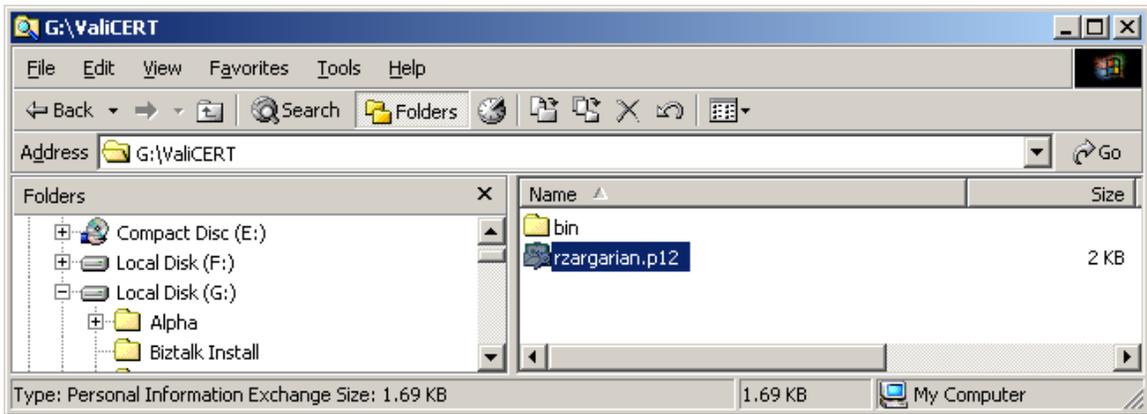


3 How to import a Digital Certificate into Netscape Navigator

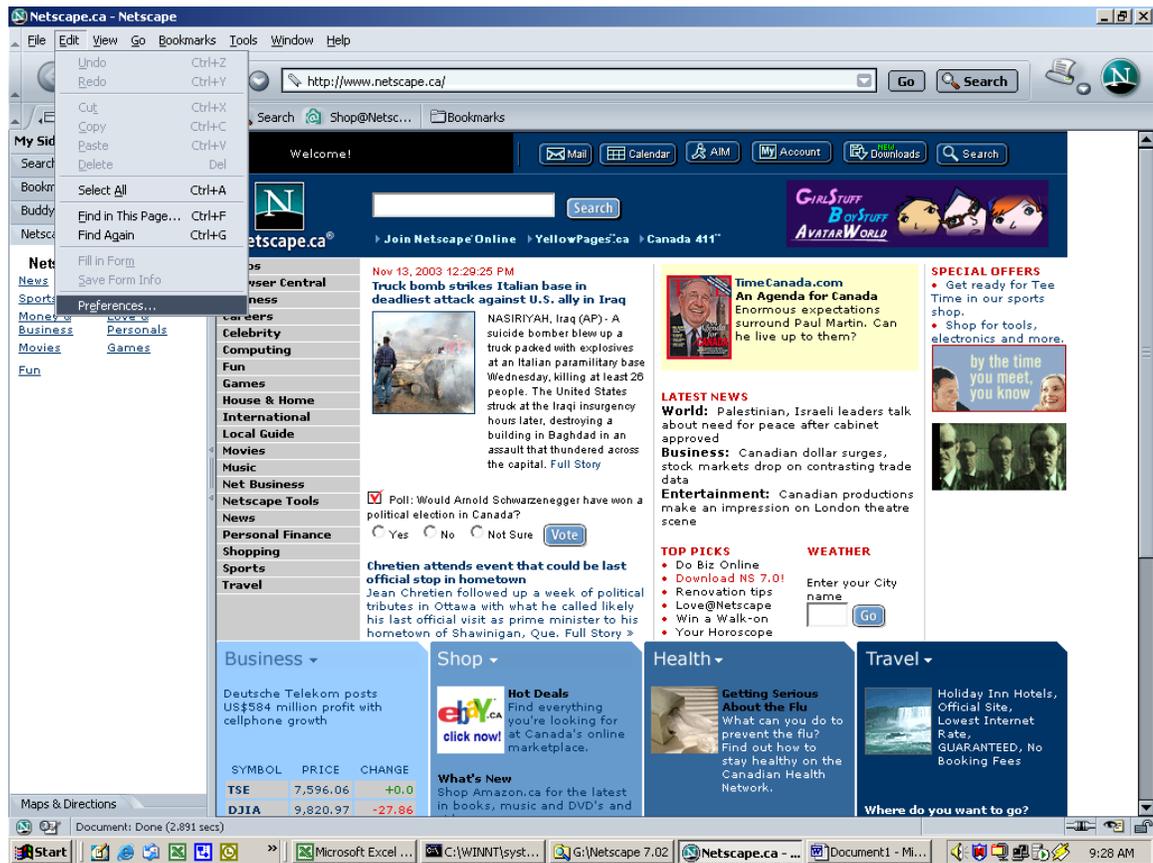
The Netscape Navigator used for this instruction is 7.02.

These procedures are to be performed by the clients who received their Certificates from DMH authorized staff (Integrated Systems Application Administrator).

Once you receive your client certificate, save it (*username.p12* file) in a local disk on the workstation.



Start the Netscape Navigator.
From the menu, select Edit > Preferences.



