Using the Secure Data Network

Centers for Disease Control and Prevention
National Center for HIV, STD, and TB Prevention
Division of HIV/AIDS Prevention

June 07, 2005 (Revision 2)

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION

SAFER • HEALTHIER • PEOPLE™

SDN Help Desk: 1-800-532-9929 or cdcsdn@cdc.gov

Notes:

Contents

Introduction 1-1
The Digital Certificate 1-1
Overview of the SDN Challenge Phrase, the Certificate Password, and the Master Password 1-1
The SDN Server 1-3

Registering for a Digital Certificate 1-3
Creating a Challenge Phrase 1-8

About Downloading and Installing the Digital Certificate. 1-9
Before Downloading the Digital Certificate. 1-10
Before Installing a Digital Certificate. 1-11
Workstation Configuration 1-11
Browser Considerations and Other Notes 1-12
Additional Settings for Internet Explorer 1-12
Allowing Cookies in Internet Explorer. 1-13
Changing Security Settings in Internet Explorer 1-13
Disabling Google Popup Blocker 1-13
Disabling Yahoo Pop-Up Blocker 1-14
Additional Information for Windows XP (SP2) 1-15
Turn Off Windows XP SP2 Pop-up Blocker 1-15
Turn Off Windows XP SP2 Firewall 1-16
Disable Windows Security Center Antivirus Alerts 1-16
Additional Settings for Netscape. 1-17
Allowing Cookies in Netscape 1-17
Managing Popup Windows in Netscape. 1-17

Downloading and Installing the Digital Certificate 1-17
Downloading and Installing a Digital Certificate in Internet Explorer. 1-17
Verifying Certificates Stored in Internet Explorer. 1-19
Downloading a Digital Certificate in Netscape 1-19

Additional Browser Functions 1-23
Exporting a Digital Certificate 1-23
Exporting from Internet Explorer. 1-23
Exporting from Netscape 1-24

Importing a Digital Certificate 1-24
Importing in Internet Explorer 1-24
Creating a Certificate Password in Internet Explorer . . 1-26
Importing in Netscape 1-28
Verifying Certificates Stored in Netscape. 1-30
Creating a Master Password in Netscape 1-30
Configuring a Browser for Automatic Certificate Selection 1-31
Configuring Internet Explorer 1-31
Configuring Netscape 1-32

Accessing the SDN 1-33
Accessing Program Activities 1-33

Additional SDN Functions 1-35
Requesting Additional Programs and Activities. 1-35
Updating the Challenge Phrase 1-38
Updating Personal Information 1-40

Forgotten Passwords 1-42
Forgotten Certificate Password or Master Password 1-42
Forgotten Challenge Phrase. 1-42

Chapter 1

SYSTEM OVERVIEW

Introduction

The Secure Data Network, or SDN, is used by anyone who wishes to send files to CDC or receive files from CDC. While the SDN has many other capabilities, only its use in support of file transfers is discussed in this document.

It is CDC policy that all data sent to CDC must be transmitted in a protected manner. To accomplish this:

1. Digital certificates are issued to ensure that only authorized persons can access the SDN.
2. All data are encrypted, thus protecting data from unauthorized eavesdropping while in transit.

In order for the system to work, each user must first register for a digital certificate, and then install the issued certificate on the machine used to access the SDN. This certificate identifies the client machine to the SDN Web server. The certificate also establishes a secure transmission between the client machine and the SDN server at CDC. The secure transmission encrypts all data passed between the client machine and the SDN server.

Note: Any questions regarding certificate registration, installation, export, import, or other SDN process should be directed to the SDN Help Desk at 1-800-532-9929 or by e-mail at cdcsdn@cdc.gov. Any questions regarding program activities, such as uploading data files, should be directed to the program's support team.

The Digital Certificate

Overview of the SDN Challenge Phrase, the Certificate Password, and the Master Password

The process of registering for a digital certificate has several steps, but a user only has to register for a digital certificate once; the certificate is then renewed annually. The process is illustrated on page 1-44.

During registration, you create a challenge phrase that functions as an SDN password. The Digital Certificate Authority, the organization responsible for creating and issuing certificates, requires the submission of the challenge phrase as part of your digital certificate registration. The Digital Certificate Authority records a hash (an algorithm) of the challenge phrase on the SDN server. The challenge phrase is then used to authenticate your identity in any subsequent transactions involving the digital certificate.

You have the option of creating a certificate password in Internet Explorer or a master password in Netscape. If a certificate has a password, you must supply the password to the browser before the browser will permit access to the certificate. The password serves to assure the browser that the person using the certificate is the same person who obtained and installed it.

The following information is provided to help in understanding the difference in purpose and function between the challenge phrase and the certificate or master password. The purpose of the challenge phrase is to authenticate a user before allowing access to the authorized activities on the SDN, thus the challenge phrase must be entered each time a user accesses the SDN. The challenge phrase is a set of characters created when a user submits a certificate request to the SDN. It is case-sensitive and is stored as a hash in the user database on the SDN server.

A hash is an algorithm that maps or translates the challenge phrase in such a way that the digital certificate and the SDN server can accurately interpret the result of the algorithm each time a connection is requested and the challenge phrase is correctly entered. Any other approach or attempt to reconstitute the algorithm into the challenge phrase will fail. Therefore, the challenge phrase is not visible to anyone at CDC or elsewhere.

CAUTION: Because a challenge phrase cannot be accessed by anyone at CDC, it is strongly recommended that once the challenge phrase is established, you record and securely store the challenge phrase. If the challenge phrase is forgotten, follow the procedures described in "Forgotten Challenge Phrase" on page 1-42.

The purpose of the certificate or master password is to protect a certificate installed in a browser from unauthorized use. Establishing and then correctly entering a certificate or master password indicates to the browser that you are the person authorized to access the certificate.

If the digital certificate does not have a password, anyone capable of logging in on the computer (or accessing it if the computer does not require a logon) can be presented as the holder of the digital certificate and can either export or delete the certificate. This same individual, however, cannot access the SDN server because of the challenge phrase.

In Internet Explorer, a certificate password can only be created when importing the digital certificate. The master password for Netscape can be created at any time. Because the creation and use of these passwords is a transaction between you and the browser, neither the SDN nor anyone at CDC can see whether or not you created a certificate or master password.

Depending on the operating system in use, two users can be given a unique logon for the same computer. They would not have access to the same browser settings and would not see the other user's certificate. In this case, password protecting the certificate may not be necessary. When multiple users access one computer using the same logon or when the computer does not utilize a logon process, CDC recommends, but does not mandate, the use of a certificate password.

Note: For instructions regarding the creation of a certificate password, refer to "Creating a Certificate Password in Internet Explorer" on page 1-26. For instructions regarding the creation of a master password, refer to "Creating a Master Password in Netscape" on page 1-30.

The SDN Server

The SDN server is a special Web server protected by two firewalls and requiring a Secure Sockets Layer (SSL) connection. To access the SDN server via the Internet, enter *https://sdn.cdc.gov* in the **Address** box of a supported browser and press **Enter**. The "s" after "http" indicates the use of SSL to secure, encrypt, and transport data.

This server manages traffic between computers both inside and outside of the CDC Local Area Network (LAN), and is configured so that only Web browsers containing CDC-authorized digital certificates may connect to it. Attempted connections from other browsers are refused.

After accessing the SDN server via the Internet, the browser may prompt you to specify which digital certificate to use. You may have more than one digital certificate installed in a browser, because other federal and non-federal systems also require the use of unique, digital certificates. In some cases, multiple certificates for the SDN may exist on a machine that either utilizes a common logon or none at all. Depending on the configuration of the browser, this prompt to specify a certificate may be displayed even if the browser only has one digital certificate installed.

Note: Browsers can be configured to skip this prompt and use the CDC digital certificate by default if it is the only certificate installed in the browser. See "Configuring a Browser for Automatic Certificate Selection" on page 1-31 for details.

If you established a password for the digital certificate when the certificate was imported or installed, you are prompted for this password whenever you attempt to access the SDN Web site. This step informs the browser that the person using the digital certificate is the person who obtained and installed it and, therefore, is the person authorized to access the SDN Web page.

Once the SDN server receives a valid SDN digital certificate from the browser, the SDN server establishes a Secure Sockets Layer (SSL) connection with the browser. This means the Internet connection between the SDN server and the browser is encrypted and the exchange of data is secure.

The SDN server contains a CDC-issued digital certificate, the purpose of which is to assure clients that they are communicating with the CDC SDN server. At connection time, the server relays its digital certificate information to the browser, which may, depending on its configuration, display it to the user.

The SDN server determines the identity of the user from the digital certificate. The identity of the user determines the customized menu of program activities that the browser displays.

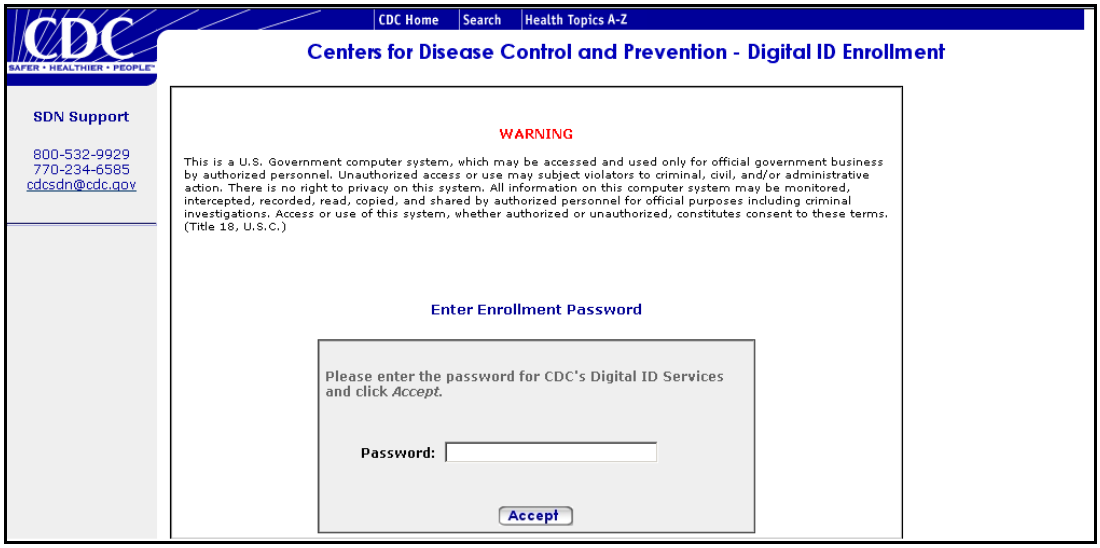
Registering for a Digital Certificate

Digital certificates are issued to specific users for use on the workstation from which they will access the SDN Web site. Every individual who will access the SDN Web site must register for an SDN digital certificate.

To register for a digital certificate, complete the following steps:

1. Open either Internet Explorer or Netscape, enter *https://ca.cdc.gov* in the **Address** field, and then press **Enter**.

The browser displays the Digital ID Enrollment page:



2. Enter the site password.

Note: Contact the SDN Help Desk at 1-800-532-9929 or by e-mail at cdcsdn@cdc.gov to obtain the site password.

3. Click **Accept**.

The browser displays the System Requirements and Digital ID Subscriber Agreement page.

4. Review the information concerning digital certificate registration and click **Enroll** at the bottom of the form.

The browser displays the Step 1: Enter Personal Information page:

Centers for Disease Control and Prevention - Digital ID Enrollment

To begin enrollment for a CDC Digital ID, complete this enrollment form and click *Next*.

Please Note:

- Internet Explorer 5.x or greater or Netscape Communicator 6.x, or greater is required to use the CDC Secure Data Network. If your browser doesn't meet this requirement, please upgrade your browser before applying.
- Be sure your email address is correctly entered. Without a valid email address you will be unable to install your digital certificate.

Step 1: Enter Personal Information

Items with (*) are required.

Prefix		Preferred Name	
* First Name		Middle Name	
* Last Name		Degree	
* Email Address		CDC User ID (where applicable)	
* Employer		Program or Division	
* Employer Type	Academic/Research Organization		
* Job Type	Biomedical Research		
* Phone		Fax	
Work Address (130 characters maximum)		* U.S. State (required for US)	Pick a State
		U.S. County	Pick a County
* City		* Zip Code	
* Country	United States		
* Alternate Contact :			
* Name		* Phone	

Next

Questions? Go to the Online Help or Contact SDN Support

5. Complete the fields on the Step 1: Enter Personal Information page.

Note: Fields marked with a red asterisk are required.

