



**BRITISH
COLUMBIA**

Ministry of Health Planning
Ministry of Health Services

Accessing the Ministries' Web Business Services

Access Administrator's Guide For Primary Health Care Sites

Installing Digital Certificates with IE 6.0 & Confidentiality Undertakings

Prepared by HealthNet Access Services (HAS)
Information Management Group

February 2003

Version 1.0

Contents

Contents	2
1. Introduction	3
2. About Browser Encryption Strength	3
3. Primary Health Care Access Administrator Responsibilities	3
4. New User Account - Information Required	4
5. Receiving a Digital Certificate through Email	5
6. Installing a digital certificate into a Browser	5
7. Need Help? Had a problem installing the digital certificate?	17
8. Confidentiality Undertaking Document	18

1. Introduction

This guide includes:

- Responsibilities of the Primary Health Care Access Administrator (PHC AA)
- Instructions for installing the provided Ministry of Health Services and Health Planning's digital certificate on to each computer that will be used to access the MOHP\S web business services; and,
- Guidelines for completing a Confidentiality Undertaking. A sample is provided for purposes of customizing, or incorporating into your organization's confidential document.
- Screen displays included in this guide: MOHP\S web business services do not provide HelpDesk support for the use of browsers other than Internet Explorer 6.0. However, if you do use a previous version, the screens presented may not be the same. If this is the case, please reference the Help provided with your version of the browser in order to complete any activities described in this document.

2. About Browser Encryption Strength

The encryption strength of your browser is important. The Ministry of Health Planning and the Ministry of Health Services (hereafter the "MOHP\S") wants to provide strong protection for the personal information that is transmitted. Browsers support either strong encryption or weak encryption. MOHP\S web business services uses strong encryption (128-bit) so your browser must be able to support this stronger encryption level.

To find out the strength of encryption your browser supports, you will need to look at the browser's "Help" menu item called "About Internet Explorer". An "About box" should appear, and in the middle of the box you should see: "Cipher Strength: 128-bit". If it says "40-bit" or "56-bit" instead of "128-bit", then the encryption strength is too weak and the encryption strength of the browser must be upgraded. Visit the Microsoft.com site should you need to upgrade your browser.

3. Primary Health Care Access Administrator Responsibilities

The Primary Health Care Access Administrator ('PHC AA') is responsible for:

- Advising Teleplan Support Centre of any user account updates - requesting new user accounts or editing existing accounts. Clients who change jobs, duties, or leave their organization, and no longer require access to MOHP\S web business services, must have their User IDs revoked. The PHC AA will advise Teleplan Support Centre of these changes, as soon as possible.
- Confidentiality Undertakings – ensuring this is signed and securely stored, for each user
- Digital certificates - installing on each computer and ensuring secure storage of this file.

4. New User Account - Information Required

As the Access Administrator, you can request additional staff members be given access to the PHC web business services. Each new User will be given a User ID and password. To request new user accounts, please send an email to Teleplan Support Centre, at hlth.teleplan@gems1.gov.bc.ca and provide the following information for each user:
(this table may be useful to copy and assist in keeping track of user requests and status)

New User Account - Information required by Teleplan Support Centre:	
Your Organization Name	
Your Organization ID	
User's Full Name	
User's Email Address	
User's Telephone Number	
MSP Payee #	
Security Tasks required for each user accessing PHC web business services:	
Required Action	Completed? Dates, Comments....
Confidentiality Undertaking <ul style="list-style-type: none"> ▪ a confidentiality document must be signed by each user and kept on file, in the event of security audits 	
Digital Certificate Installation <ul style="list-style-type: none"> ▪ each machine used to access the MSP Direct web business services must have a digital certificate installed on it. 	

5. Receiving a Digital Certificate through Email

As the PHC Access Administrator, you will receive the digital certificate, as an attachment (approximately 3kb in size), within an email with the subject line of 'Confirmation of Approved PHC Web Business Service (Cert)', from HealthNet Access Services (HAS).

To Save the Digital Certificate from the email to a diskette:

1. Double-click on the attachment file within the email
2. On the **Opening Mail Attachment** dialog box, select **Save it to disk**
3. Insert a diskette in the machine's floppy drive, and **Save** the file to that drive.

This diskette will be required to install the digital certificate to each machine where users require access to the MOHP\S web business services.

Security Note:

This diskette should be retained in a secured location.