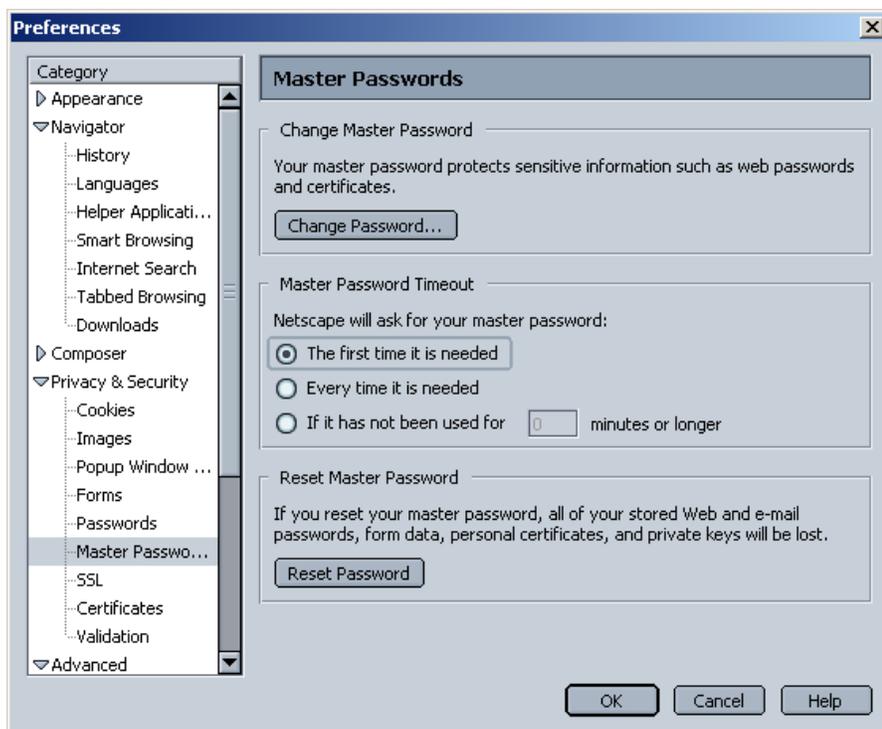
Click on the small triangle next to “Privacy & Security” option.

Select the “Master Password” option.

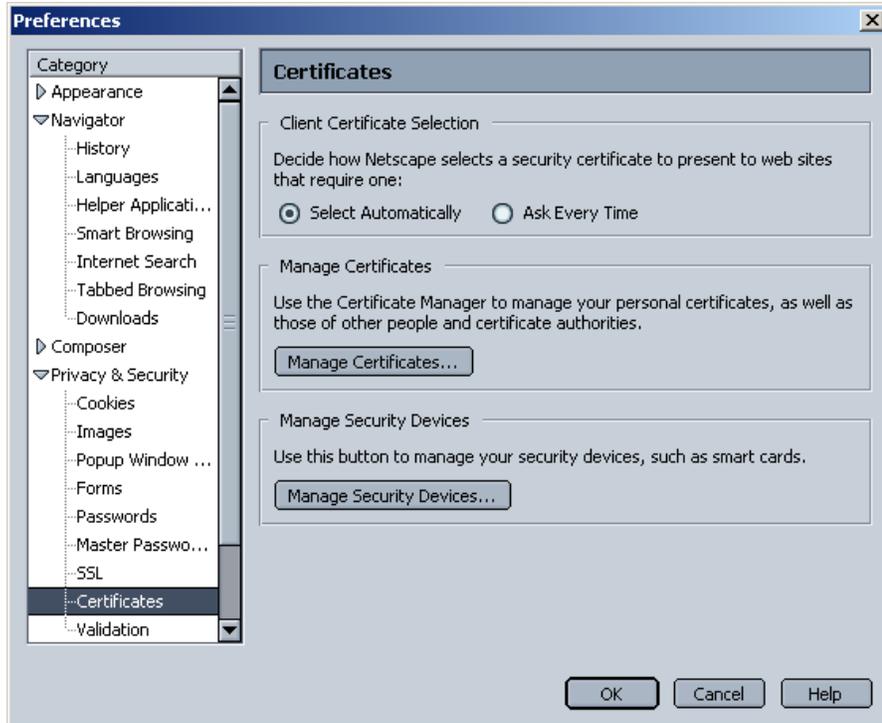
Click on the “Change Password” button and establish a master password.

Under “Master Password Timeout”, choose an option that best fits your security preferences.

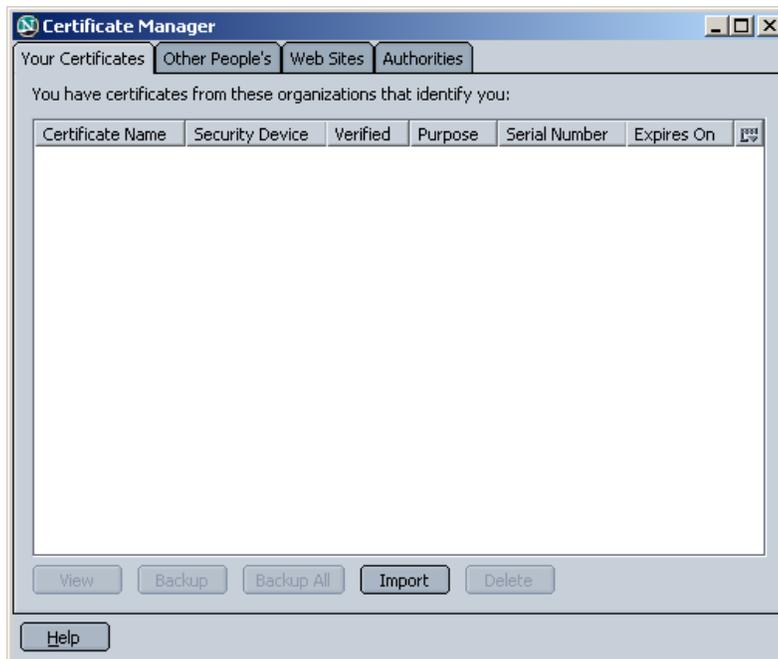
NOTE: This password is used by Netscape and is not related to your Digital Certificate password. Choose anything you want for your password, but remember that Netscape will occasionally require you to enter this “Master Password” to allow you to perform security and administrative tasks.