6. Click **Next**.

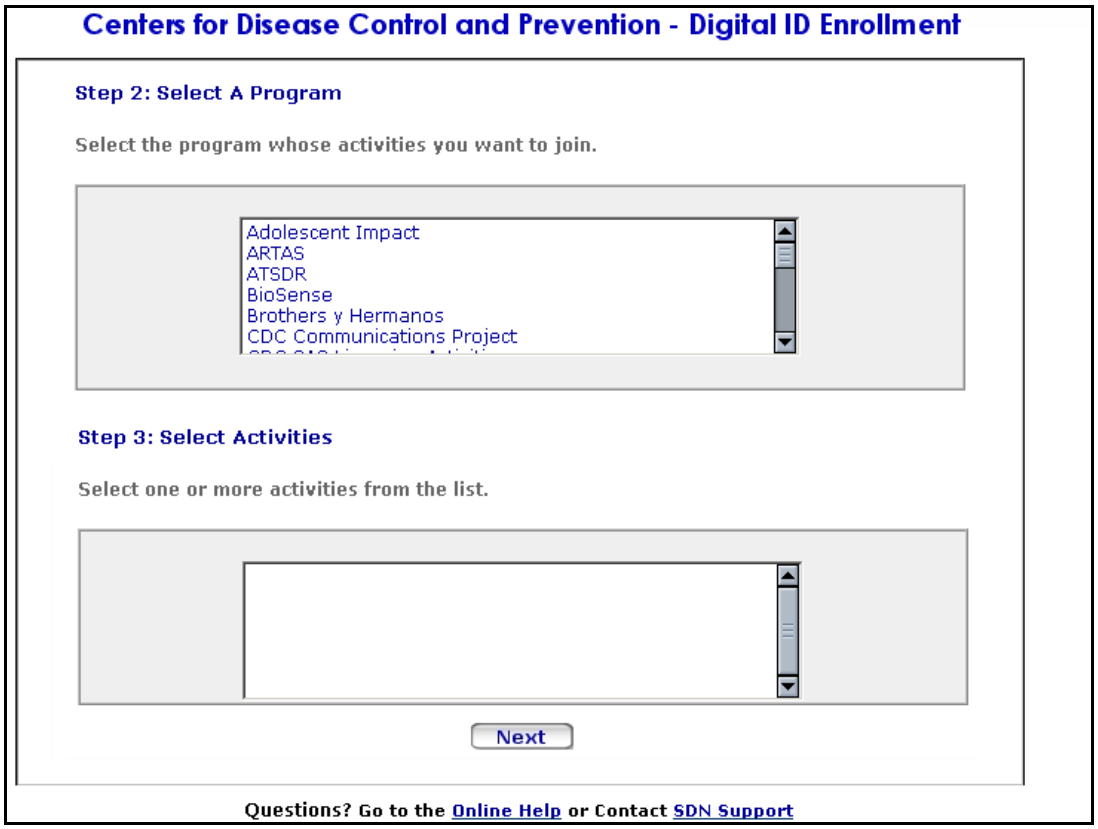
The browser displays a confirmation message containing your e-mail address.

Note: It is imperative that the correct e-mail address is entered. The system notifies you via e-mail that registration was successful and, after the certificate is issued, sends you an e-mail with a link to download the certificate.

7. Verify the accuracy of the e-mail address displayed in the confirmation message and do one of the following:

- Click **OK** if the e-mail address is correct.
- Click **Cancel** if the e-mail address is incorrect. Correct the e-mail address on the Enter Personal Information page and repeat steps 6 and 7.

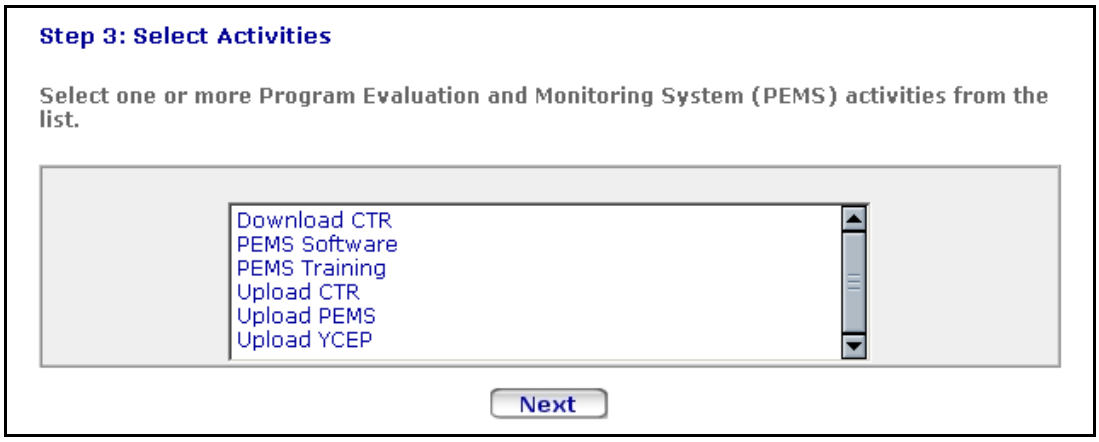
After you confirm the e-mail address is correct, the browser closes the confirmation message and displays the Step 2: Select a Program page:



8. In the **Step 2: Select A Program** list, select the appropriate program.

Note: You can request only one program during registration. If additional programs are required, follow the procedures in "Requesting Additional Programs and Activities" on page 1-35 after downloading and installing the certificate.

The browser displays a list of associated program activities in the **Step 3: Select Activities** list:



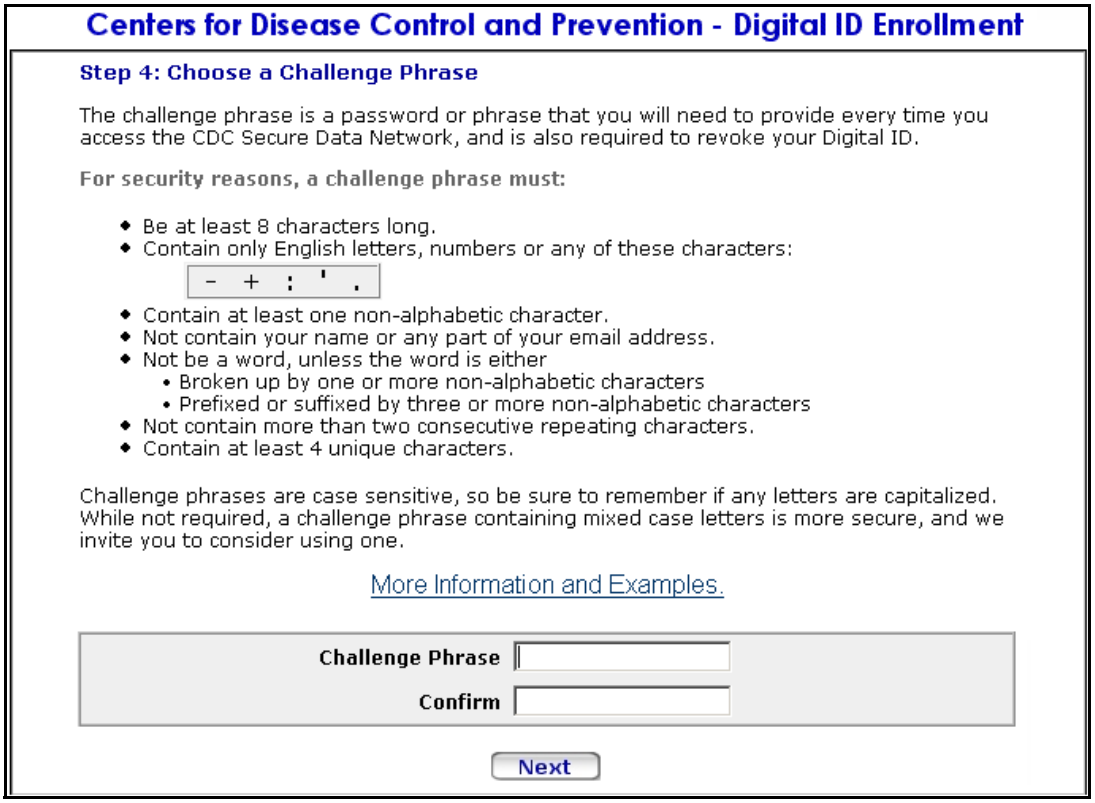
Note: Pop-up blockers can interfere with the display of the **Select Activities** list. If this list is not displayed, disable all pop-up blocking software and then select the appropriate program from the **Step 2: Select A Program** list.

9. From the **Step 3: Select Activities** list, select the necessary activities.

Note: To select more than one activity, press and hold the **CTRL** key while clicking each activity.

10. Click **Next**.

The browser displays the Step 4: Choose a Challenge Phrase page:



The SDN server requires the challenge phrase be correctly entered every time a user attempts to access the https://sdn.cdc.gov Web site. It is also required when an applicant installs a digital certificate and when the user renews the certificate.

Note: For specific criteria that must be followed when creating a challenge phrase, refer to "Creating a Challenge Phrase" on page 1-8.

11. Enter a challenge phrase and then click **Next**.

The browser displays a message indicating the request for the certificate has been submitted:

Digital Certificate Request Received

Your request for a digital certificate has been received.

You will receive an e-mail when your request is approved, which includes instructions for installing your digital certificate.

Please note that processing time may vary, depending upon the nature of the enrollment request. If you do not receive an e-mail notification within 72 hours, you may inquire about the status of your request by contacting the program administrator.

An automatic e-mail message is generated and sent to the address entered on the Step 1: Enter Personal Information page. This is not an e-mail indicating you have been approved for the certificate. If this verification e-mail message is not received within a couple of hours, contact the SDN Help Desk by phone at 1-800-532-9929 or by e-mail at cdcsdn@cdc.gov.

Creating a Challenge Phrase

The challenge phrase entered must meet all of the following conditions:

- ☒ Is at least eight characters long.
- ☒ Contains only English letters, numbers, spaces, or any of the following special characters:
  - (hyphen) **+** (plus) **:** (colon) **'** (apostrophe) **.** (period)
- ☒ Contains at least one non-alphabetic character.
- ☒ Does not contain your name or any part of your e-mail address. Is not a word, unless the word is either:
  - ☒ Interrupted by one or more non-alphabetic characters, or
  - ☒ Prefixed or suffixed by three or more non-alphabetic characters.
- ☒ Does not contain more than two consecutive repeating characters.
- ☒ Contains at least four unique characters.

Note: A challenge phrase is case sensitive.

Words are not secure challenge phrases because they will not stand up to password-cracking programs that use large dictionaries of words to try to guess passwords. You can begin creating a challenge phrase with a word, such as "produce", and make it acceptable for security purposes by adding a non-alphabetic character in the middle or by adding three characters as a prefix, suffix, or combination thereof. For example:

- ☒ pro+duce
- ☒ produce-98
- ☒ 8.produce5

You can also use multiple words or a phrase separated by a non-alphabetic character. For example:

- ☒ cart'pony
- ☒ eat more:greens

Because a name and e-mail address could be known to someone trying to guess a challenge phrase, they receive special treatment. If a name or e-mail address is found delimited by non-alphabetic characters anywhere in the challenge phrase, the challenge phrase will be rejected. For example, the challenge phrase “bill is great” submitted by Bill S. Great would be rejected. The challenge phrase “billis only so-so” would be accepted because the name “bill” is not explicitly delimited by non-alphabetic characters.

The same process applies to other parts of your name, as well as the construct of your e-mail address up to the @ symbol. Your entire e-mail address is also prohibited from appearing anywhere in the challenge phrase.

All of the rules governing the creation of a challenge phrase are designed to make it harder for a password-cracking program, or a person, to guess SDN challenge phrases. To help achieve that goal, the process that validates challenge phrases uses the same word dictionary that is used by many of the cracking programs.

The validation process strips up to two non-alphabetic prefixes and/or suffixes, and does a word lookup on what is left. If you want to use a word that is found in the dictionary, break it up with a non-alphabetic character or add more than two non-alphabetic characters as prefixes or suffixes.

Another aspect of the word lookup involves case. If the word being looked up contains at least two uppercase and two lowercase letters, a case sensitive word lookup is performed, otherwise the lookup is case insensitive. If the word being tested (after prefixes and suffixes are stripped) is “Procedure”, that word will fail a case insensitive lookup because “procedure” is in the dictionary. If “ProcEdure” is the word being tested, it will be accepted because a case sensitive lookup will not find “ProcEdure” in the dictionary.

About Downloading and Installing the Digital Certificate

After you submit a digital certificate registration, it is sent to the Program Digital Certificate Administrator (PDCA) for review. The PDCA may contact you to verify information submitted on the form. Once the PDCA approves the request for a certificate, the SDN Digital Certificate Administrator must approve or deny the request. If approved, CDC SDN Support automatically sends an e-mail to the address you entered and verified. This e-mail indicates the administrator has approved your SDN enrollment request, the digital certificate has been issued, and it is ready to be retrieved. The e-mail includes a hyperlink used to download and install the digital certificate.

Before Downloading the Digital Certificate

In order to download and install a certificate on a computer that limits access by utilizing user IDs and passwords, you must be logged on as an administrator or a member of the Administrators group. The rights to install components are normally assigned to the operating system administrator only and not to a power user, standard user, or guest account. If any doubt exists as to whether or not you have component installation rights, contact the local network administrator for assistance.

CAUTION: It is imperative that you verify your logon rights before clicking the hyperlink sent in the e-mail from CDC. This hyperlink can be used only once. If you click the hyperlink without the proper rights, the installation will fail and the hyperlink will be deactivated.

If you do not have the rights to install components on the computer, but attempt to download and install the certificate anyway, the process may be completed without successfully installing the certificate. To verify the installation of the certificate, refer to "Verifying Certificates Stored in Internet Explorer" on page 1-19 or "Verifying Certificates Stored in Netscape" on page 1-30. If the certificate cannot be verified, you must register for a new certificate.