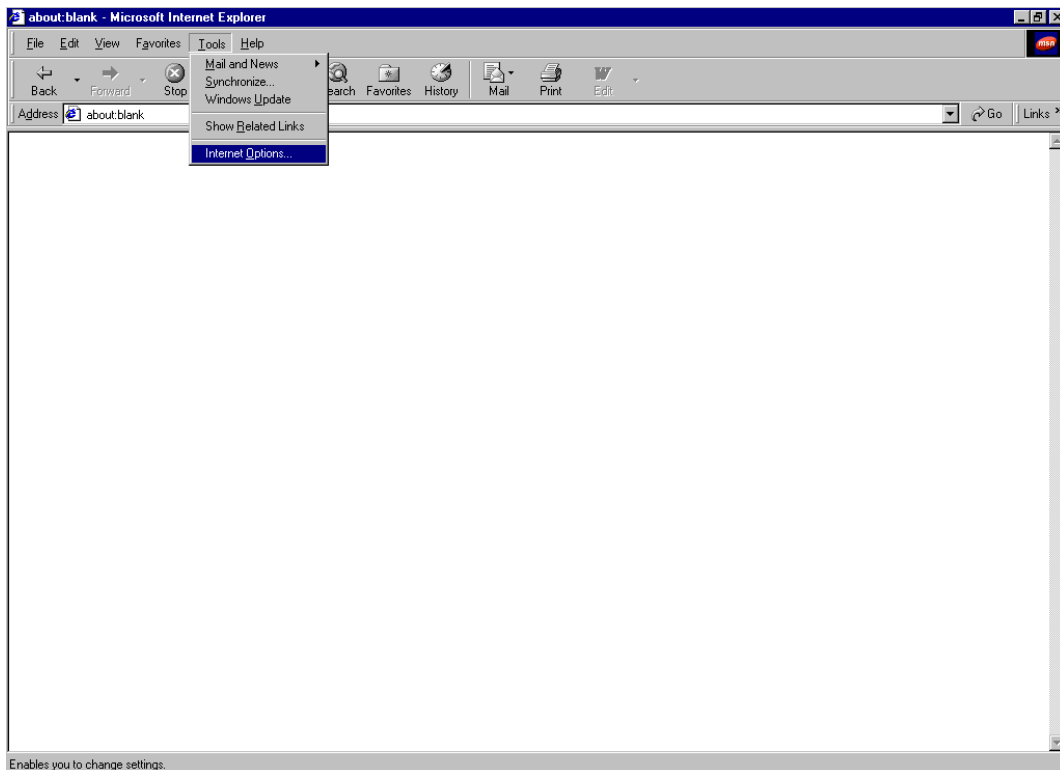
6. Installing a digital certificate into a Browser

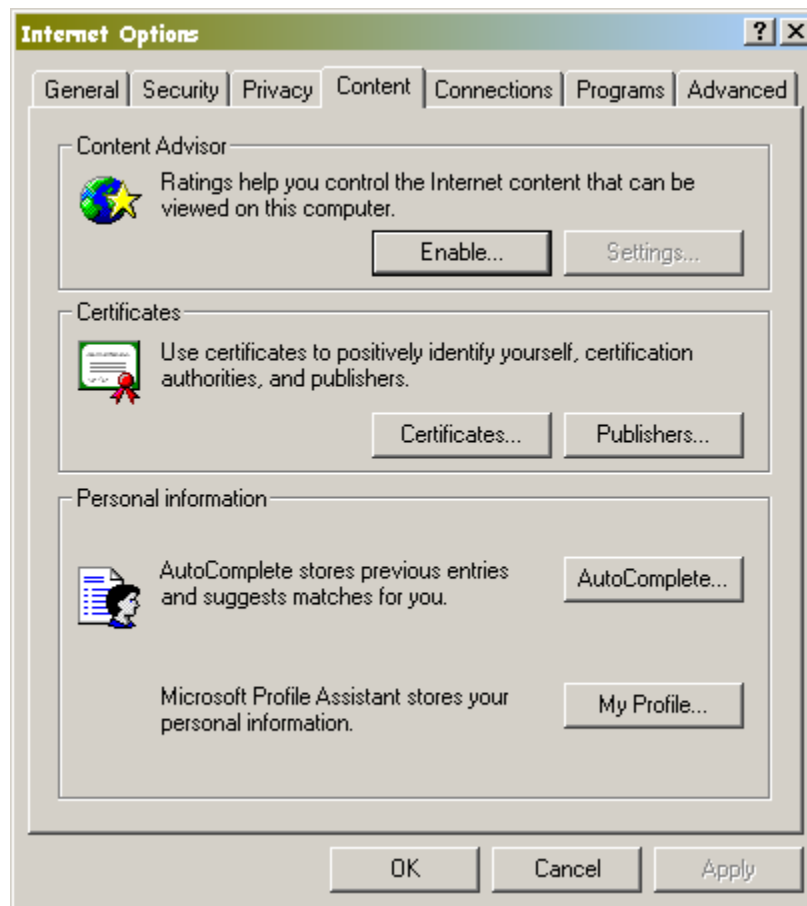
The digital certificate issued to your organization must be installed on all computers that will be used to access the MOHP\S web business services. After phoning and getting your digital certificate password, from the MOHS\P HelpDesk, you are ready to install it to each machine that will be used to access the MOHS\P web business services.