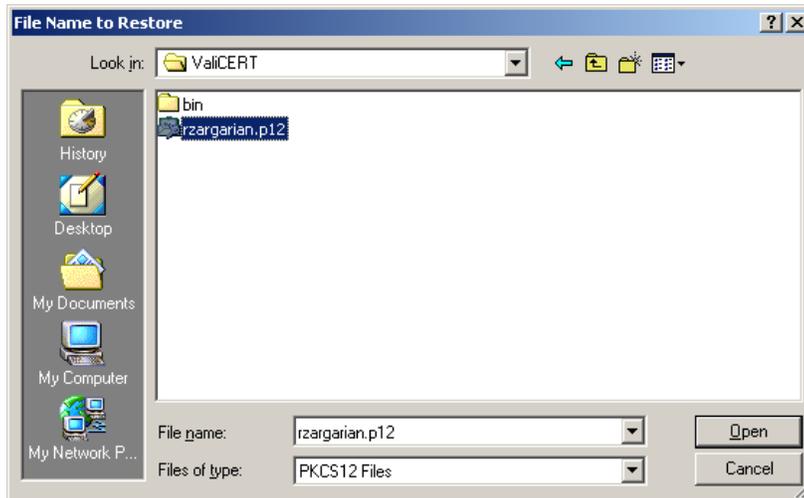
From the right hand menu under “Privacy and Security” select the “Certificates”. In Client Certificate Selection, leave the “Select Automatically” option selected. Click on the “Manage Certificates” button.



On the Certificate Manager window, click the “import” button.



Navigate to the location where you saved your Digital Certificate.
Select it and click Open.



You might be prompted to enter a “Master Password”. Enter the master password
you created (changed) earlier and click OK.



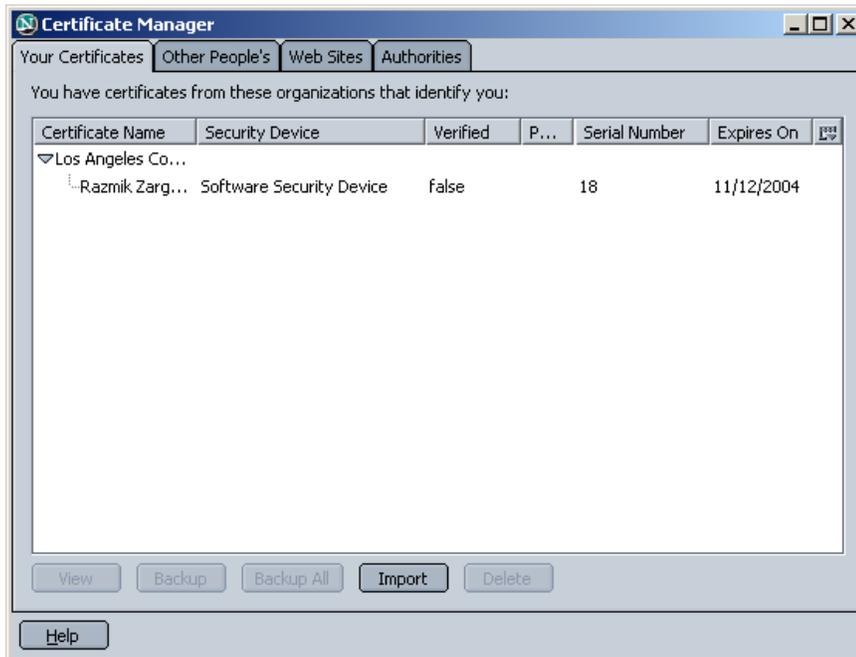
Enter the password that you received with your Digital Certificate and click OK.



Click OK on the “Alert” message.



Close the Certificate Manager windows by clicking on the X at the top right corner.



Click OK to close the Preferences window.