Before clicking the hyperlink in the message from CDC SDN Support, ensure the following:

- ☒ You are logged on as an administrator or a member of the Administrators group.
- ☒ Pop-up blockers are turned off. Instructions for disabling pop-up blockers in Internet Explorer and Netscape are listed in "Additional Settings for Internet Explorer" on page 1-12, "Additional Information for Windows XP (SP2)" on page 1-15, and "Additional Settings for Netscape" on page 1-17.
- ☒ Script and ActiveX blocking must be turned off. This blocking can be done by both Internet Explorer and antivirus programs. For more information, see "Changing Security Settings in Internet Explorer" on page 1-13.
- ☒ Cookies should be allowed. Instructions are listed in "Allowing Cookies in Internet Explorer" on page 1-13 and "Allowing Cookies in Netscape" on page 1-17.
- ☒ Firewalls on the computer should be turned off. Network firewalls must be set to allow Java scripts. For more information, see "Turn Off Windows XP SP2 Firewall" on page 1-16.

Notes:

- If your preferred browser is Internet Explorer and your computer uses the Windows XP (Service Pack 2) operating system, review "Additional Information for Windows XP (SP2)" on page 1-15 before downloading and installing the certificate.
- If your preferred browser is Netscape, review "Additional Settings for Netscape" on page 1-17 before downloading the certificate.
- If downloading to your machine is not possible due to system settings, download the certificate to a computer that is set up to allow digital certificate downloads, and then export the digital certificate to disk or CD. Insert the disk or CD into a drive on your computer and import the digital certificate into the browser. For information about exporting a certificate, see "Exporting a Digital Certificate" on page 1-23. For information about importing a certificate, see "Importing in Internet Explorer" on page 1-24 or "Importing in Netscape" on page 1-28.
- After downloading and installing the certificate, restore settings to their previous configurations.
- Should you encounter problems when installing a digital certificate, contact the SDN Help Desk for assistance at 1-800-532-9929, or by e-mail at cdcsdn@cdc.gov.

Before Installing a Digital Certificate

Workstation Configuration

Ensure that the installation workstation meets the following requirements:

- ☒ Intel-based system with a 486 CPU or greater
- ☒ Windows 98, Windows NT 4.0 or greater
- ☒ Internet connectivity
- ☒ Internet Explorer 6.x or greater, or Netscape 6.0 or greater
- ☒ Browser cipher strength - 128 bit or greater

Browser Considerations and Other Notes

Ensure that the preferred browser, either Internet Explorer or Netscape, is updated with all the latest service packs and security patches (and then rebooted) before attempting to download the certificate. If you do not have rights to upgrade the browser or are not confident regarding the upgrading process, please contact local IT support for assistance.

Notes:

- Do not attempt to install the certificate in a proprietary browser provided by an Internet Service Provider (ISP), such as AOL or MSN.
- There may be other applications or software installed and running that could impact the installation. All other applications or software should be closed or disabled.
- The SDN requires that the browser's encryption (cipher) strength be at least 128 bits. To check the encryption strength of the browser, open the browser, click the **Help** menu and select **About Internet Explorer** or **About Netscape** (depending upon the browser opened). If the dialog box that opens does not specify 128 bits, the browser cannot be used to install the digital certificate:

Additional Settings for Internet Explorer

This section contains additional instructions for changing Internet Explorer settings that may interfere in downloading the SDN digital certificate. Complete the steps in this section after receiving the digital certificate approval e-mail, but before clicking the link in the e-mail and beginning the download of the certificate. After following the steps in this section to allow cookies and disable pop-up blockers and after completing the download and installation of the digital certificate, reverse the steps to return to the previous settings.

Note: These steps only apply to downloading a certificate from the Internet. CDC recommends that you work with your IT team to coordinate Internet Explorer settings when installing an exported certificate.

Allowing Cookies in Internet Explorer

To allow cookies in Internet Explorer, do the following:

1. Click **Start** and select **Control Panel**.
2. In Control Panel, double-click **Internet Options**.
3. In the **Internet Properties** dialog box, click the **Privacy** tab and move the slider to the lowest setting (**Accept All Cookies**).
4. Click **OK**.

Changing Security Settings in Internet Explorer

To change the Internet security settings and enable ActiveX controls in Internet Explorer, do the following:

1. Click **Start** and select **Control Panel**.
2. In Control Panel, double-click **Internet Options**.
3. Click the **Security** tab.
4. Click the **Internet** icon, and then click the **Custom Level** button.
5. In the **Security Settings** dialog box, click **Enable** below the **Automatic prompting for ActiveX control** option in the **Settings** box.
6. Select **Low** from the **Reset to** list and click **Reset**.

   Internet Explorer displays a warning message.
7. Click **Yes** in the message.
8. Click **OK** to close the **Security Settings** dialog box.
9. Click **OK** to close the **Internet Options** dialog box.

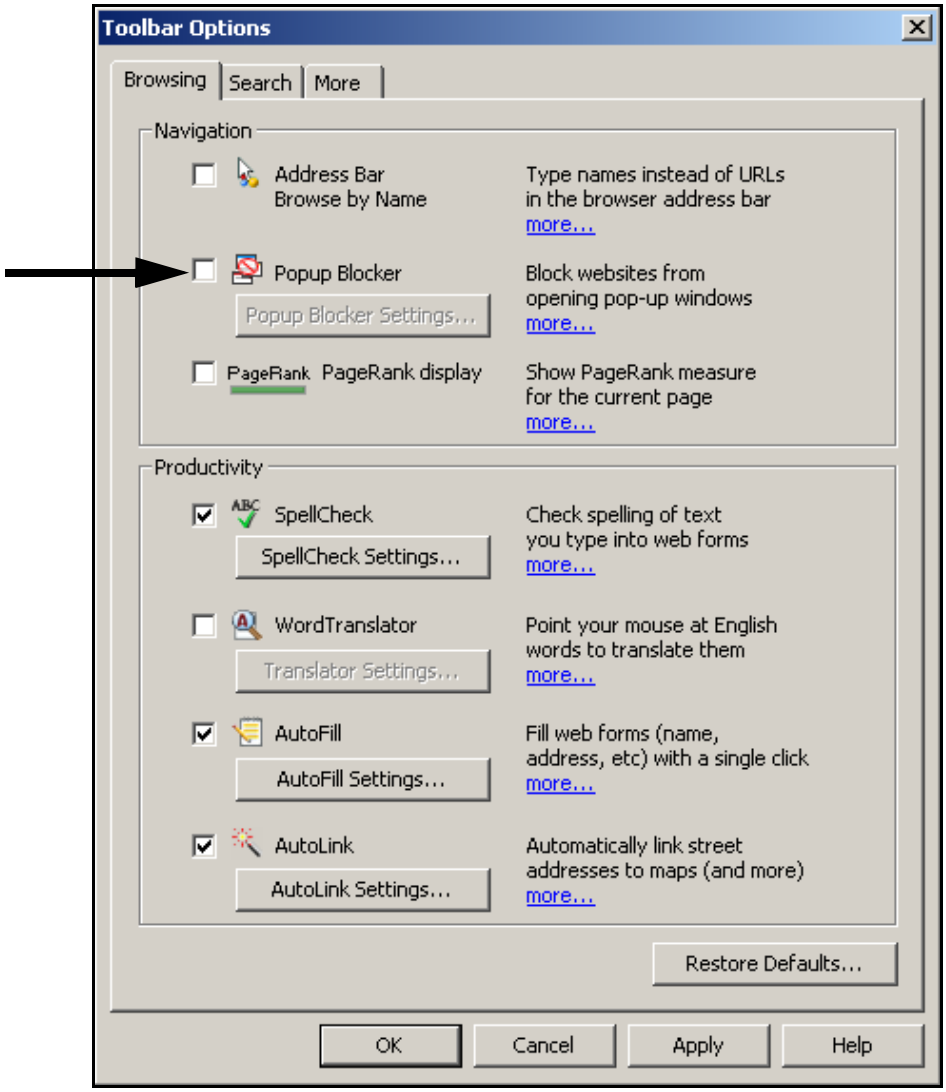
Disabling Google Popup Blocker

If the Google toolbar is installed, its popup blocker must be disabled before downloading the certificate. To disable the Google Popup Blocker for Internet Explorer, do the following:

1. On the **Google** toolbar, click **Options**.

   Note: If **Options** is not visible on the toolbar, click the **Google** logo button and select **Options**.

2. In the **Toolbar Options** dialog box, clear the **Popup Blocker** check box:



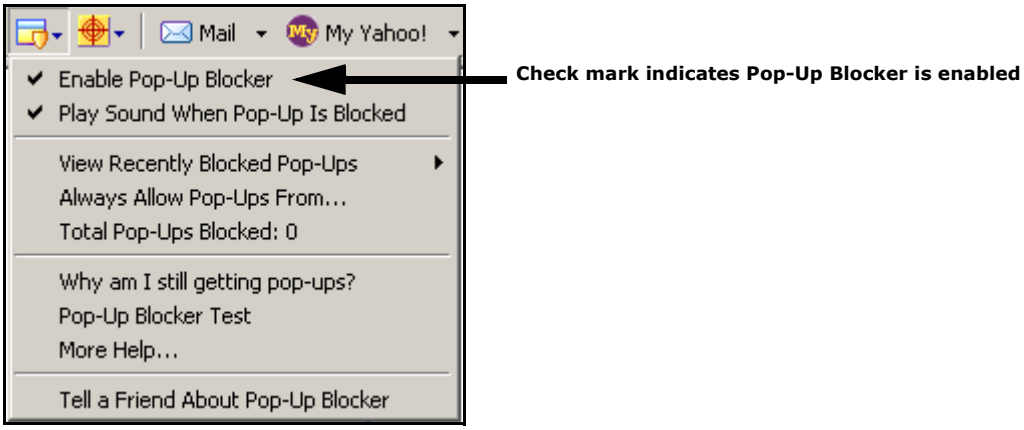
3. Click **OK**.

Disabling Yahoo Pop-Up Blocker

If the Yahoo toolbar is installed, its pop-up blocker must be disabled before downloading the certificate. To disable the Yahoo Pop-Up Blocker for Internet Explorer, do the following:

1. On the **Yahoo** toolbar, click the **Pop-Up Blocker** button.

The browser displays the **Pop-Up Blocker** menu:



2. Select **Enable Pop-Up Blocker**.

The browser closes the **Pop-Up Blocker** menu and disables the feature.

Additional Information for Windows XP (SP2)

This section contains additional instructions for Internet Explorer running under the Windows XP (Service Pack 2) operating system. Completing these instructions prevents interference with the download of the SDN digital certificate when pop-up blocker, firewall, or antivirus software are present.

Complete the steps in this section after receiving the digital certificate approval e-mail, but before clicking the link in the e-mail and beginning the download of the certificate. After you disable pop-up blocker, firewall, and antivirus software, download and install the digital certificate. After the certificate is installed, enable pop-up blocker, firewall, and antivirus software.

Note: These steps only apply to downloading the certificate using Internet Explorer on a Windows XP (SP2) machine. CDC recommends that you work with your IT team to coordinate Windows XP (SP2) settings when installing an exported certificate.

Before downloading the certificate, ensure the following:

- ☒ The XP Service Pack 2 pop-up blocker is turned off. For more information, see "Turn Off Windows XP SP2 Pop-up Blocker" on page 1-15.
- ☒ Firewalls on the computer are turned off, including the one built into Windows XP. For more information, see "Turn Off Windows XP SP2 Firewall" on page 1-16.
- ☒ Antivirus alerts are disabled in the Windows Security Center. For more information, see "Disable Windows Security Center Antivirus Alerts" on page 1-16.

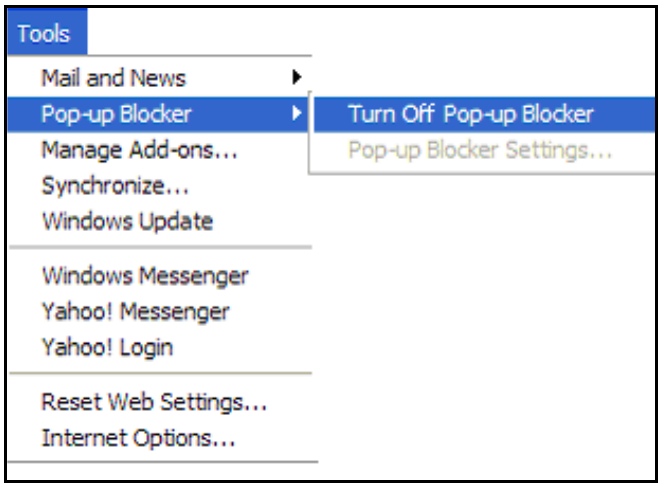
Turn Off Windows XP SP2 Pop-up Blocker

Service Pack 2 for Windows XP turns on Pop-up Blocker in Internet Explorer and sets it to **Medium** by default. This setting blocks most automatic pop-ups and can interfere with the downloading of the SDN digital certificate.

To disable Pop-up Blocker, do the following:

1. Open Internet Explorer.

2. Click the **Tools** menu, point to **Pop-up Blocker**, and select **Turn Off Pop-up Blocker**:



Turn Off Windows XP SP2 Firewall

Service Pack 2 for Windows XP turns on Firewall in the Security Center by default; however, some computer manufacturers and network administrators may disable Firewall. To turn off Windows XP SP2 Firewall, do the following:

1. Click **Start** and select **Control Panel**.
2. In Control Panel, double-click **Security Center**.
3. Click **Firewall**.
4. On the **General** tab of the **Firewall** dialog box, select **Off**.

Disable Windows Security Center Antivirus Alerts

Note: If your computer is part of a network, your security settings are typically managed by a network administrator. If so, the Security Center does not display your security status or send alerts and you can skip these steps.