IMPORTANT NOTE:

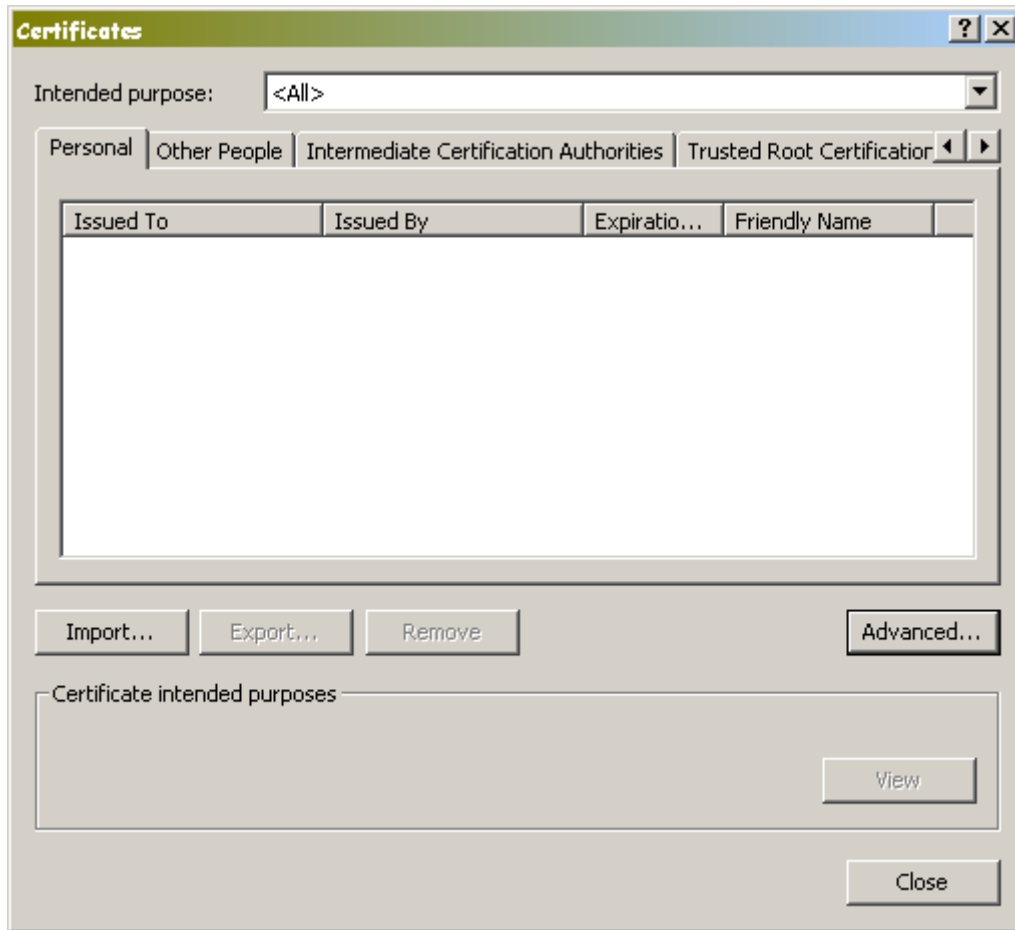
Each user must be logged onto his/her machine, at the time the certificate is installed on that machine.

1. Open **I**nternet **E**xplorer Browser.
2. Click on the **T**ools menu from the top function bar.
3. Choose **I**nternet **O**ptions.





