



**BRITISH
COLUMBIA**
Ministry of Health Services

Accessing the Ministry Secure File Delivery Service (SFDS)

**A Guide for New Users
To SFDS
And Digital Certificate Installation**

May 2004

Preface

Purpose This document provides information and procedures for coordination and system administrative support to users for the *healthnetBC* Web Applications.

Audience This document is intended for users requiring access to Secure File Delivery Service (SFDS) and for Access Administrators who are responsible for receiving and installing digital certificates (required for access), and requesting and distributing Userids and passwords to new users of the service.

Structure This document includes the following chapters.

Introduction Introduces the document

Prerequisites Identifies computer requirements and instructions for accessing *healthnetBC*

Terms and conventions This document uses standard conventions for displaying information.

COURIER Indicates text that you type.

ARIAL BOLD Indicates a label that appears on a screen (for example, a field name or push-button label).

Italics Indicates variable text that you type when entering a command or a citation to another document.

Bold Use this style for emphasis.



Indicates a note to give you additional information or to emphasize a particular procedure.



Indicates a warning or alert. To avoid making an error, you need to pay particular attention to the information contained in these alerts.



Indicates a useful tip or shortcut, which you can use to save time and keystrokes.

Contents

Introduction	5
Access Administrator Roles	5
Understanding Secure Access	5
Public/Private Key Pairs	6
Digital Certificates	6
SSL Protocol.....	7
Directory of Users.....	7
Prerequisites	8
Checking your Web Browser	8
In Internet Explorer:.....	8
In Netscape Navigator:.....	8
Ministry Password Requirements	9
Confidentiality Undertaking	9
Support.....	10
Installing Digital Certificates	10
Prior to Installing the Digital Certificate	10
In Internet Explorer.....	11
In Netscape Navigator.....	12
Accessing the Secure File Delivery Service Web Page	14
Change Password Screen	15
Using the Change Password Screen	15

Introduction

healthnetBC Web Business Services provides convenient web access to basic information about Ministry clients. This information is used in a variety of ways, from determining whether a specific client is eligible for health services, to helping an employer administer employee's Medical Service Plan premiums.

Because of the private nature of the client data, world wide access via web to that data, and the potential for fraud, the system must be certain of user identity and authorization. *healthnetBC* Web Business Services uses two security mechanisms, user IDs and passwords to identify users and digital certificates to ensure that the user is sitting at a valid computer in a trusted organization.

Access Administrator Roles

Access Administrators are responsible for ensuring secure access within the organization. These responsibilities include:

- Requesting new user registration and required permissions,
- Providing, and in some cases installing\removing from computers, the Ministry digital certificates,
- Maintaining current access records by providing *healthnetBC* Access Services (HAS) with all staff changes so that LDAP updates (e.g., modifying, deleting, revoking, of users) can occur. These updates are emailed to *healthnetBC* Access Services via email at Hlth.HnetConnection@gems1.gov.bc.ca,
- Ensuring secure storage of signed Confidentiality Undertakings, for each user accessing *healthnetBC* Web Business Services.

Within the Health Authorities, Access Administrators have been designated.

For some offices outside of the Health Authority (such as Mental Health), *healthnetBC* Access Services (HAS) provides this role.

HSCIS users also have designated Access Administrators.

Each user is responsible for ensuring the security of their own passwords.

Understanding Secure Access

The Internet is an untrustworthy network. To protect confidentiality of information sent over the Internet, and to guard against unauthorized access, *healthnetBC* Web Business Services use SSL encryption and digital certificates. Local PCs must be set up to accept these high-level security techniques.

Encryption is translating data into an unreadable form. It is the most effective way to achieve data confidentiality. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plaintext; encrypted data is called ciphertext. The encrypted data travels over the Internet using the Secure Sockets Layer protocol (SSL).

There are two kinds of encryption. One kind is based on two parties sharing knowledge of a single secret key. The secret key is used both to encrypt and decrypt the data. A problem with secret key encryption is that it is difficult to securely share the secret key between two remote parties.

The other kind of encryption is based on two mathematically related keys; one called the public Key, and the other called the 'private key'. This second kind of encryption is called Public Key encryption.