To disable Windows Security Center antivirus alerts, do the following:

1. Click **Start** and select **Control Panel**.
2. In Control Panel, double-click **Security Center**.
3. Under **Virus Protection** in the Security Center, click **Recommendations**.

   The **Recommendations** button is not available if the **Virus Protection** setting is marked **ON**.
4. In the **Recommendations** dialog box, select the **I have antivirus software that I'll monitor myself** check box, and then click **OK**.

   When you use this procedure, the Security Center displays your Virus Protection setting as **Unknown**, and does not send you alerts.

Additional Settings for Netscape

This section contains additional instructions for changing Netscape settings that may interfere in downloading the SDN digital certificate. Complete the steps in this section after receiving the digital certificate approval e-mail, but before clicking the link in the e-mail and beginning the download of the certificate. After following the steps to allow cookies and disable pop-up blockers and after completing the download of the digital certificate, reverse the steps to return to the previous settings.

Note: These steps only apply to downloading a certificate from the Internet. CDC recommends that you work with your IT team to coordinate Netscape settings when importing an exported certificate.

Allowing Cookies in Netscape

To allow cookies in Netscape, do the following:

1. Open Netscape, click the **Edit** menu and select **Preferences**.
2. In the **Preferences** dialog box, expand the **Privacy & Security** category, and click **Cookies**.
3. Select **Enable all Cookies**.
4. Click **OK**.

Managing Popup Windows in Netscape

To allow popup windows in Netscape, do the following:

1. Open Netscape, click the **Edit** menu and select **Preferences**.
2. In the **Preferences** dialog box, expand the **Privacy & Security** category, and click **Popup Windows**.
3. Clear the **Block unrequested popup windows** check box.
4. Click **OK**.

Downloading and Installing the Digital Certificate

Note: If your browser is Internet Explorer and your computer uses the Windows XP operating system, review the information in "Additional Information for Windows XP (SP2)" on page 1-15 before completing any of the steps in this section.

Downloading and Installing a Digital Certificate in Internet Explorer

To download and install a digital certificate in Internet Explorer, do the following:

1. After receiving the verification e-mail, do one of the following:
   - If Internet Explorer is the default browser, click the hyperlink in the e-mail.
   - Open Internet Explorer. Copy the complete hyperlink in the message, paste the hyperlink in the **Address** field of the Internet Explorer window, and press **Enter**.

Note: For either option, ensure that the hyperlink is unbroken and is not wrapping to a second line in the e-mail message.

2. Enter the challenge phrase and then click **Submit**.

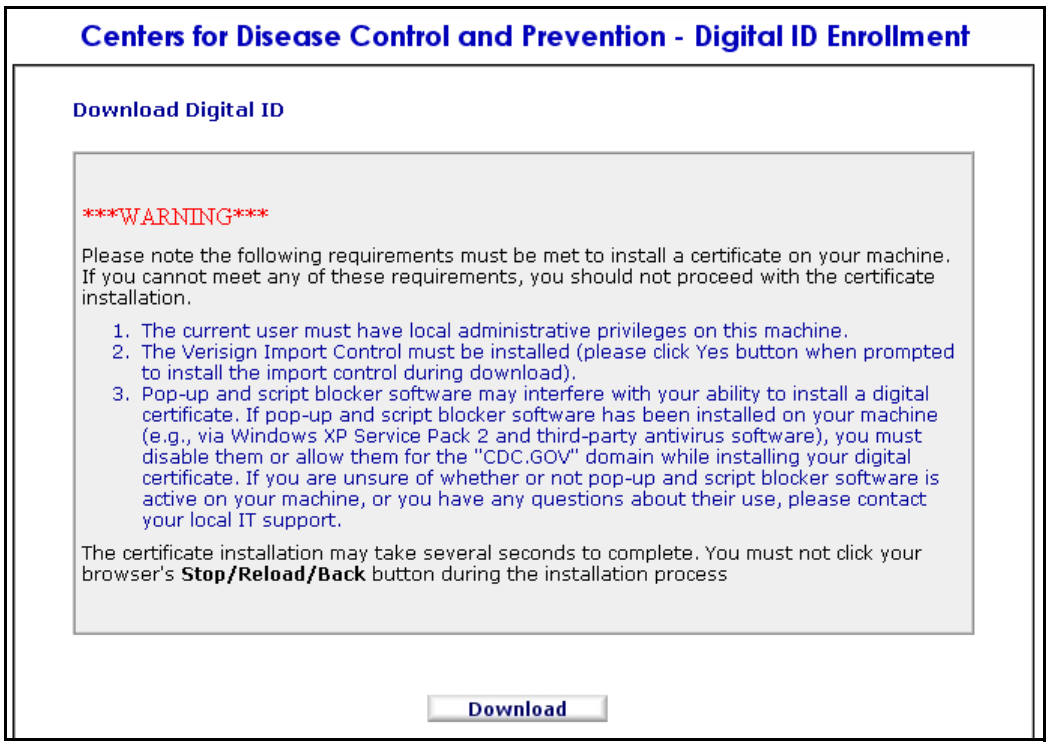
Note: The challenge phrase is case sensitive. If you cannot remember the challenge phrase, you cannot download the certificate and you must register for a new certificate.

After the successful entry of the challenge phrase, Internet Explorer displays the personal information that was entered by the registrant on the Step 1: Enter Personal Information page.

3. Click **Confirm**.

Note: If some information is incorrect, do not update the entries at this time. If you do, the installation will stop and you will have to register for a new certificate. Correct the information after installing the certificate. For more information, see "Updating Personal Information" on page 1-40.

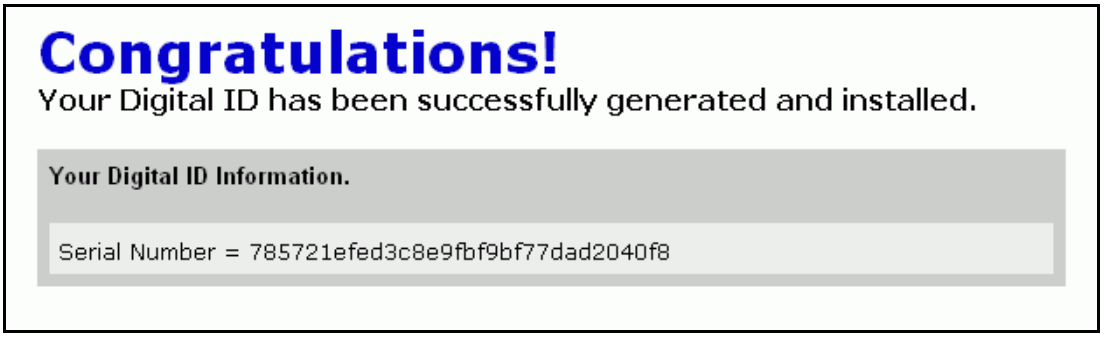
Internet Explorer displays a warning regarding installation requirements:



CAUTION: The VeriSign Import Control is required for installation. If the control is not found on the computer, Internet Explorer displays a prompt to install the control. You must accept the control installation or the certificate installation will fail.

4. Click **Download**.

After the certificate is successfully installed, Internet Explorer displays a verification page:



Verifying Certificates Stored in Internet Explorer

To verify the certificates stored in Internet Explorer, do the following:

1. Open Internet Explorer, click the **Tools** menu, and select **Internet Options**.
2. In the **Internet Options** dialog box, click the **Content** tab.
3. On the **Content** tab, click the **Certificates** button.
4. Click the **Personal** tab.

   Internet Explorer displays a list of stored certificates. If the SDN certificate is not displayed, the certificate failed to install. You must register for a new certificate.

Downloading a Digital Certificate in Netscape

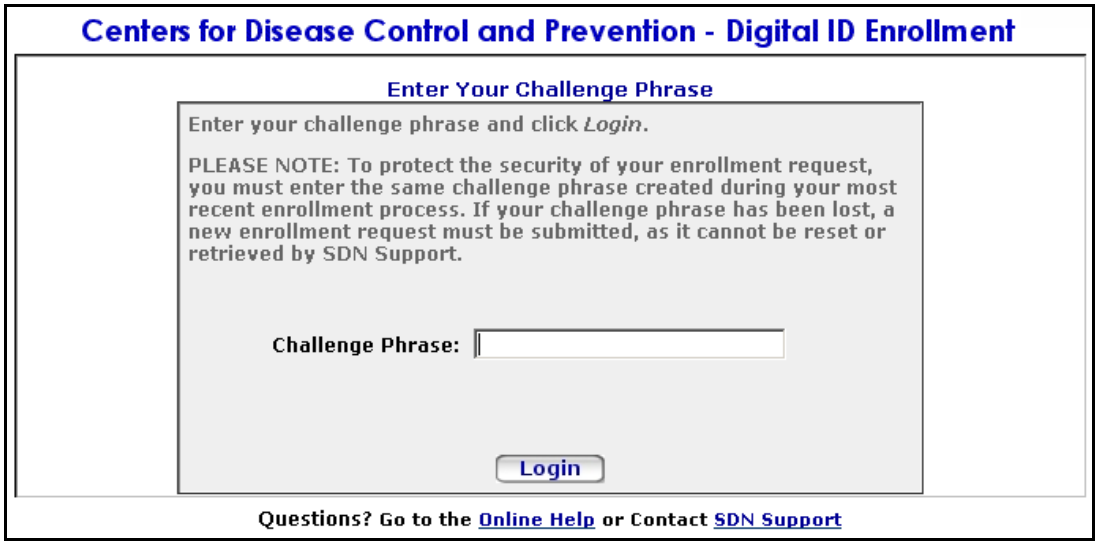
Netscape does not permit the automatic installation of a digital certificate. The certificate must be downloaded to the desktop and then imported into Netscape.

To download a digital certificate in Netscape, do the following:

1. After receiving the verification e-mail, do one of the following:
   - If Netscape is the default browser, click the hyperlink in the e-mail.
   - Open Netscape. Copy the complete hyperlink in the message, paste the hyperlink in the **Address** field of the Netscape window and press **Enter**.

     Note: For either option, ensure that the hyperlink is unbroken and is not wrapping to a second line in the e-mail message.

Netscape displays the Secure Data Network - Login page:



2. Enter the challenge phrase and then click **Login**.

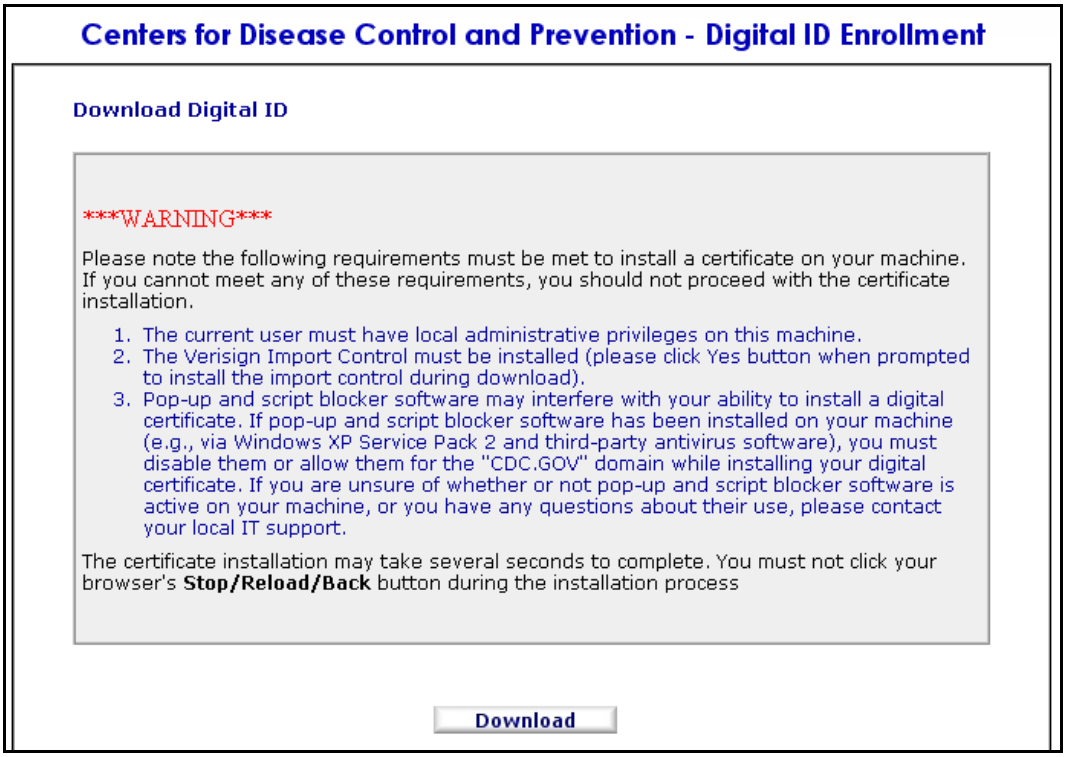
Note: The challenge phrase is case sensitive. If you cannot remember the challenge phrase, you cannot download the certificate and you must register for a new certificate.

After the successful entry of the challenge phrase, Netscape displays a Confirm Person Information form. This is the same personal information that was entered on the Step 1: Enter Personal Information page during enrollment.

3. Click **Confirm**.

Note: If some information is incorrect, do not update the entries at this time. If you do, the download will stop and you will have to register for a new certificate. Correct the information after importing the certificate. For more information, see "Updating Personal Information" on page 1-40.