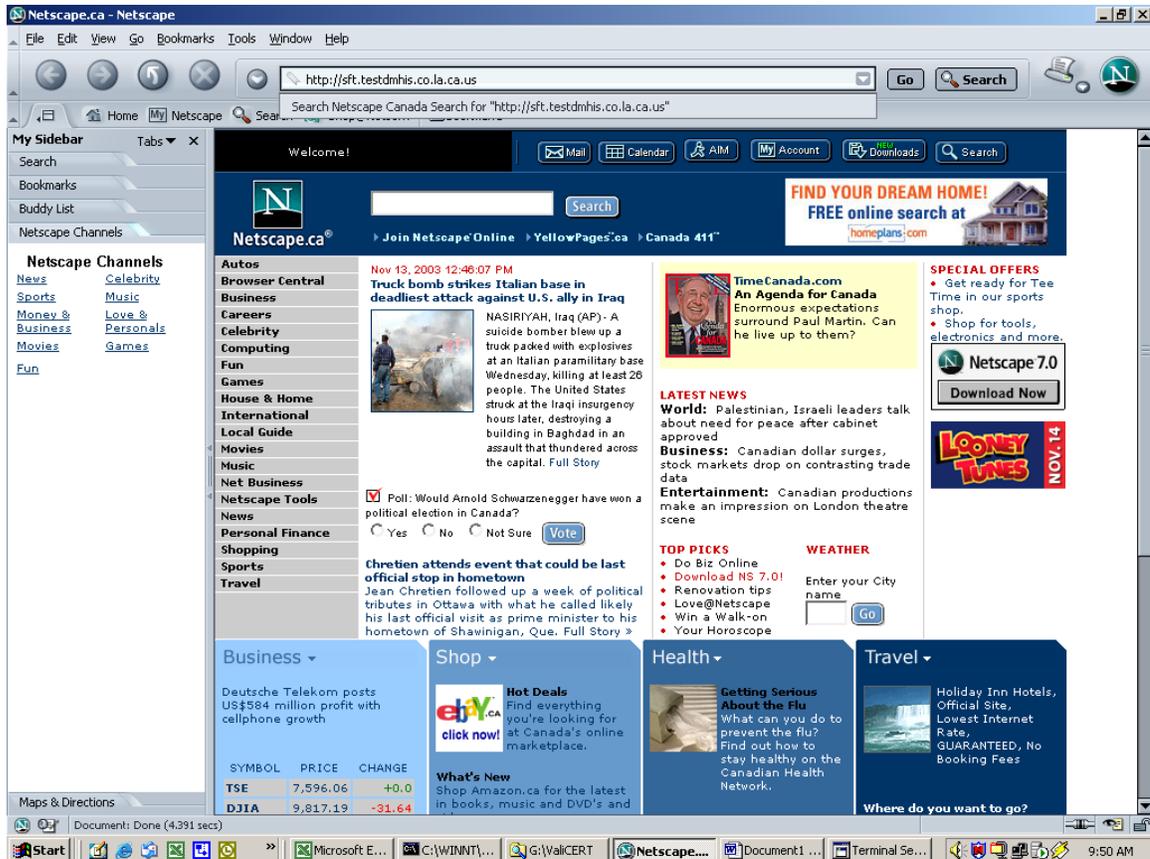


4 Test Your Certificate

4.1 Netscape Navigator Users

In the address field enter: <https://sft.dmhis.co.la.ca.us:8443/> For Production Environment and click the “Go” button.

In the address field enter: <https://sft.testdmhis.co.la.ca.us:8443/> For Test Environment and click the “Go” button.



On the next alert message, select “Accept this certificate permanently” and click OK.

NOTE: If you choose to leave this setting on the default “Accept this certificate temporarily for this session”, you will be prompted with this alert every time you enter the site.



Click OK on the alert regarding the domain name mismatch.

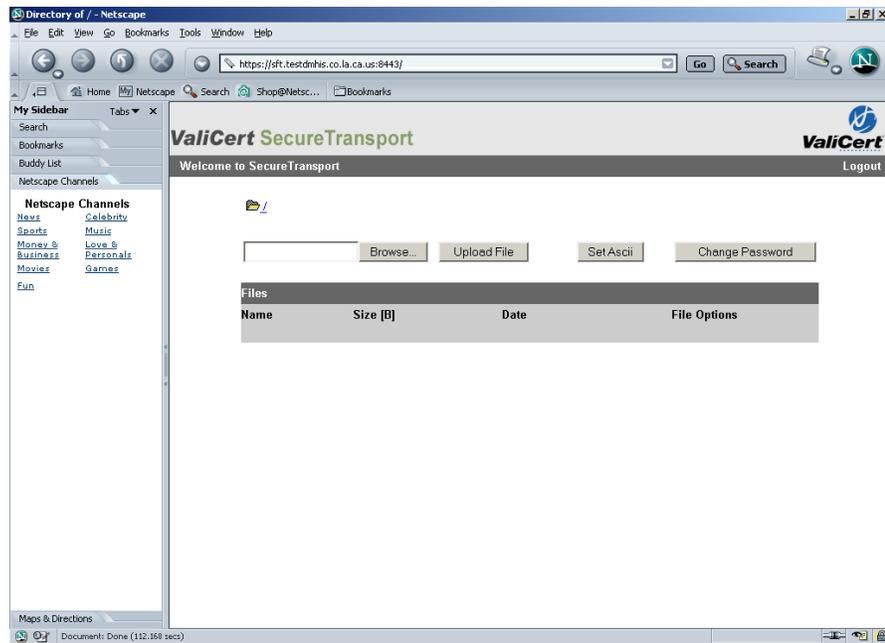


NOTE: Depending on your browser settings, you may be presented with the following alert. If you uncheck the "Alert me" you won't be prompted with this alert next time you visit the site.

Click OK.



The browser should now present you with the Secure File Transfer site.