Public/Private Key Pairs

In Public Key encryption, only the private key can decrypt information encrypted by the Public key, and vice versa. The Public and private keys are related but it is virtually impossible to figure out the private key from the public key. With this mechanism, two parties can safely pass their Public keys to each other over untrusted channels; it is not necessary to protect the Public keys. Then the respective Public keys are used to encrypt private information to be shared between them.

Anyone can know the sender's Public key used to encrypt the message. Only the recipient of the message knows the private key used to decrypt the message. Each party can be comfortable in the knowledge that only the holder of the (closely guarded) private key can decrypt the information.

The recipient's public key travels over the Internet to the sender enclosed in a digital certificate.

Digital Certificates

A digital certificate is a tamper-proof document that contains a public key and some information relating to the identity of the legitimate holder of the related private key. A digital certificate can be used to verify that a user sending a message is who they claim to be and to provide the receiver with the means to encode a reply. The sender's public key and identification is included and encrypted within in the Certificate Authority's (CA) certificate. With the sender's information, the recipient can read the encrypted information and return an encrypted reply.

An organization that issues digital certificates is called a Certificate Authority (CA). For *healthnetBC* Web Business Services, certificates are issued by a Government-operated CA. These certificates are for use with *healthnetBC* Web Business Services only; they intentionally cannot be used by any other organizations.

The Access Administrator will install the digital certificate on all machines used by authorized users. Access is not possible without the digital certificate installed on a machine that requires access to the *healthnetBC* Secure File Delivery Service and web applications. *healthnetBC* Access Services (HAS) distributes digital certificates and the associated passwords to the Access Administrators, for installation of the digital certificate and for advising new users of their Userids and passwords.

SSL Protocol

The Secure Sockets Layer protocol is the most widely accepted Internet authentication and encryption protocol used to set up communication between clients and servers. SSL client software use standard techniques of public key cryptography to check that a server's certificate and public key ID are valid and have been issued by a CA listed in the client's list of trusted CAs. The same is true when a server validates a client's digital certificate.

The SSL protocol includes the SSL record protocol and the SSL handshake protocol. The Record protocol defines the format used to translate the data, and the Handshake protocol involves exchanging a series of messages between server and client to establish connection.

SSL encryption comes in two strengths, 40-bit encryption and 128-bit encryption. The bit size is the length of the cryptographic code within the key. The longer the key, the more difficult it is to break the encryption code. Microsoft and Netscape both offer browsers that enable different levels of encryption. *healthnetBC* servers and clients require the stronger 128-bit encryption.

Directory of Users

We all use directories of one sort or another every time we use the Internet or our own Intranets. The Directory Access Protocol (DAP) is the Internet standard for accessing information in the directory on the Web. LDAP is the Lightweight version for corporations or companies. You can put just about anything into directories including text, photos, URL's, pointers to whatever, binary data or Public key certificates.

The Ministry's LDAP directory authenticates their access clients in conjunction with the SSL Handshake protocol. The directory contains information about the client's server, Public key, certificates serial numbers, and validity periods. When the client is authenticated, the SSL Handshake proceeds and the client is authorized to access the requested resources.

If the certificate has been revoked from the user's entry in the LDAP directory, the server will refuse to authenticate that certificate or establish a connection.

The Access Administrator can request changes to the LDAP (e.g., adding , modifying or deleting, revoking) users by contacting *healthnetBC* Access Services (HAS) at **hlth.hnetconnection@gems1.gov.bc.ca** . *healthnetBC* Access Services (HAS), who create the Userids, passwords, service permission groups and SFDS mailboxes, provide the required LDAP user access maintenance.

Prerequisites

Organizations must apply to and be authorized by the Ministry to access the *healthnetBC* Web Business Services. This access requires a jointly signed Ministry Data Access Agreement, an installed Ministry digital certificate, a Userid and a password.

Checking your Web Browser

One of the following web browsers is required to access the *healthnetBC* Web Business Services:

- Internet Explorer Version 6.0 with 128 bit encryption (**Supported by the Ministry**)
- Netscape Navigator Version 4.5x (or higher) with 128 bit encryption (**Not Supported by the Ministry other than as per the instructions provided in this document**)

User the following steps to determine if your are using 128-bit encryption.