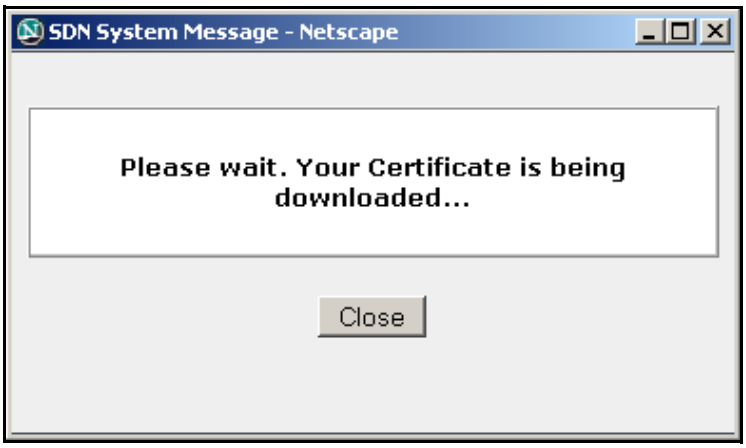
Netscape displays the Download Digital ID page and warnings regarding how to proceed:



CAUTION: The VeriSign Import Control is required. If the control is not found on the computer, Netscape displays a prompt to install the control. You must accept the control installation or the download will fail.

4. Click **Download**.

Netscape displays a message regarding the certificate download:



When finished downloading the certificate, Netscape displays the Digital ID Installation Complete page:

Your Digital ID has been created and is ready to be installed.

Next step...

Install the Encryption Digital ID

- Located in this directory:
  ../p12\
- In the file named:
  Joe_User_11163437991400.p12

Download P12 File

- The password is:
  QFKKRMBH77R7J325

WARNING

The digital certificate cannot be loaded automatically into Netscape, and requires that you download the certificate file and install it into your browser. The password provided above will allow you to perform the certificate installation, and should be provided when prompted. If you lose this password, you must contact CDC SDN Support.

This page displays the location of the certificate on the server, the name of the file, a **Download File** button, and the password for importing the certificate after downloading it. The password is used to protect the private key embedded within the certificate file.

5. Print the page in order to have a hard copy of the password, or copy the password to a Notepad file or another document.

Note: If this password is lost, the certificate cannot be imported.

6. Click **Download File**.

Netscape displays an **Opening** dialog box with options regarding how to handle the file.

7. Select **Save it to disk** and click **OK**.

Netscape displays the **Enter name of file to save to** dialog box.

8. Select **Desktop** from the **Save in** list and click **Save**.

Netscape saves the file to the desktop.

9. Import the certificate by following the Netscape instructions listed in "Importing in Netscape" on page 1-28.

Note: To verify the certificate was successfully imported, follow the instructions listed in "Verifying Certificates Stored in Netscape" on page 1-30.

Additional Browser Functions

Exporting a Digital Certificate

Once the certificate has been successfully installed, CDC strongly recommends that the owner of the certificate export a copy of the certificate. Exporting a copy of the certificate serves as a backup in case of the accidental deletion or corruption of the certificate. Having a copy of the certificate also allows you to load the certificate on other machines you may be using.

Note: Export the certificate to an external storage device such as a diskette or CD-ROM and lock the disk in a secure location.

During the export, the private key embedded in the certificate must be exported with the certificate. A function within the browser requires that the private key be password protected when exported. This password is required when importing the certificate. If you are not prompted to create a password to protect the key during the export process, the certificate is not being exported with the private key and therefore cannot be used to access the SDN.

The steps for exporting a certificate from Internet Explorer differ from the steps used in Netscape. Follow the appropriate procedures listed in "Exporting from Internet Explorer" on page 1-23, or "Exporting from Netscape" on page 1-24.

Exporting from Internet Explorer

To export a digital certificate from Internet Explorer, do the following:

1. Insert an external storage device in the appropriate drive.
2. Open Internet Explorer, click the **Tools** menu, and select **Internet Options**.

   Internet Explorer displays the **Internet Options** dialog box.
3. Click the **Content** tab and click the **Certificates** button.
4. Select the certificate to be exported, and click the **Export** button.

   Internet Explorer displays the Certificate Export Wizard.
5. Click **Next**.
6. If the certificate is password protected, you are prompted to enter the password.
7. Click **Next**.
8. When prompted to export the private key with the certificate, select **Yes**, and then click **Next**.

   Note: The certificate can only be exported with a ***.pfx** file name extension.
9. Ensure that **Enable strong protection** and **Include all certificates in the certification path** are selected and click **Next**.
10. Enter and confirm a password to protect the key and click **Next**.

    Note: This password is required when importing the certificate. Store this password in a secure location.

11. Do one of the following:

- Enter a path for the external storage device and a file name for the export file.
- Click **Browse**, navigate to the location where you want to export the certificate, and enter the file name.

12. Click **Next**.

13. When a summary of the information entered is displayed, do one of the following:

- Click **Back** to make any changes.
- If the information is correct, click **Finish**.

14. When Internet Explorer displays the 'Export was successful' message, click **OK** to close the message.

Exporting from Netscape

To export a digital certificate from Netscape, complete the following steps:

1. Insert an external storage device in the appropriate drive.

2. Open Netscape, click the **Edit** menu, and select **Preferences**.

3. Expand the **Privacy & Security** category and click **Certificates**.

4. In the Certificates panel, click **Manage Certificates**.

5. Select the certificate to be exported and click **Backup**.

6. Select the path for the external device and enter a name for the file (certificate).

7. Click **Save**.

8. If a master password was created for the browser, enter the master password in the dialog box and click **OK**.

9. In the **Choose a Certificate Backup Password** dialog box, enter a password for the exported file.

Note: This password is required when importing the certificate. Store this password in a secure location.

10. Click **OK** to export the file.

11. When Netscape displays the 'Export was successful' message, click **OK** to close the message.

Importing a Digital Certificate

A certificate may need to be imported for many reasons, such as the certificate needs to be loaded on another workstation or the original certificate became corrupt. The steps for importing a certificate in Internet Explorer differ from the steps used in Netscape. Follow the appropriate procedures listed in "Importing in Internet Explorer" on page 1-24, or "Importing in Netscape" on page 1-28.

Importing in Internet Explorer

To import a digital certificate in Internet Explorer, do the following:

1. Insert the external storage device that contains the password-protected certificate.

2. Open Internet Explorer, click the **Tools** menu and select **Internet Options**.

Internet Explorer displays the **Internet Options** dialog box.

3. Select the **Content** tab and click the **Certificates** button.
4. Click the **Import** button.

   Internet Explorer displays the Certificate Import Wizard.
5. Click **Next**.

   The Certificate Import Wizard displays the File to Import screen.
6. Click **Browse**, navigate to the location of the digital certificate in the **Open** dialog box, and double-click the file name of the certificate.

   Note: Alternatively, you can enter the drive, path, and certificate name in the **File name** box.
7. Click **Next**.

   The Certificate Import Wizard displays the Password screen.
8. Enter the password created during exporting.
9. Select both of the following options:

   - **Enable strong private key protection**
   - **Mark the private key as exportable**
10. Click **Next**.

    The Certificate Import Wizard displays the Certificate Store screen.
11. Select **Automatically select the certificate store based on the type of certificate**, and click **Next**.

    The Certificate Import Wizard displays the Completing the Certificate Import Wizard screen and the specified settings.
12. Click **Finish**.

    Internet Explorer displays an **Importing** dialog box:

Note: If the security level displayed in the **Importing** dialog box is not set to **High**, you may want to protect the certificate with a password, a process that can take place only during importing. To create a certificate password, skip the remaining importing instructions and follow the steps in "Creating a Certificate Password in Internet Explorer" on page 1-26.

13. Click **OK**.

Internet Explorer displays a successfully imported message.

14. Click **OK**.

Internet Explorer displays the imported certificate in the list of certificates on the **Personal** tab of the **Certificates** dialog box.

Creating a Certificate Password in Internet Explorer

CAUTION: If a certificate password is forgotten, the certificate cannot be used. This password is stored on the local machine as a hash and cannot be accessed. If the password is forgotten, the certificate holder must register for a new certificate. CDC recommends that this password be recorded and stored in a locked location.

In Internet Explorer, assigning a password to a certificate can take place only during the importing process. To create a certificate password, begin by importing the certificate using the steps in "Importing in Internet Explorer" on page 1-24.

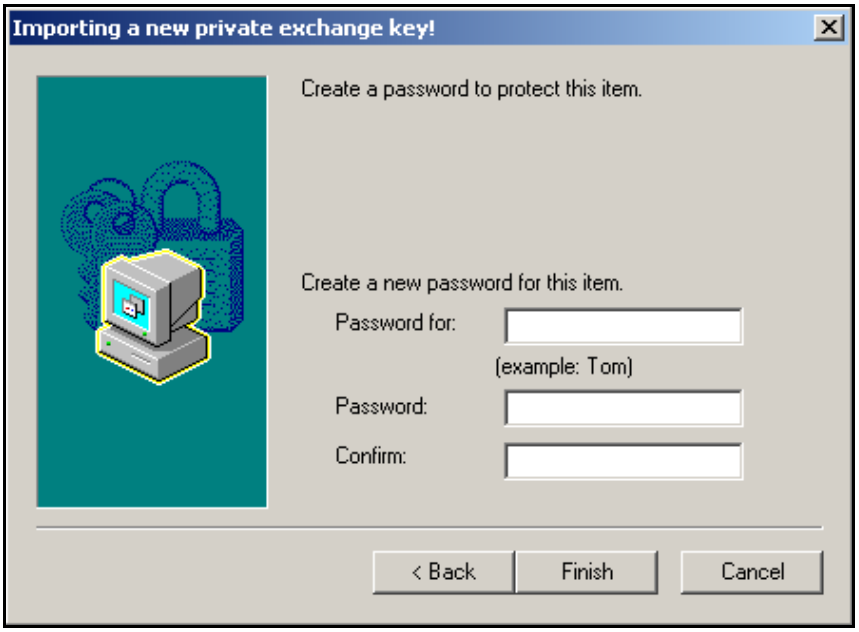
To create a certificate password in Internet Explorer, do the following:

1. If the security level displayed in the **Importing** dialog box is not set to **High**, click the **Set Security Level** button:

Internet Explorer displays the Choose a security level appropriate for this item screen:

2. Select **High** and click **Next**.

Internet Explorer displays the Create a password to protect this item screen:



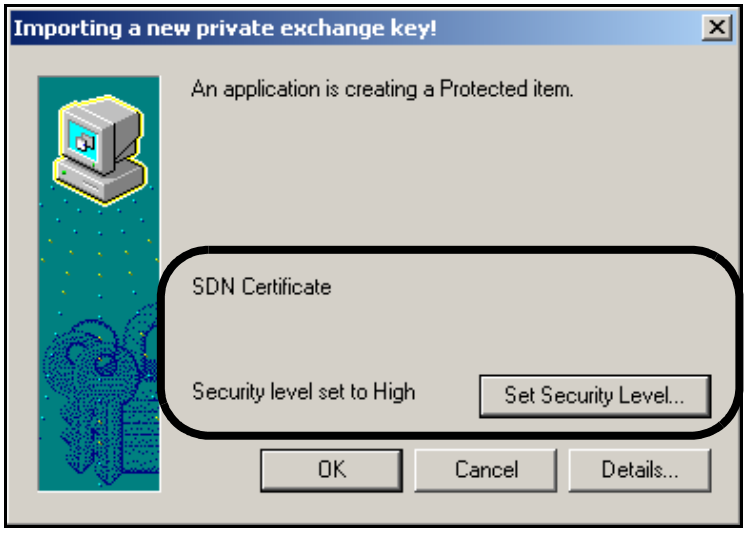
3. Enter a name for the certificate in the **Password for** field.

For example, enter *SDN Certificate*.

4. Enter the password you want to create for the item in the **Password** and **Confirm** fields.

5. Click **Finish**.

   Internet Explorer returns to the **Importing** dialog box and displays the name of the certificate along with the new security level:



6. Click **OK**.

Importing in Netscape

Importing in Netscape applies to both downloaded and exported certificates. If you are importing a certificate stored on an external device, such as a flash drive or disk, insert the external storage device into the appropriate drive or port before proceeding.

To import a digital certificate into Netscape, do the following:

1. Open Netscape, click the **Edit** menu, and select **Preferences**.
2. In the **Preferences** dialog box, expand the **Privacy & Security** category, and click **Certificates**.
3. Click the **Manage Certificates** button.

   Netscape displays the **Certificate Manager** dialog box.
4. Click the **Your Certificates** tab, if not already displayed.
5. Click **Import**.

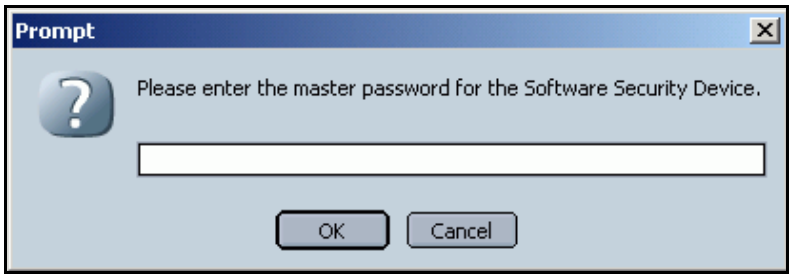
   Netscape displays the **File Name to Restore** dialog box.
6. Navigate to the location of the digital certificate and double-click the file name.

   Note: You can also enter the drive, path, and certificate name in the **File name** box and click **Open**.