4. Click on the **Content** tab.
5. Click on the [**Certificates...**] button.

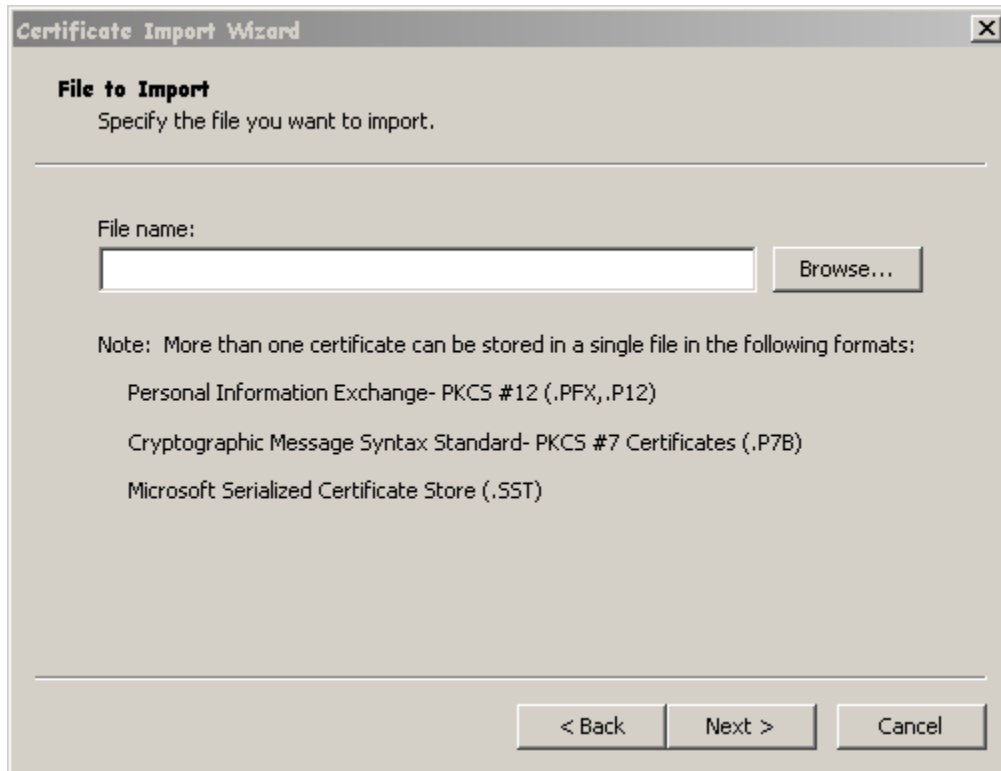


6. Click on the [**I**mport...] button

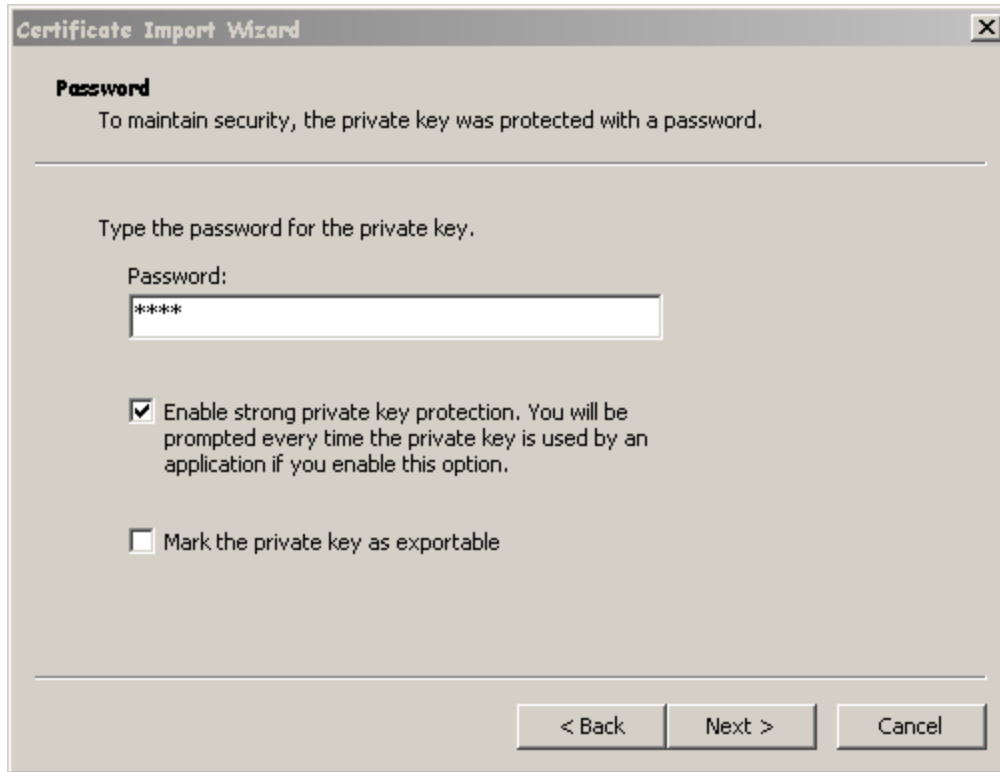
NOTE: Your Browser will present only those certificates that you have imported.