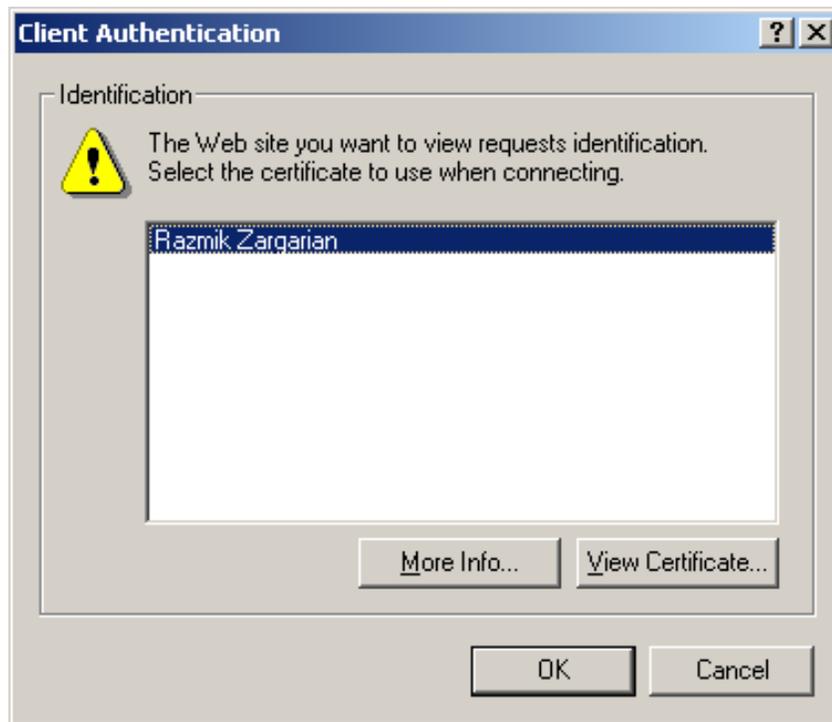
4.2 Internet Explorer Users

Start the Internet Explorer. Type the URL for the DMH site that you need in the Address field and press Enter (or click Go).

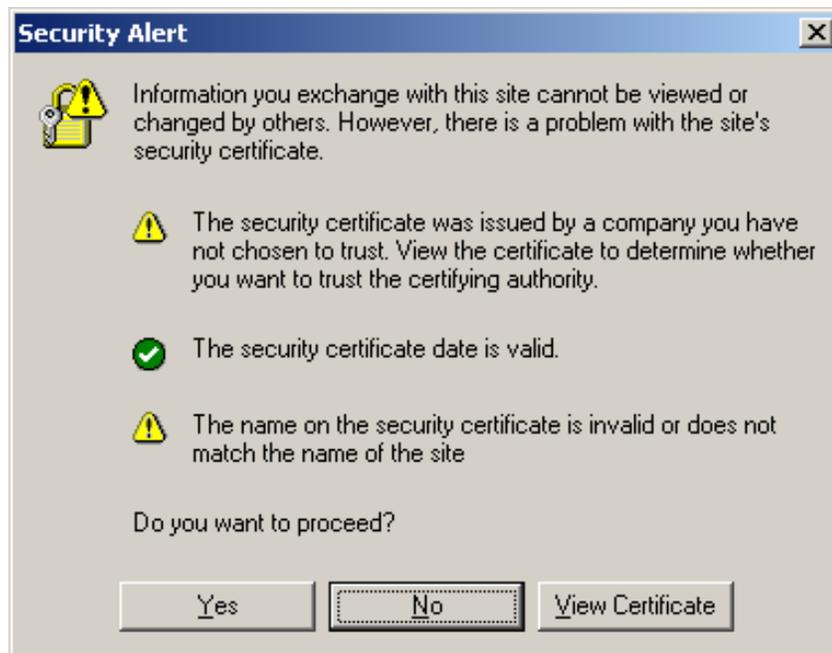
<https://sft.dmhis.co.la.ca.us:8443/> Production Environment

<https://sft.testdmhis.co.la.ca.us:8443/> Test Environment

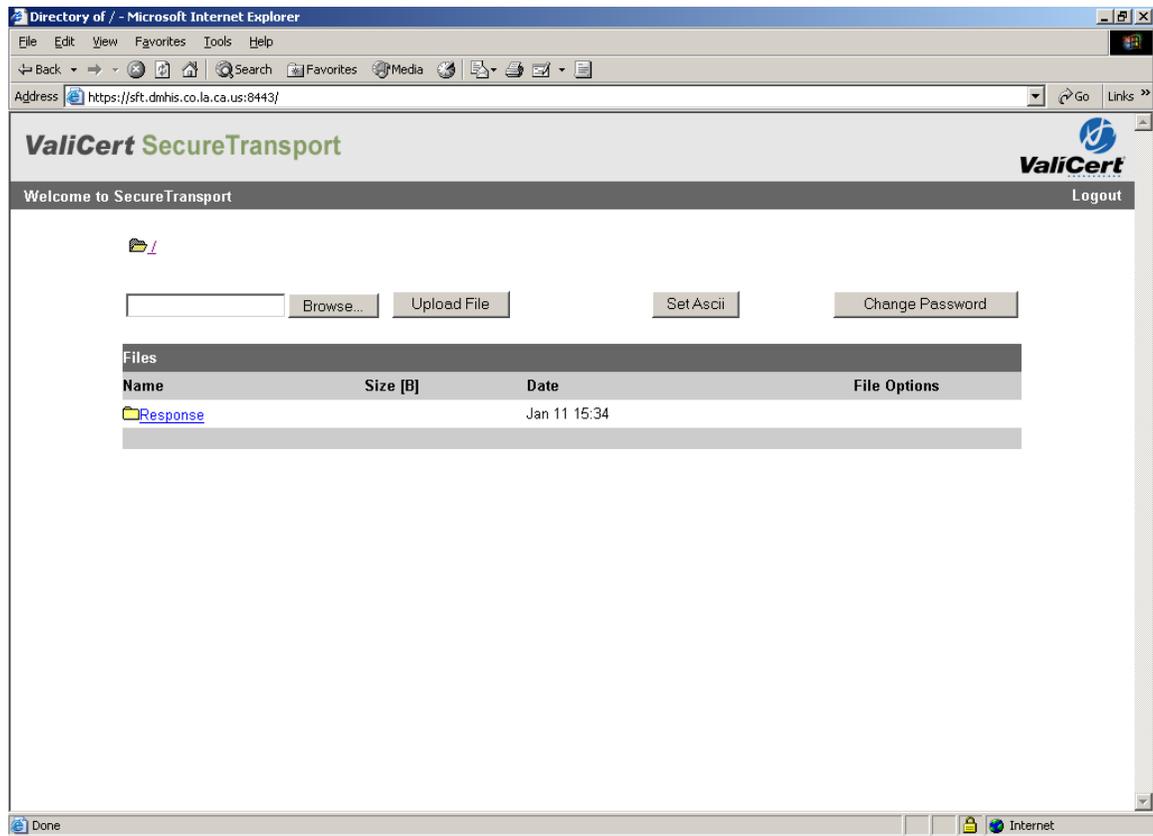
You will be prompted with a Client Authentication screen. Click OK.