   Netscape displays either a password prompt or the **Change Master Password** dialog box.

7. Do one of the following:

- If a master password has been established for this browser, enter the master password and click **OK**:



- If a master password is not in use and you want to protect the certificate with an additional password, create a master password by following the procedures found in "Creating a Master Password in Netscape" on page 1-30.
- If a master password is not in use and you do not want to establish a password for the browser, click **Cancel** and then confirm your decision in the message Netscape displays.

Netscape displays a **Password Entry** dialog box for the digital certificate:

8. Do one of the following:

- If you are importing a downloaded certificate, enter the password downloaded with the certificate.
- If you are importing an exported certificate, enter the password created during the exporting process.

9. Click **OK** to complete the import process.

Netscape displays a successfully restored message:

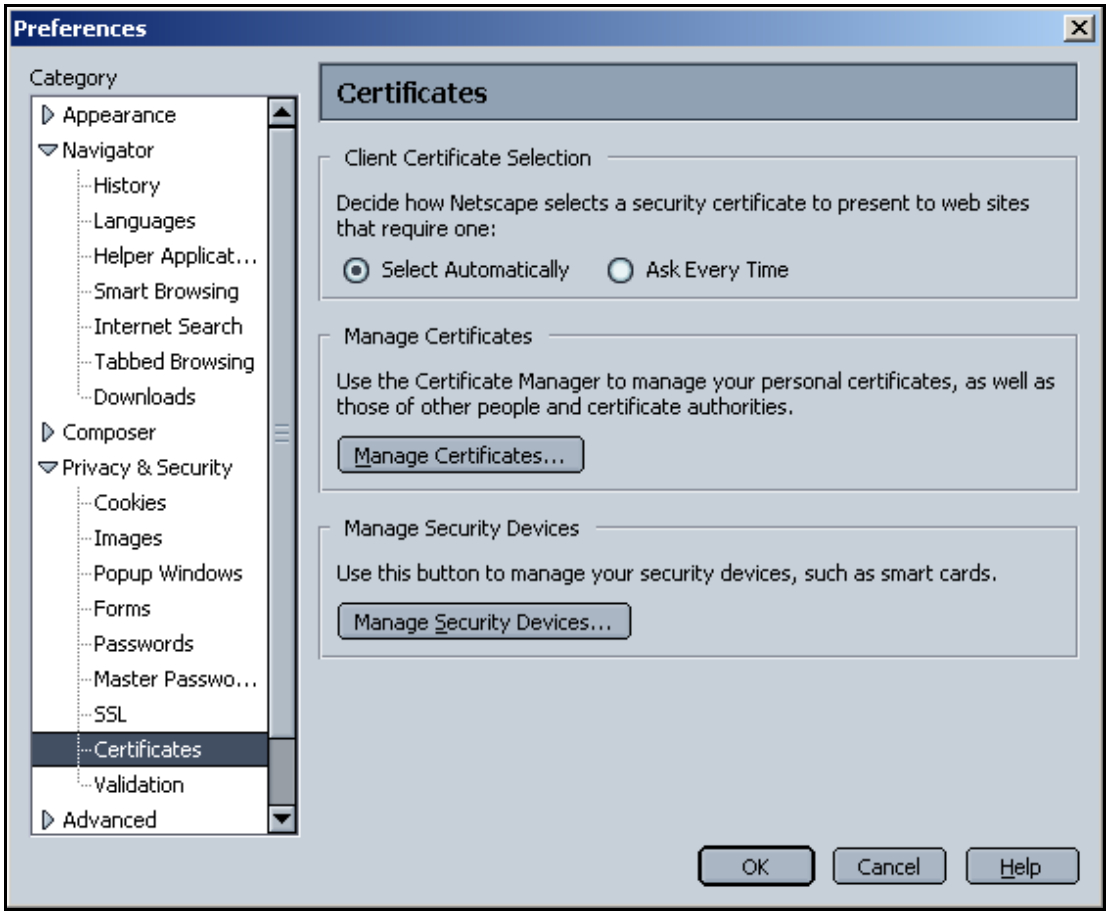
10. Click **OK**.

Netscape displays the imported certificate on the **Your Certificates** tab of the **Certificate Manager** dialog box.

Verifying Certificates Stored in Netscape

To verify the certificates you have successfully imported and stored in Netscape, do the following:

1. Open Netscape, click the **Edit** menu, and select **Preferences**.
2. In the **Preferences** dialog box, expand the **Privacy & Security** category, and click **Certificates**:



3. Click the **Manage Certificates** button.

   Netscape displays the **Certificate Manager** dialog box.
4. Click the **Your Certificates** tab, if not already displayed.
5. Select the SDN certificate in the list, and select **View**.

   If the SDN certificate is not displayed, the certificate failed to import. If repeated attempts to import the certificate fail, you must register for a new certificate.

Creating a Master Password in Netscape

To create a master password in Netscape for stored certificates, do the following:

1. Open Netscape, click the **Edit** menu, and select **Preferences**.
2. In the **Preferences** dialog box, expand the **Privacy & Security** category, and click **Master Password**.

3. Click **Change Password** and enter a password in the **New password** and **New password (again)** fields:

4. Click **OK**.

   Netscape displays a confirmation message:

5. Click **OK**.

   Note: Store this password in a secure location. If the Master Password is forgotten, it must be reset. All stored certificates are lost when the master password is reset.

Configuring a Browser for Automatic Certificate Selection

Internet Explorer and Netscape can be configured to bypass the certificate selection window and automatically select a certificate when only one exists in the certificate store. Completing this procedure eliminates one of the windows requiring a response when accessing the SDN. Depending upon the browser, follow the procedures in "Configuring Internet Explorer" on page 1-31 or "Configuring Netscape" on page 1-32.

Configuring Internet Explorer

To configure Internet Explorer to skip the certificate selection prompt if only one certificate is installed, open Internet Explorer and do the following:

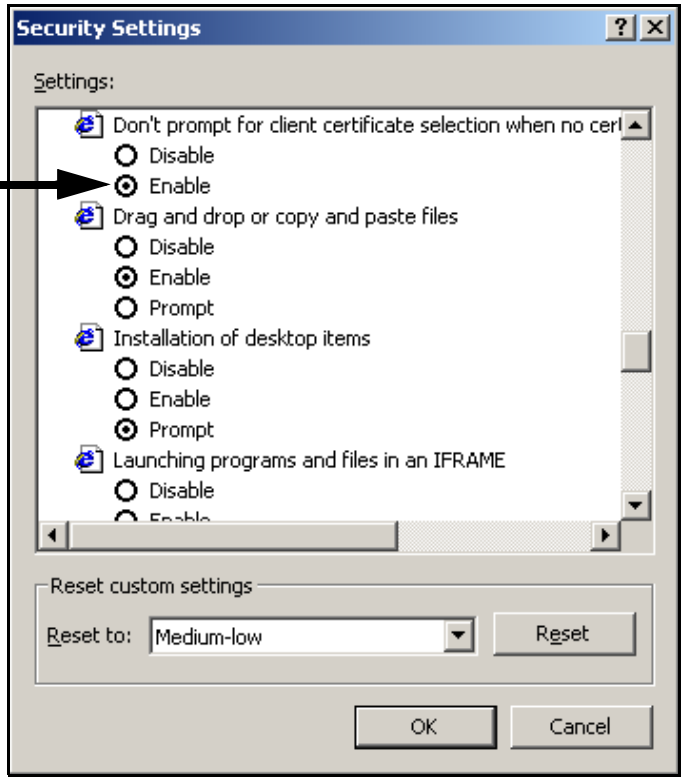
1. Click the **Tools** menu and select **Internet Options**.

   Internet Explorer displays the **Internet Options** dialog box.

2. Click the **Security** tab, and then click the **Custom Level** button.

   Internet Explorer displays the **Security Settings** dialog box.

3. Scroll to the **Don't prompt for client certificate selection when no certificate or only one certificate exists** setting and select **Enable**:



4. Click **OK** to close the **Security Settings** dialog box.

   Internet Explorer displays a warning message.

5. Click **Yes** to close the message.

6. Click **OK** to close the **Internet Options** dialog box.

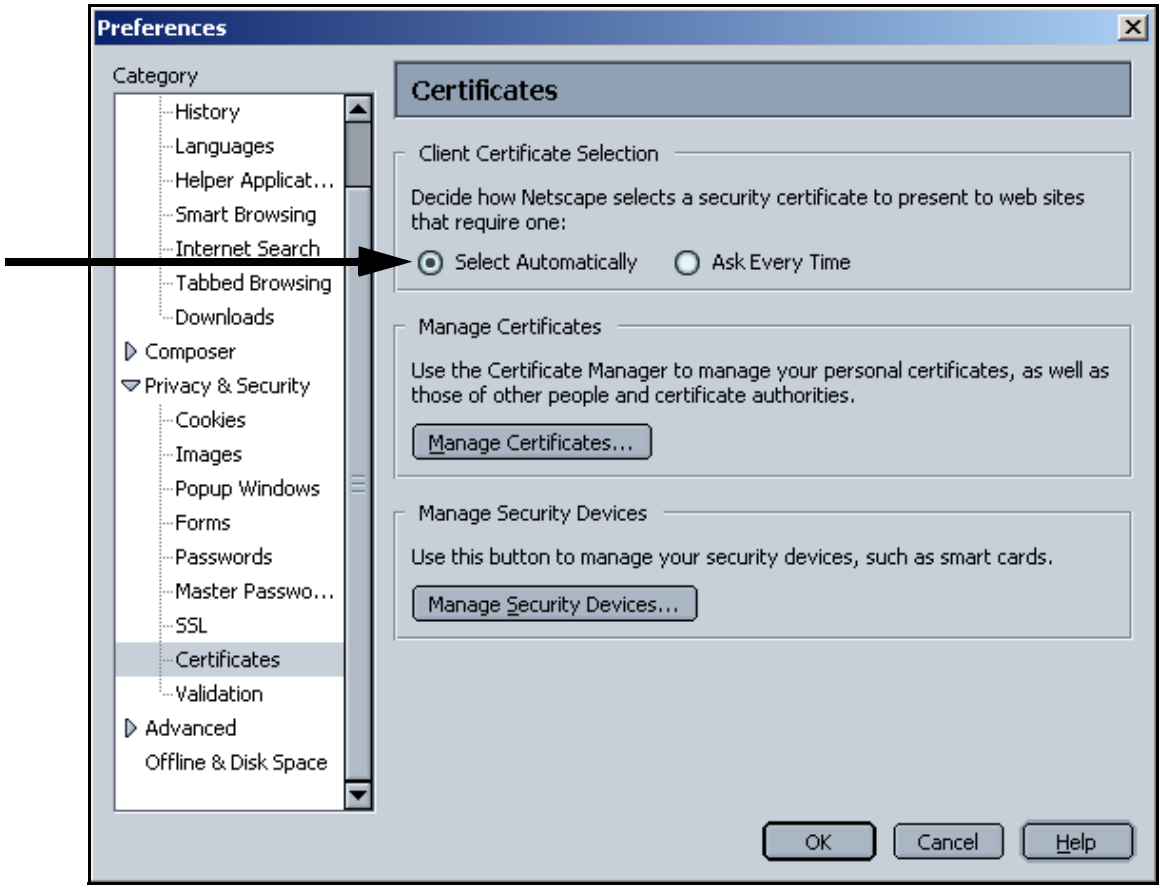
Configuring Netscape

To configure Netscape to skip the certificate selection prompt if only one certificate is installed, open Netscape and do the following:

1. Click the **Edit** menu, and select **Preferences**.

2. In the **Preferences** dialog box, expand the **Privacy & Security** category, and click **Certificates**.

3. In the **Client Certificate Selection** area of the **Certificates** panel, select the **Select Automatically** option:



4. Click **OK** to save the Certificates settings.

Accessing the SDN

Accessing Program Activities

To access the SDN and program activities, do the following:

1. Enter *https://sdn.cdc.gov* into the **Address** box of the appropriate browser and press **Enter**.

   The browser may display a list of available certificates. If only one certificate is installed on the browser, this list can be bypassed. Refer to "Configuring a Browser for Automatic Certificate Selection" on page 1-31 for details.

2. If the browser displays a list of available certificates, select the SDN certificate from the list and click **OK**.

   The browser may display a password dialog box if a certificate or master password was established.

3. If the browser displays a certificate or master password dialog box, enter the appropriate password and click **OK**.

The browser displays the Login page:

4. Enter the SDN challenge phrase and click **Submit**.

Note: If you forget the challenge phrase, follow the procedure listed in "Forgotten Passwords" on page 1-42.

The browser displays the CDC Public Health Partners page and the available program activities:

5. Click the appropriate activity.

Note: For a graphical overview of the steps used to access the SDN, see "Overview of the Steps Required to Access the SDN" on page 1-45.