In Internet Explorer:

1. Start Internet Explorer browser.
2. On the toolbar click on **Help** and select **About Internet Explorer** from the drop-down menu.
3. On the pop-up window the version number and cipher strength are the first two lines under the logo.

If your version is less than required above, or cipher strength is listed as 40-bit or 56-bit you will require an update from Microsoft.

4. Click **OK** to return to your browser.
5. Enter the following URL address in your browser address bar and click **GO**.

<http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp>

6. Follow the instructions on the screen and download the correct High Encryption Pack for your particular browser version.

Or - Download the latest version of Internet Explorer with 128-bit encryption included.

7. Exit all programs and restart your computer to activate the encryption pack.

In Netscape Navigator:

1. Start Netscape Communicator browser.
2. On the toolbar click on **Help** and select **About Communicator** from the drop-down menu.
3. Somewhere on the left side of the screen you should see: “**This version supports U.S. security...**”. If it says “**International security**” instead of “**U.S. security**”, then the encryption strength is too weak and the browser must be upgraded

4. Click **OK** to return to your browser.
5. Netscape Navigator is available only with 128-bit encryption for the US and trade approved countries, including Canada. To upgrade to US security, you must upgrade your browser to the a later version.
6. Access Netscape Navigator web page. Follow the instructions on the screen and upgrade your browser version. Be sure to select one that is 4.7x or better and with 128-bit encryption.
7. Close your browser and re-open it to the new version.

Ministry Password Requirements

The Ministry system prompts the user to change the password at the first log in and will prompt the user for a change every 42 days.

These rules apply to passwords:

- Passwords must be six (6) or more characters long
- Passwords must contain at least one number, and at least one alpha character
- Passwords must not be obviously related to the user's name or User ID
- Passwords must never be shared with other users. If your password becomes known by another individual, it should be changed immediately.
- Passwords cannot be reused.

Confidentiality Undertaking

Before being allowed access to *healthnetBC* Web Business Services, each user must sign a confidentiality undertaking (provided your the Access Administrator), in which they promise to treat as confidential all Ministry client information they will have access to. The Access Administrator must confirm this prior to granting user access, and retain the document onsite for auditing purposes.

Users within the **public sector** (hospital employees, etc.) are covered by the *Freedom of Information and Protection of Privacy (FOIPP) Act*, and as such are assumed already to have signed an appropriate confidentiality undertaking, as a requirement of their employment.

Every **private sector** user of *healthnetBC* Web Business Services must sign a pledge or undertaking which binds them to the confidential treatment of all information related to Ministry clients. The Ministry provides private sector organizations with required wording that may be used as a stand-alone undertaking or added to the organization's own confidentiality pledge. Access administrators must ensure that these agreements are signed before granting access to services.

Support

Contact information:

Secure File Delivery Service (SFDS)	Ministry of Health Services HelpDesk (250) 952-1234 HLTH.Helpdesk@gems1.gov.bc.ca
-------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------

The Ministry of Health Services HelpDesk is available each business day from 8:00 a.m. to 5:00 p.m. to provide service support.

Installing Digital Certificates

Each registered user must have the Ministry's digital certificate installed on their machine in order to access *healthnetBC* Web Business Services. Within the Health Authorities, the Access Administrator is responsible for coordinating the installation of the digital certificate. For all other health employers, it is the responsibility of the person receiving the digital certificate to install on the PC which will be transmitting the data and for storing the certificate in a secure place.

healthnetBC Access Services generates the digital certificate (and creates a password), records the information in their database and then emails the certificate to the authorized user.

Ministry of Health Services supports:

- **Internet Explorer Version 6.0**

Netscape Navigator support is no longer provided by the Ministry, other than as far as installing it on the computer.

If you are using a different browser version, the screens presented may not be the same as described within this document. Refer to the Help provided with your browser version in order to complete any activities described in this document.

You must be logged on to your machine at the time the certificate is installed.