Click Yes on the Security Alert screen.



The Secure File Transfer web site is displayed. Your certificate test is complete.

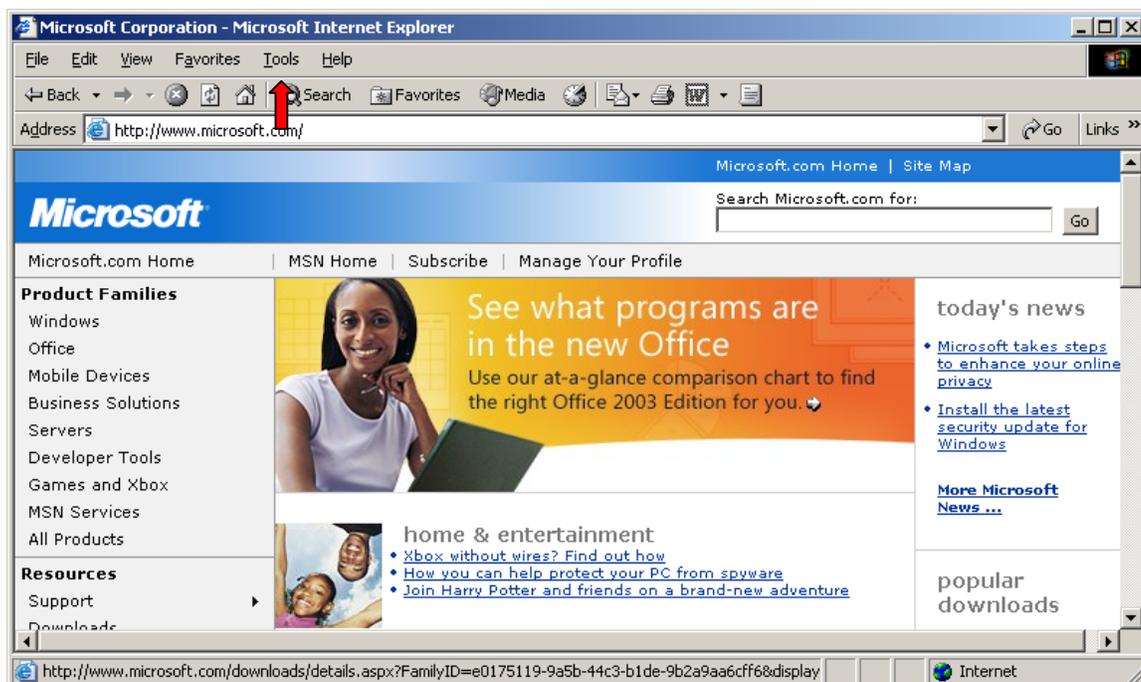


If you see this web site, your certificate worked and you are ready to transfer files.

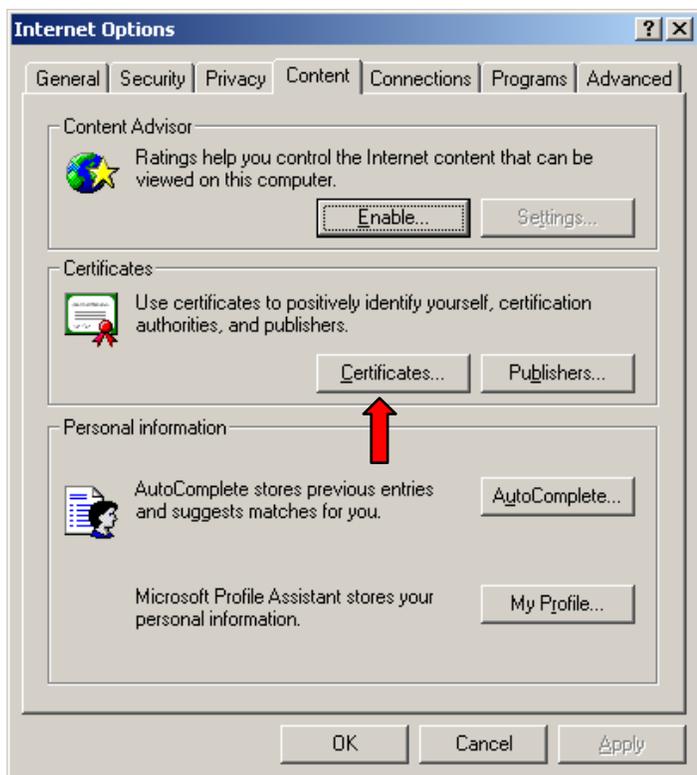
5 How to remove your Digital Certificate