7. Click on the [**N**ext >] button.



8. **Insert the diskette** on which you saved the site digital certificate.
9. Click on the [**Browse...**] button.
10. Select the **3 1/2 Floppy drive**.
11. Ensure that you select **All Files <*. *>** in the **Files of Type** field.
12. Click on your **Certificate** filename.
13. Click on the **Open** button.
14. Click on the [**N**ext >] button.

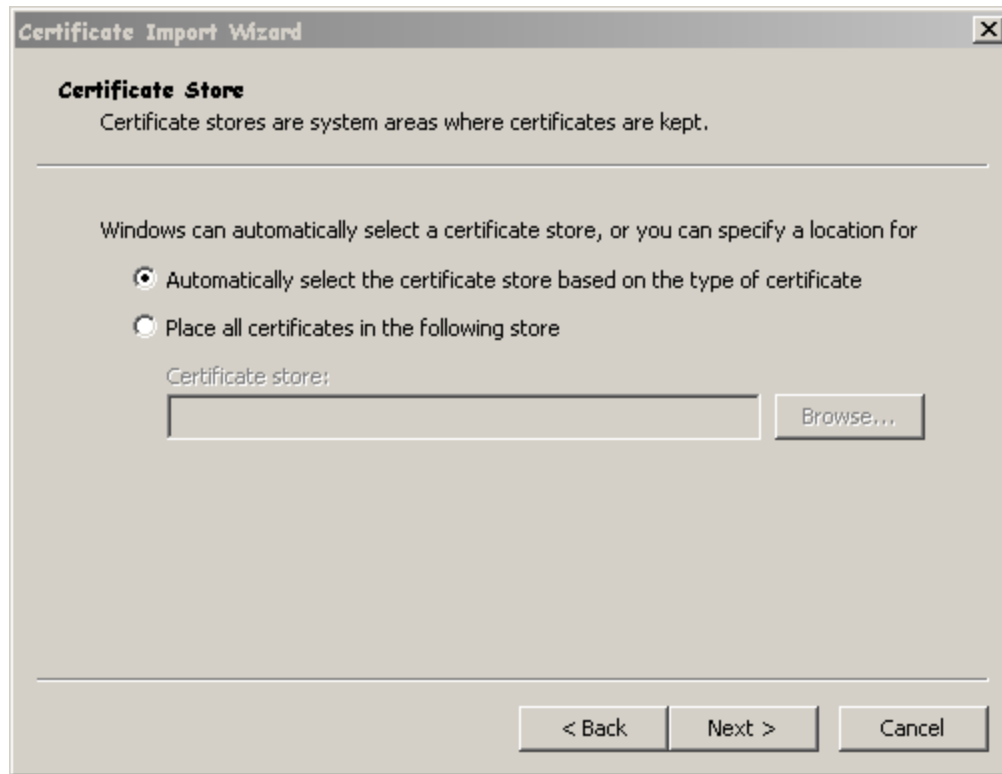


15. **Type in the password** that was provided to you by the HealthNet Access Service's Systems Support Coordinator.
16. Click in the box beside **Enable strong private key protection**, to select that option.

IMPORTANT NOTE:

Do NOT select “Mark the private key as exportable”.

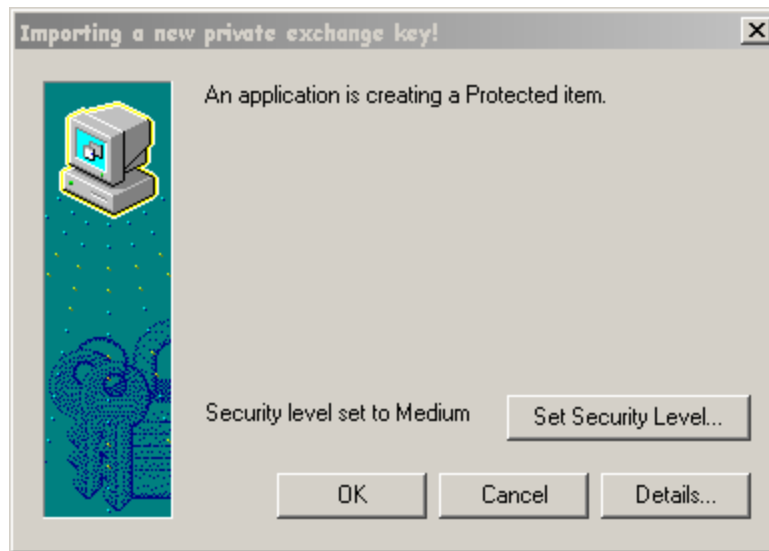
17. Click on the [**N**ext >] button.