Prior to Installing the Digital Certificate

You will receive the digital certificate as an attachment via email from *healthnetBC* Access Services and must first save the file to a secure location on your personal computer or local area network (LAN). Alternately, you can save it to a diskette. Please note the location where you have saved the digital certificate as you will need it to proceed further.

You must also contact the Ministry of Health Services HelpDesk at 250-952-1234 to receive the password for your digital certificate.

In Internet Explorer

If your browser is Microsoft Internet Explorer, read and follow these instructions.

1. Open your **Internet Explorer** browser
2. From the **Tools** menu from the top function bar, choose **Internet Options**.
3. Select the **Content** tab and click the **Certificates** button.
The list box displays certificates that have been imported.
4. Click the **Import...** button.
The **Certificate Manager Import Wizard** is displayed.
5. On the first window, click **Next**.
The wizard displays the **Select File to Import** screen.
6. Make sure that you have copied the digital certificate from your email attachment to your PC or LAN drive.
Select the file location with the **Browse** button.
In the **Files of Type** field, leave as “Personal Information Exchange .pfx”
7. Scroll through and locate the correct certificate file for *healthnetBC* .
8. Click the **Open** button.
The wizard returns to the **Select File to Import** screen. The certificate file name from the diskette displays in the text box.
9. Click **Next**.
The wizard displays the **Password Protection For Private Keys** screen.
10. Enter the password that was provided to you by the Help Desk. You must phone them to obtain this information.
11. Select the **Enable strong private key protection** check box.
 DO NOT select *Mark The Private Key As Exportable*.
12. Click **Next**.
The wizard displays the **Select Certificate Store** screen. Check to be sure the radio button next to **Automatically select the certificate store based on the type of certificate** is selected.
13. Click **Next**.
The wizard displays the **Completing the Certificate Manager Import Wizard** screen.
14. Click **Finish**.
The import program opens to the **Private Key Container** window.
15. Click the **Set Security Level...** button and set the security level to **Low**. If Low is unavailable, select Medium.
16. Click on **Next**. You are notified that you have selected Low. Click on **Finish**.

17. The import program returns to the Private Key Container screen. Click **OK**.
18. The import is successful. Click **OK**.
19. You are now returned to the Certificates window in your browser. Your certificate should be displayed in the list box. Click **Close** and **OK** to return to your browser.

Deleting a certificate from Internet Explorer

1. Open your **Internet Explorer** browser
2. From the **Tools** menu from the top function bar, choose **Internet Options**.
3. Select the **Content** tab and click the **Certificates** button.
The list box displays certificates that have been imported.
4. On the **Personal** tab, select the certificate to be deleted. Click **Remove**.
5. On the **Certificate Manager** dialog box, click **Yes**
6. Click **Close** to return to your browser.

In Netscape Navigator

If your browser is Netscape Communicator, read and follow these instructions.

1. Open your Netscape Navigator browser
2. From the **Communicator** menu on the top function bar, Select **Tools / Security Info**. From the drop down menu.

Or Click the **Security** icon  located on the tool bar.

3. Under the heading **Certificates**, click on **Yours**.

The list box will display certificates that have already been downloaded. There are no certificates on the computer if the list box is very narrow.

4. Click on **Import a Certificate**. You may have to scroll down to the bottom of the screen to find this button.

Your browser may display the **Set up Your Communicator Password** dialog box.



DO NOT CREATE A PASSWORD. This creates a secure area and password protects your certificates within Netscape. Each time you need your certificates you will be requested for your password. If you forget your password, you can not access your certificates.

5. **DO NOT ENTER ANY INFORMATION** (leave all fields blank) and Click **OK**. Your browser will advise you that you did not create a password. Click **OK** to acknowledge.

Your browser displays the **File Name to Import** dialog box.

6. Make sure that you have copied the digital certificate from your email attachment to your PC or LAN drive.

Select the file location with the **Browse** button.

In the **Files of Type** field, select to show **2002** from the drop down list.

7. Scroll through and locate the correct certificate file for *healthnetBC* .
8. Click the **Open** button.

A Password entry dialog box is displayed.

9. Enter in the password that was provided to you by the HelpDesk.
10. Click **OK**.

Your browser displays a notice that the certificate import is complete.