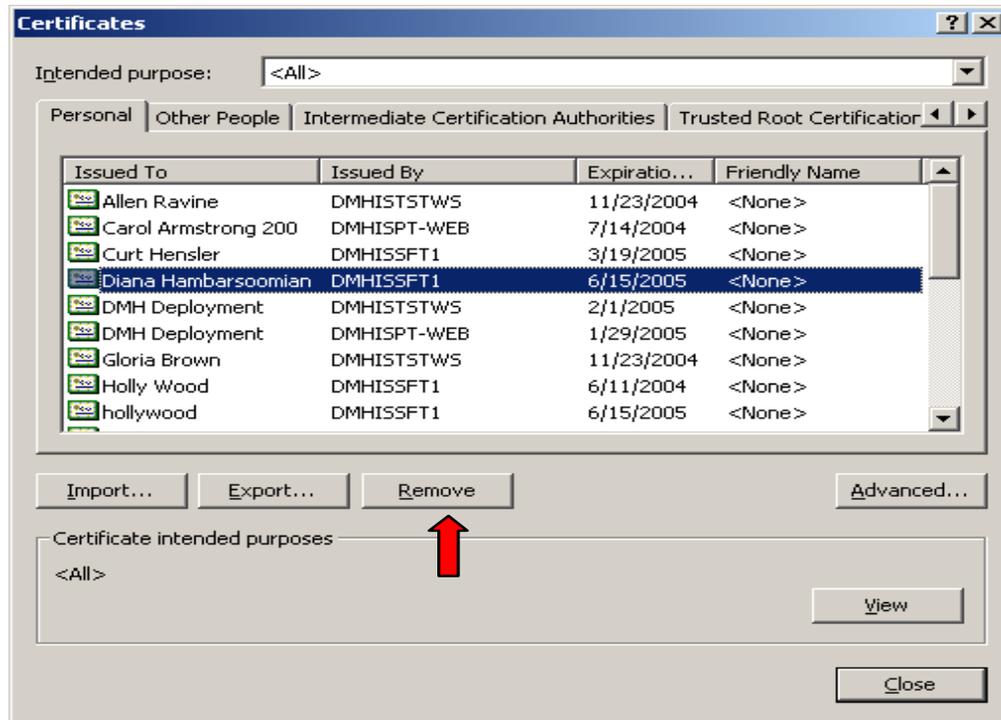
5.1 Internet Explorer Users

Open Internet Explorer. Click on the **Tools/Internet Options**



Click on the **Content** tab. Click on the **Certificates**. Select your name and click **Remove**.