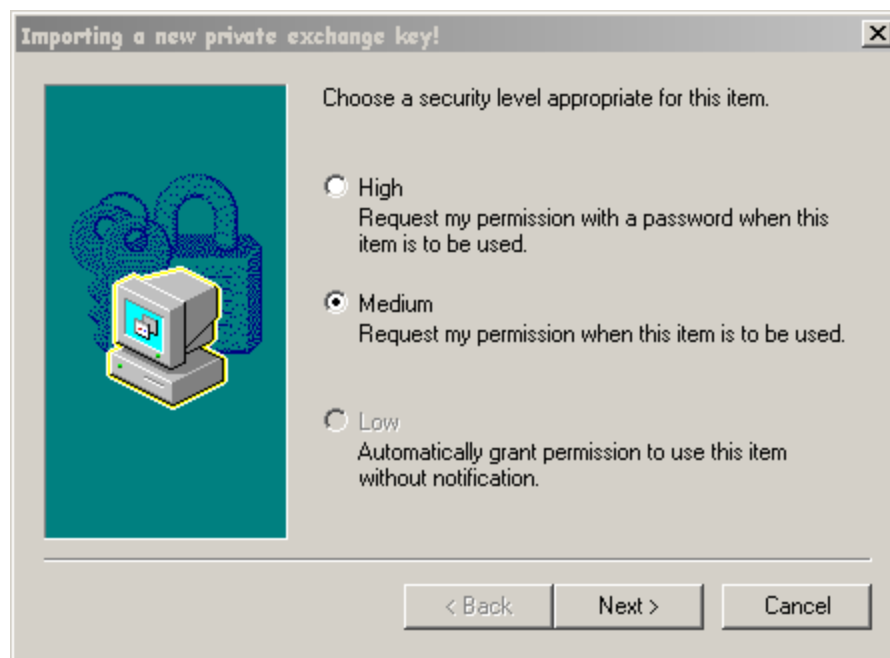
18. Ensure that 'Automatically select the certificate store based on the type of certificate' is selected. Click on the **[Next >]** button.