11. Click **OK** to return to the Security info screen.
12. Click **OK** to return to your browser.

Deleting a certificate from Netscape

1. Open your Netscape Navigator browser
2. From the **Communicator** menu on the top function bar, Select **Tools / Security Info**. From the drop down menu.
3. Under the heading **Certificates**, click on **Yours**.

The list box displays certificates that have been imported.

4. Select the certificate to be deleted. Click **Remove** .
5. On the **dialog box**, click **Yes**
6. Click **Close** on the Security Info window to return to your Netscape.

Accessing the Secure File Delivery Service Web Page

The URL for the SFDS web site is <https://hnfile.hnet.bc.ca/>

1. Your Access Administrator will provide you with your Userid and password.
2. The first time you access this site, we suggest that you add it as a bookmark to your list of Favorite sites for easy access the next time that you log in.
3. When you attempt to access the site, you will be prompted to select a digital certificate to use when connecting. Select your organization certificate (which may be the only one you have) and click **OK**.
4. When presented with the Security Alert screen, click on **Yes**.
4. At the login screen, type in your Userid and Password and click on **Login**.
5. The first time you access this site, you will be prompted to change your password. (see the Change Password section later in this chapter for more details.)
6. After logging in to the Secure File Delivery Service web screen, you will be presented with the *healthnetBC* Services Menu, from which you will select your application.

BRITISH COLUMBIA

Contact Us ► Help ?

B.C. Home

Ministry of Health Services

healthnetBC

Exit this e-service ►

Ministry of Health Services

Welcome to the Ministry Secure File Delivery Service

The Secure File Delivery Service (SFDS) uses industry-standard strong encryption to ensure that information sent through this service cannot be read while it is travelling over the Internet. It also uses digital certificates for authentication to reduce the threat of unauthorized access.

Userid:

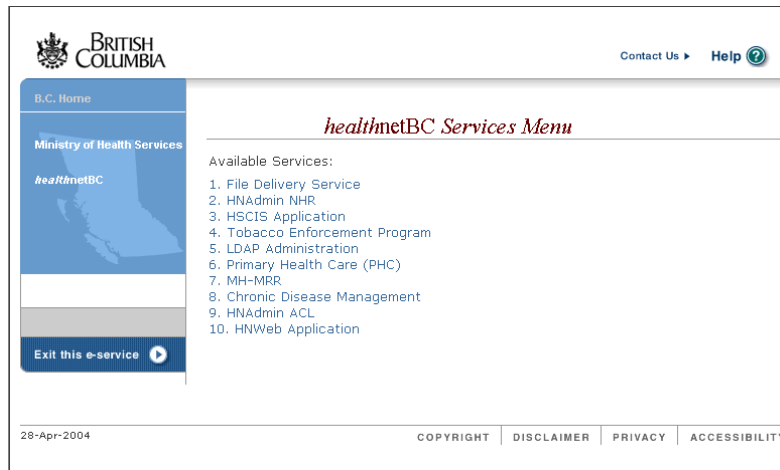
Password:

Login Clear

12-May-2004

COPYRIGHT | DISCLAIMER | PRIVACY | ACCESSIBILITY

Secure File Delivery Service Login Screen



healthnetBC Services Menu Screen

Each user will only see the applications listed that they have access permission to use.

Change Password Screen

The **Change Password** Screen is used to change your password. You will be prompted to change your password the first time you access SFDS, and every 42 days thereafter.

The following rules apply to passwords:

- Passwords must be six (6) or more characters long
- Passwords must contain at least one number, and at least one alpha character
- Passwords must not be obviously related to the user's name or User ID
- Passwords must never be shared with other users. If your password becomes known by another individual, it should be changed immediately.
- Passwords cannot be reused.

Using the Change Password Screen

1. Type your existing password in the *Old Password* text box.
2. Type your new password in the *New Password* text box.
3. Re-type your new password in the *Confirm New Password* text box.
4. Select the **'Start Over'** push button if you have made an error and wish to retype the information.
5. Select the **'Change Password'** push button to change your password.

A message will be displayed indicating that the change of password was successful or identifying the error (i.e., the new password does not conform to the password rules or the New Password and Confirm New Password are different).