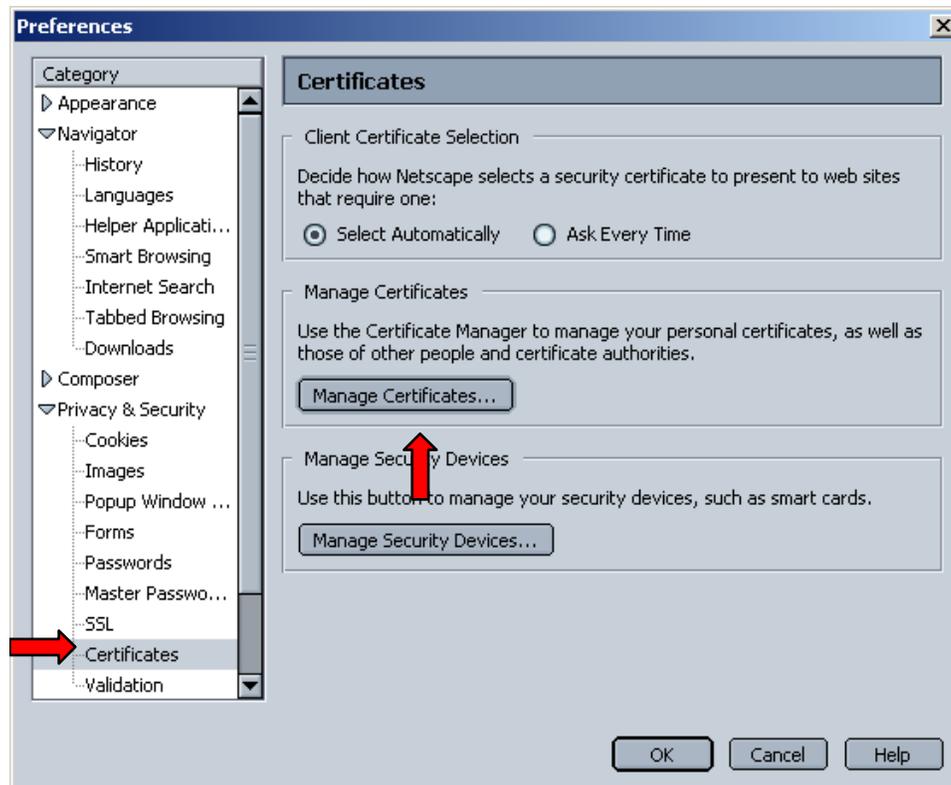


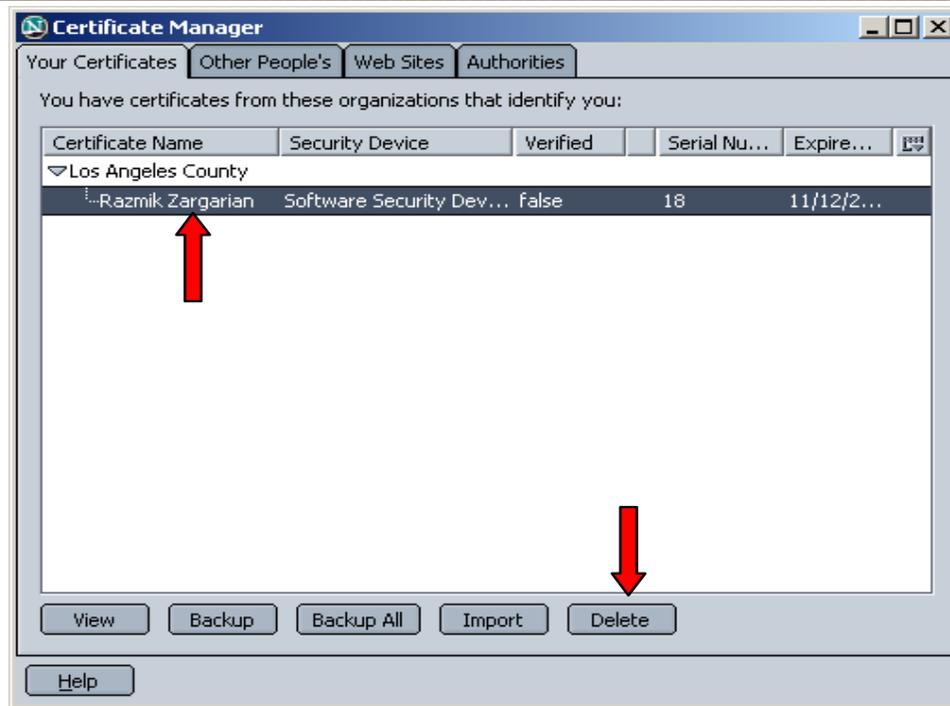
5.2 Netscape Navigator Users

Open Netscape. From the Menu, click Edit/Preferences.



Click on the small triangle next to Privacy and Security. Select Certificates. Select the old certificate and click Delete.





After you have removed your test Digital Certificate please delete it.

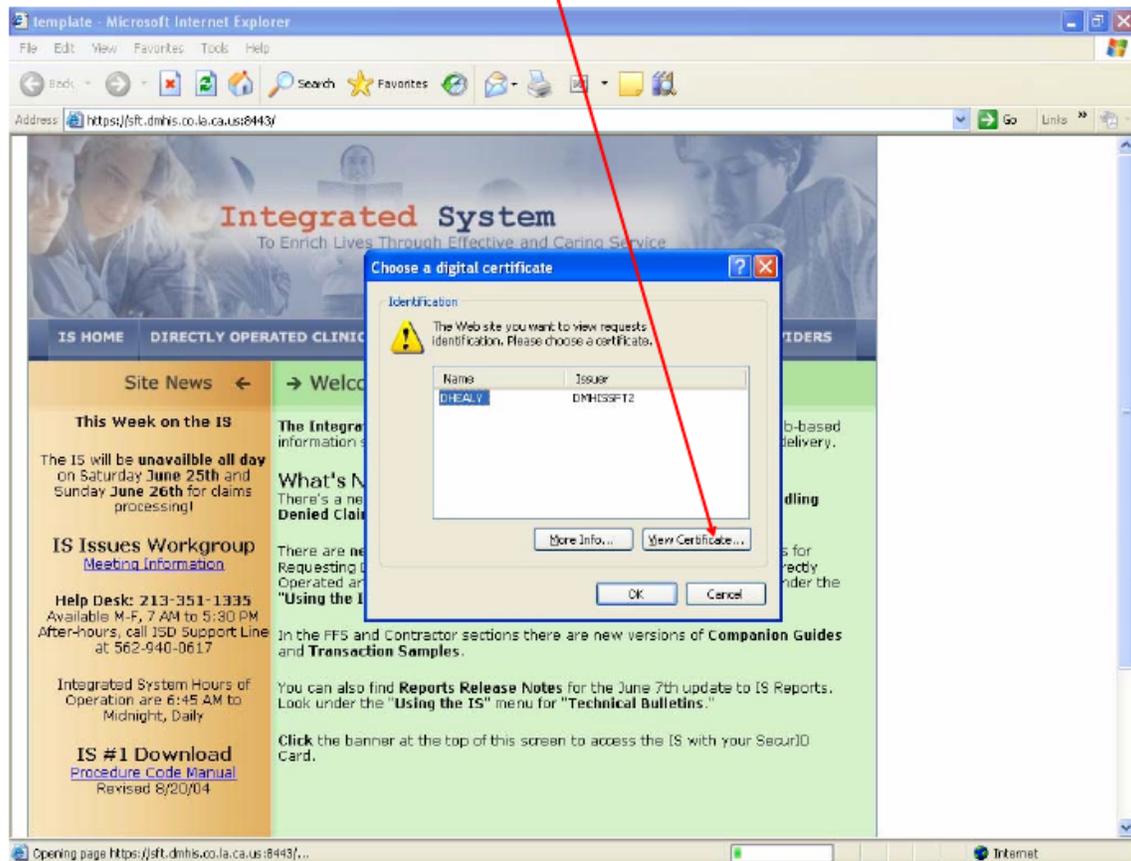


Click OK.

6 How to Check the Expiration Date of the Digital Certificate

To check the expiration of your Production Digital Certificate:

1. Log in to SFT upload site (<https://sft.dmhis.co.la.ca.us:8443/>). When the Digital Certificate validation window appears, **Click on View Certificate...**



2. The certificate will provide the following information:
 - a. Issued to: *Biller Name*
 - b. Issued by: DMHSSFT2
 - c. Valid from: *start date* To: *expire date*