19. Click on the [**Finish**] button.

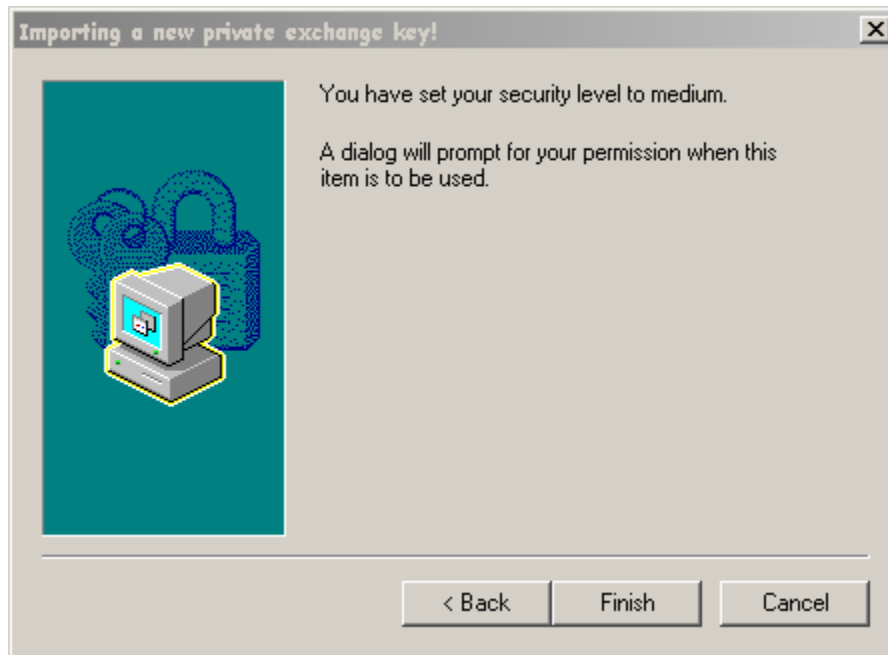


20. Click on the [Set Security Level...] button.



21. Click in the circle beside **Medium**, to select that security level option.

22. Click on the [Next >] button.



23. Click on the [**Finish**] button.

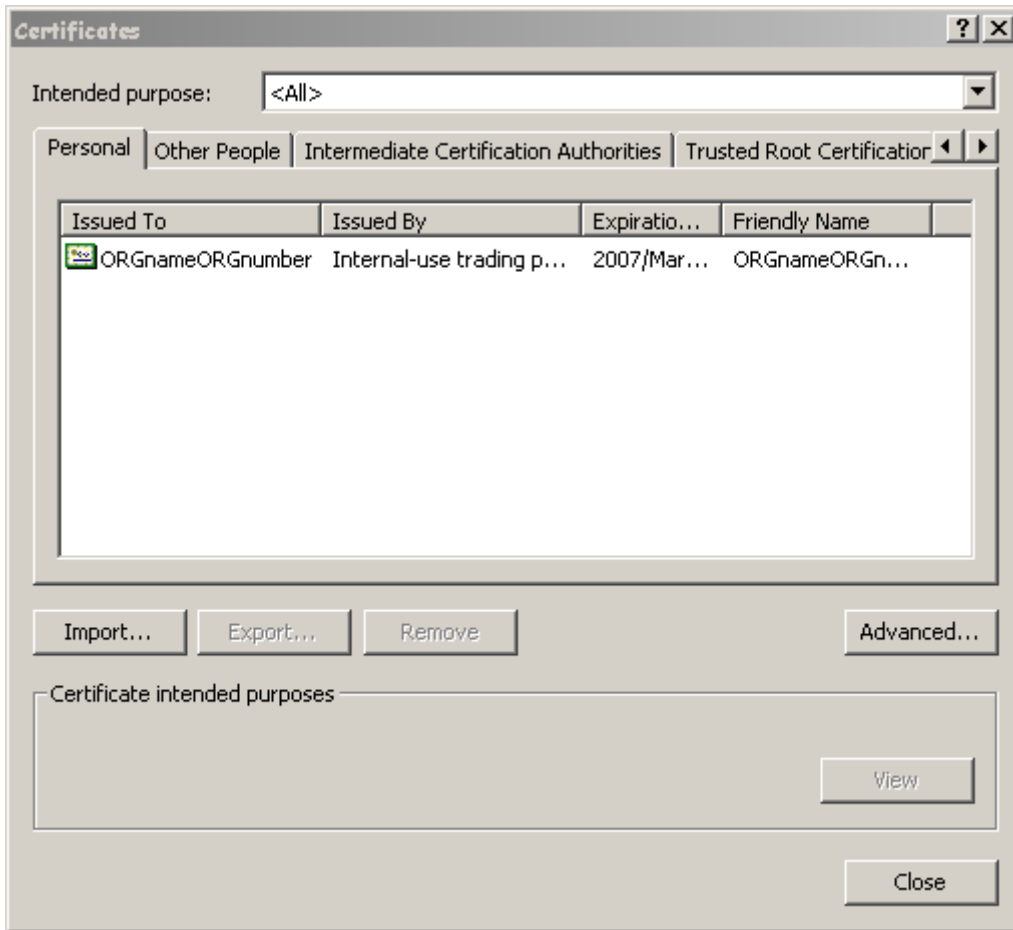


The security level has now been set, and displays on the screen beside the [**Set Security Level**] button

24. Click on the [**OK**] button.

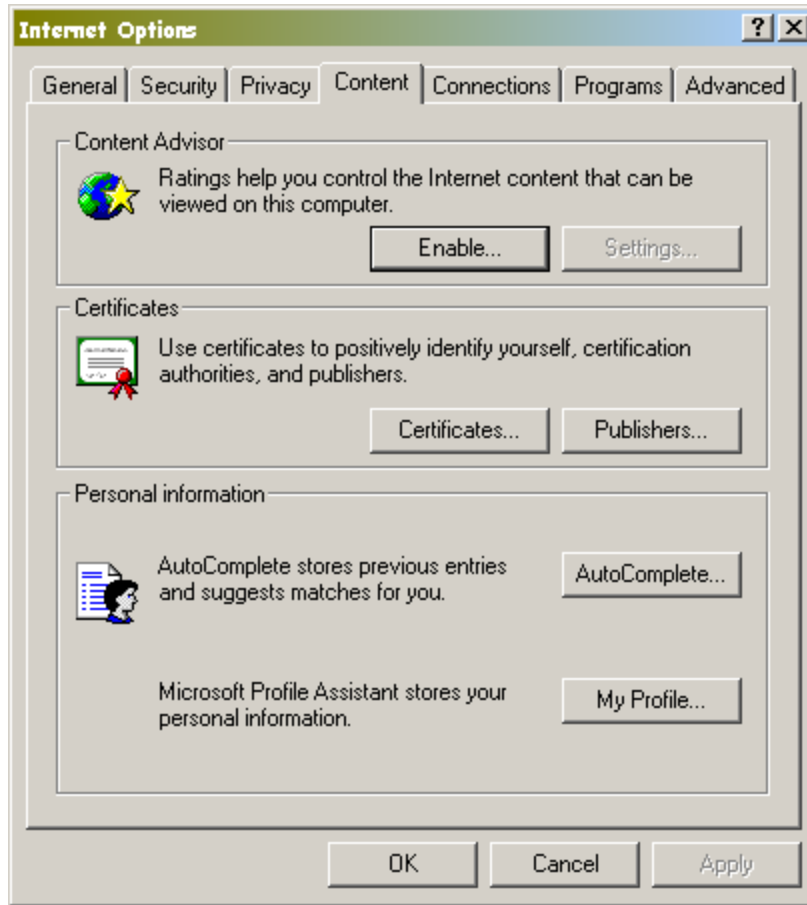


25. Click on the [OK] button.



The import of the digital certificate is now complete.

26. Click on the [Close] button.



27. Click on the [OK] button, to exit Internet Options.

Proceed with further installs of the digital certificate on any other machines that will be used to access the MOHP\S web business services.

7. Need Help? Had a problem installing the digital certificate?

If you experience any problems during the digital certificate installation, please contact the MOHP\S HelpDesk at (250) 952-1234.

8. Confidentiality Undertaking Document

The template on the following page is a sample of the Ministry's Confidentiality Undertaking. The organization **MUST** use this wording, but may choose to either use it as a stand alone confidentiality pledge for their employees, or to incorporate this wording within the organization's existing confidentiality agreement structures.

All users must sign a confidentiality document prior to accessing the MOHS\P web business services.

Signed confidentiality undertakings are to be retained by the organization and used in conjunction with an education program related to privacy and confidentiality of client records.

The organization must produce the signed undertaking for review and audit at the request of the Ministry of Health Planning and Ministry of Health Services.



Ministry of Health Planning
Ministry of Health Services

CONFIDENTIALITY UNDERTAKING

for private sector users who will be accessing
Ministry of Health Planning and Ministry of Health Services' client data

BETWEEN: _____ (the Organization)
(name)

AND: I, _____ (the user)
(name)

WHEREAS:

THE ORGANIZATION HAS ENTERED INTO AN AGREEMENT WITH THE MINISTRY OF HEALTH PLANNING & MINISTRY OF HEALTH SERVICES (MOHP\S) PERMITTING ACCESS TO SPECIFIC CLIENT DATA ON CERTAIN MOHP\S DATABASES; AND

THAT AGREEMENT INCLUDES SECURITY AND CONFIDENTIALITY CLAUSES RESTRICTING THE ACCESS FOR PURPOSES AUTHORIZED BY THE MINISTRY.

I promise to abide by the following terms and conditions:

1. I will not use or access the information in the MOHP\S databases to which I have been granted access, for any purpose other than those which have been authorized by the Ministry of Health Planning and Ministry of Health Services.
2. I will at all times treat as confidential all information related to MOHP\S clients and will not permit the publication, release or disclosure of the same without the prior written authorization of the MOHP\S. For the purpose of this agreement, information related to MOHP\S clients includes, but is not limited to:
 - (i) the individual's name, address or telephone number
 - (ii) the individual's age, gender, marital status or family status
 - (iii) the individual's Personal Health Number (PHN)
3. I will at all times treat as confidential all information related to the security and management of MOHP\S systems and databases.
4. I will adhere to the Medicare Protection Act as it applies to the confidentiality, privacy and security of information related to MOHP\S clients.

UserName	User Signature	Date Signed
Organization Name		
* Witness Name	Witness Signature	Date Signed

** a person within the organization, such as a supervisor or manager.*