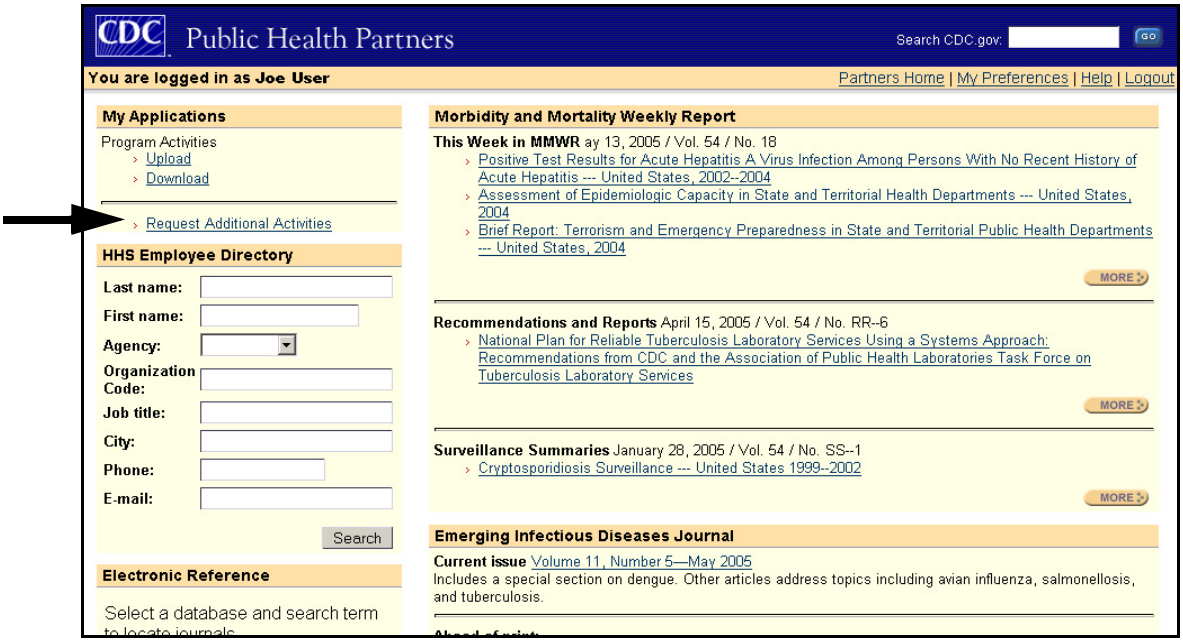
Additional SDN Functions

Requesting Additional Programs and Activities

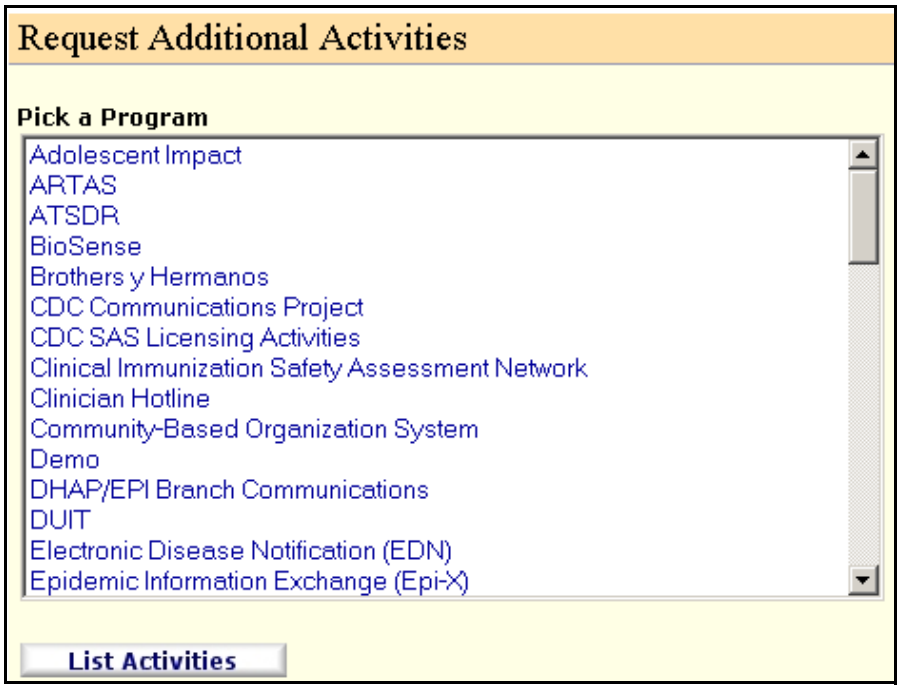
If you already have an SDN-issued digital certificate for another program, do not register for another certificate; one certificate can be used for multiple programs. If you complete another certificate registration when a certificate has already been issued to you, the PDCA may not issue you a new certificate; instead, you may be directed to the procedures described in this section.

To request additional programs and activities, log in to the SDN as described in "Accessing the SDN" on page 1-33, and do the following:

1. From the CDC Public Health Partners home page, click the **Request Additional Activities** hyperlink displayed under the list of activities:

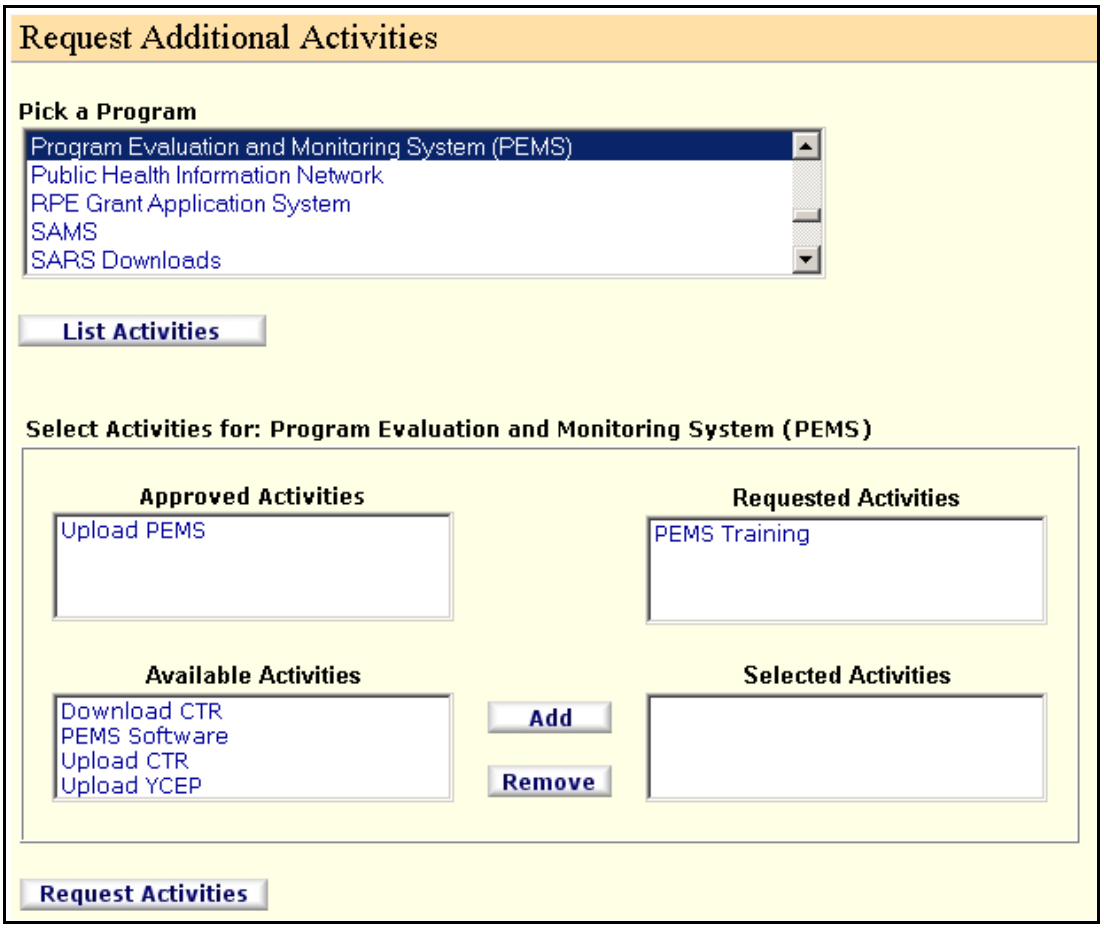


The browser displays the Request Additional Activities page and the **Pick a Program** list:



2. Select the appropriate program from the list and click **List Activities**.

The browser displays lists for selecting additional activities:



3. Select the desired activity from the **Available Activities** list and click **Add**.

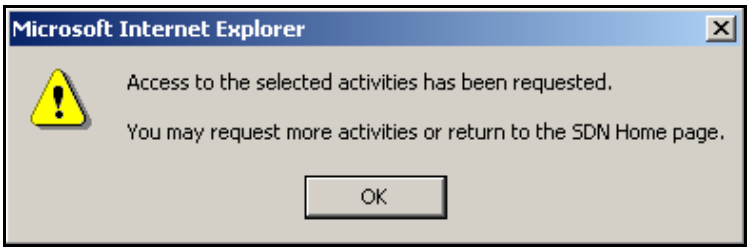
Note: Repeat step 3 to add additional activities from the selected program.

4. Click **Request Activities**.

The browser displays a confirmation message.

5. Click **OK**.

The request is sent to the appropriate PDCA for approval, and the browser displays a confirmation message:



6. Click **OK**.

Updating the Challenge Phrase

This function is available after you successfully log in to the SDN. It is used to change your challenge phrase for security purposes. This function differs from that described in "Forgotten Challenge Phrase" on page 1-42 in that updating the challenge phrase with this function will not deactivate your approved activities.

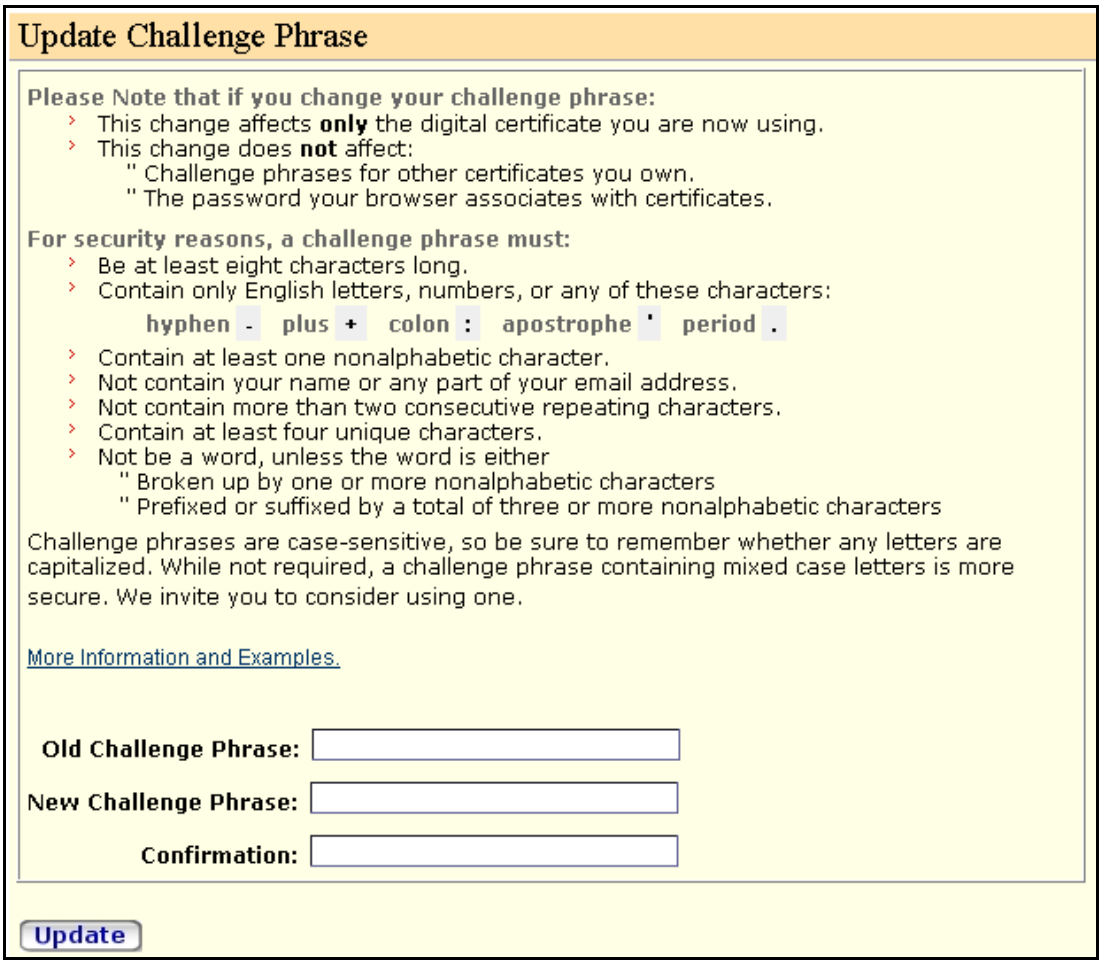
To change the challenge phrase, log in to the SDN as described in "Accessing the SDN" on page 1-33 and do the following:

1. From the CDC Public Health Partners home page, click **My Preferences**:

The browser displays the My Preferences page.

2. Click **Update Challenge Phrase**.

The browser displays the Update Challenge Phrase page:



3. Enter the current challenge phrase in the **Old Challenge Phrase** field.
4. Enter the new challenge phrase in the **New Challenge Phrase** and **Confirmation** fields.

   Note: Follow all of the challenge phrase creation rules described in "Creating a Challenge Phrase" on page 1-8.
5. Click **Update**.

   If the new challenge phrase is accepted, the browser displays a message to that effect:

The new challenge phrase will be effective the next time you log in to the SDN.

Note: It is strongly recommended that you record the new challenge phrase and store it in a locked, safe place.

6. Click **Return To Activity List Page** to return to the CDC Public Health Partners home page.

Updating Personal Information

Should you need to change the personal information submitted when registering for the digital certificate, follow the procedures described in this section. Keep the personal information associated with a digital certificate up to date. The e-mail address is especially crucial because CDC sends the notice for the annual renewal of the certificate to the listed e-mail address. In addition, an accurate phone number is helpful to CDC and SDN staff should they need to contact the certificate owner.

To update personal information, log in to the SDN as described in "Accessing the SDN" on page 1-33 and do the following:

1. From the CDC Public Health Partners home page, click **My Preferences**:

The browser displays the My Preferences page.

2. Click **Update Personal Information**.

The browser displays the Update Personal Information page:

Update Personal Information

Items with (*) are required.

Prefix		Preferred Name	
* First Name	Joe	Middle Name	
* Last Name	User	Degree	
* Email Address	jju55@cdc.gov	CDC User ID (where applicable)	
* Employer	CDC	Program or Division	DHAP
* Employer Type	Other		
* Job Type	Other		
* Phone	4045551122	Fax	4045551112
Work Address (130 characters maximum)	8 CDC Boulevard Building 10, Room 21 Atlanta, GA 30329	* U.S. State (required for US)	Georgia
		U.S. County	DE KALB
* City	Atlanta	* Zip Code	30329
* Country	United States		
* Alternate Contact :			
* Name	Jane Supervisor	* Phone	4045551133

Update Reset

3. Update entries in any of the fields to reflect current information.
4. When finished, click **Update**.

   Note: To restore the original information instead of updating, click **Reset**.

If your personal information is successfully updated, the browser displays a message to that effect:

5. Click **Return To Activity List Page** at the bottom right of the message.

Forgotten Passwords

Forgotten Certificate Password or Master Password

If you forget a certificate or master password, it cannot be recovered. These passwords are stored on the same local machine as the digital certificate. No one at CDC or locally can access the password. For this reason, you should record and store the password in a secure location as soon as it is created.

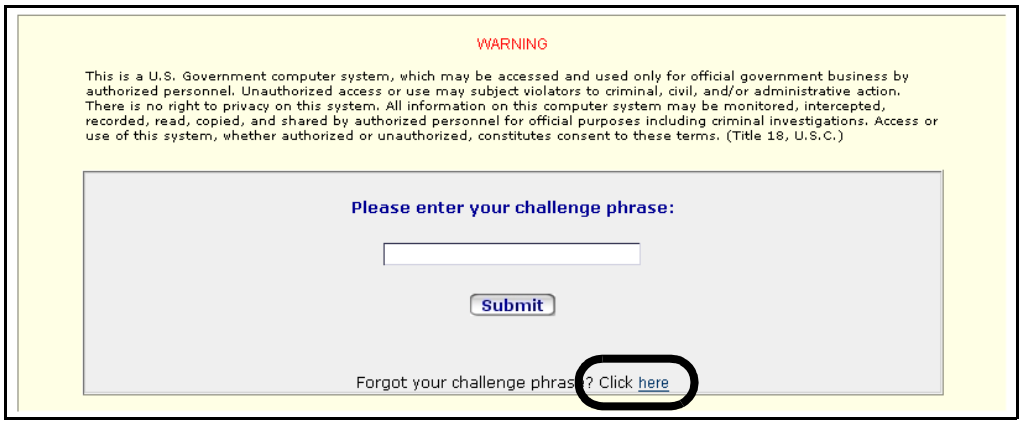
If a certificate or master password is forgotten, the PDCA must revoke the current certificate, and you must register for a new certificate. Contact the program's support team to inform them of the situation and ask them to revoke the current certificate.

Forgotten Challenge Phrase

If you forget the challenge phrase, you must establish a new one before access to the SDN system can be granted. The process of requesting a new challenge phrase begins at the SDN Login page and continues on the Forgotten Challenge Phrase page.

To submit a new challenge phrase, access the SDN Login page as described in "Accessing the SDN" on page 1-33 and do the following:

1. At the bottom of the page, click the "Click **here**" hyperlink:



The browser displays the Forgotten Challenge Phrase page. At the bottom of the page are two fields on the Create New Challenge Phrase form for entering and confirming a new challenge phrase:

Create New Challenge Phrase:

If you change your challenge phrase:

- This change affects **only** the digital certificate you are now using.
- This change does **not** affect:
  - ? Challenge phrases for other certificates you own.
  - ? The password your browser associates with certificates.

For security reasons, a challenge phrase must:

- Be at least eight characters long.
- Contain only English letters, numbers, or any of these characters:
  - hyphen - plus + colon : apostrophe ' period .
- Contain at least one nonalphabetic character.
- Not contain your name or any part of your email address.
- Not contain more than two consecutive repeating characters.
- Contain at least four unique characters.
- Not be a word, unless the word is either
  - ? Broken up by one or more nonalphabetic characters
  - ? Prefixed or suffixed by a total of three or more nonalphabetic characters

Challenge phrases are case-sensitive, so be sure to remember whether any letters are capitalized. While not required, a challenge phrase containing mixed-case letters is more secure. We invite you to consider using one.

More Information and Examples.

New Challenge Phrase: [ ]

Confirmation: [ ]

Submit Back

2. Enter the new challenge phrase in both fields and click **Submit**.

Note: Follow all of the challenge phrase creation rules described in "Creating a Challenge Phrase" on page 1-8.

After the password change is submitted, the browser displays a message from the SDN system indicating that the challenge phrase was successfully updated; however, all activities are suspended until the PDCA approves your request.

Contact the PDCA by phone in order to assure the PDCA that you, the legitimate certificate holder, requested the change and not someone else. This could happen if the certificate holder did not protect the certificate with a password. It is the certificate holder's responsibility to verify that the new challenge phrase has been approved. The SDN does not send an e-mail notification when the changed challenge phrase is approved by the PDCA.

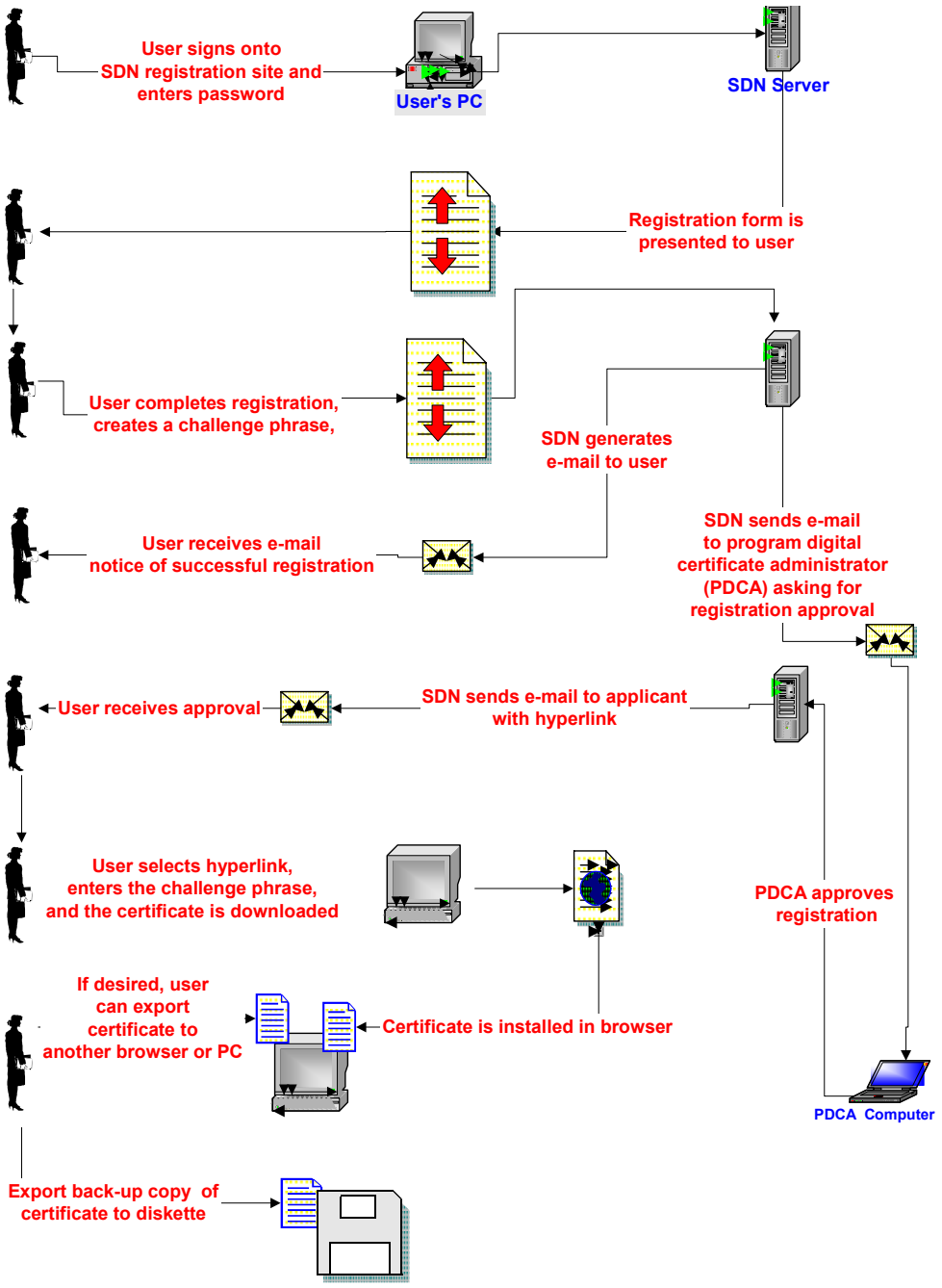


Figure 1

Overview of the Digital Certificate Registration Process

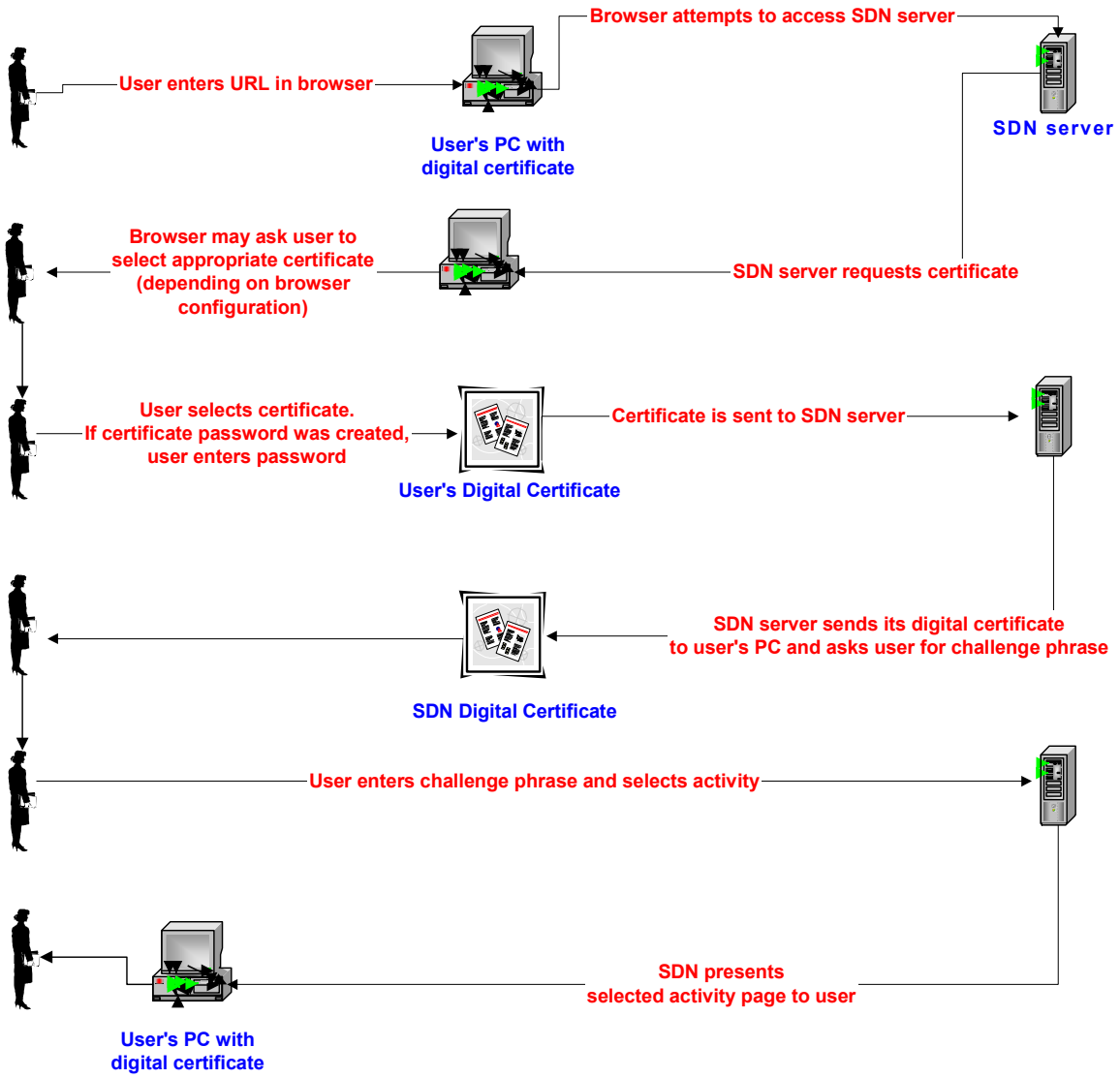


Figure 2

Overview of the Steps Required to Access the SDN

Notes: