



**BRITISH
COLUMBIA**

Ministry of Health Services

Accessing the Ministry Web Business Services

***How to Install Digital Certificates using
Internet Explorer (IE) 6.0***

A Reference Guide for Access Administrators

Prepared by *healthnetBC* Access Services (HAS)
healthnetBC
IST, Knowledge Management & Technology

April 2004

Version 1.1

Contents

Contents	2
1. Introduction.....	3
2. About Browser Encryption Strength.....	3
3. Digital Certificate Management.....	4
4. Installing a digital certificate into a Browser.....	5
5. Need Help? Had a problem installing the digital certificate?.....	16
6. Confidentiality Undertaking Document.....	17

1. Introduction

This guide includes:

- Instructions for installing the Ministry of Health Services digital certificate using Internet Explorer (IE) 6.0.
- Confidentiality Undertakings Guidelines for private sector organizations. A sample is provided to either use as a stand alone confidentiality pledge, or to incorporate into the organization's existing confidentiality agreement.
- 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 Services wants to provide strong protection for the personal information that is transmitted. Browsers support either strong encryption or weak encryption. Ministry 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. Digital Certificate Management

The designated Access Administrator (AA) for your organization is responsible for coordinating the installation of the Digital Certificate on the computers of users authorized to access the MOHP\S web business services, and for ensuring secure storage of the certificate.

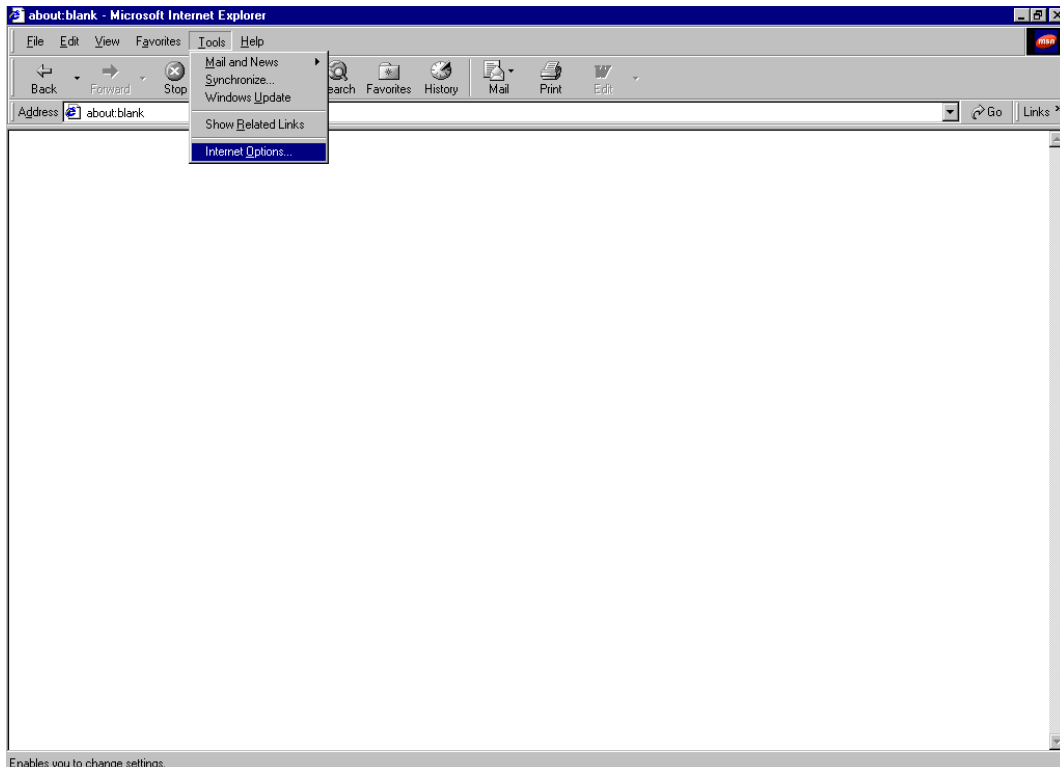
- the Digital Certificate is sent to the Access Administrator as an attachment (approximately 3kb in size) within an email from HealthNet Access Services (HAS).
- the Digital Certificate must be saved from the email to a diskette.
- the Access Administrator must call the Ministry of Health Services HelpDesk at (250) 952-1234 to obtain the digital certificate password.

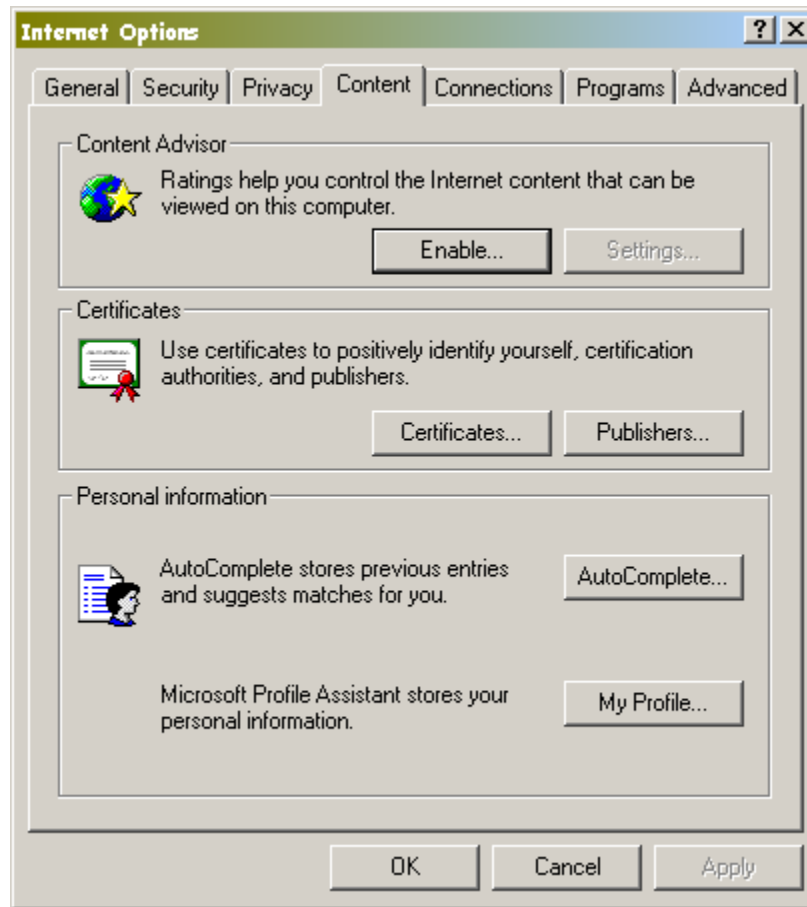
4. Installing a digital certificate into a Internet Explorer (IE) Browser

IMPORTANT NOTE:

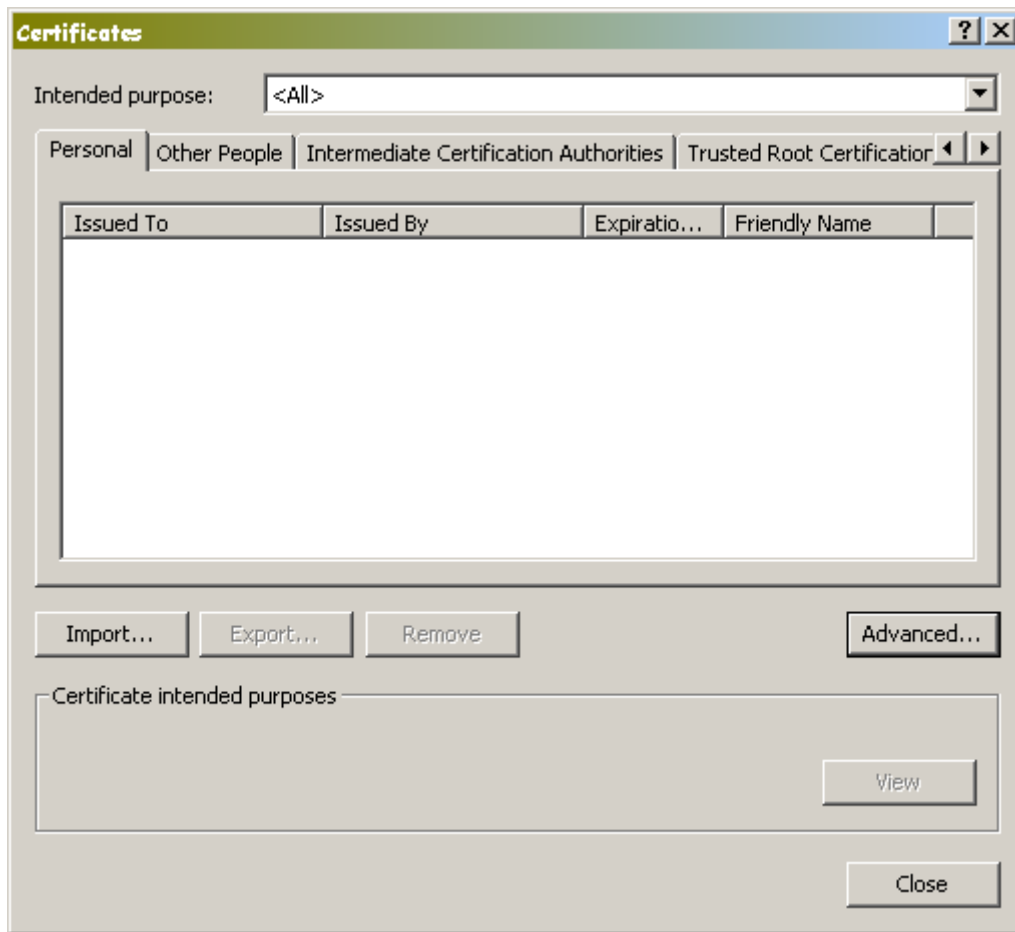
Each user must be logged onto his/her machine, at the time the certificate is installed on that machine.

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





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

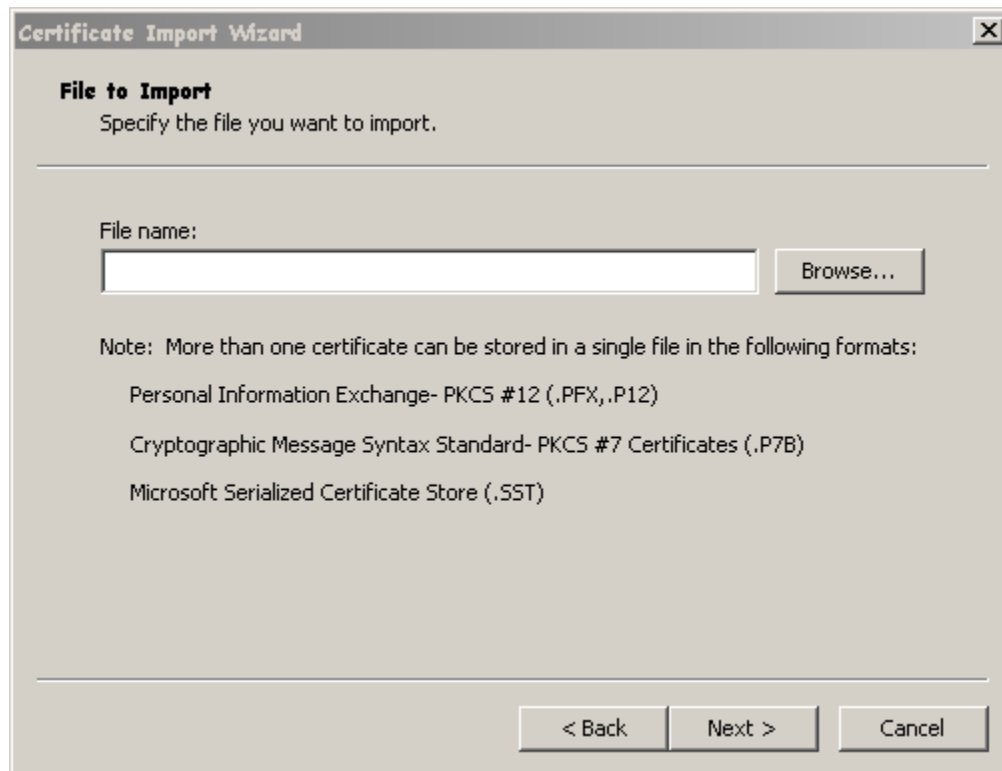


6. Click on the [**I**mport...] button

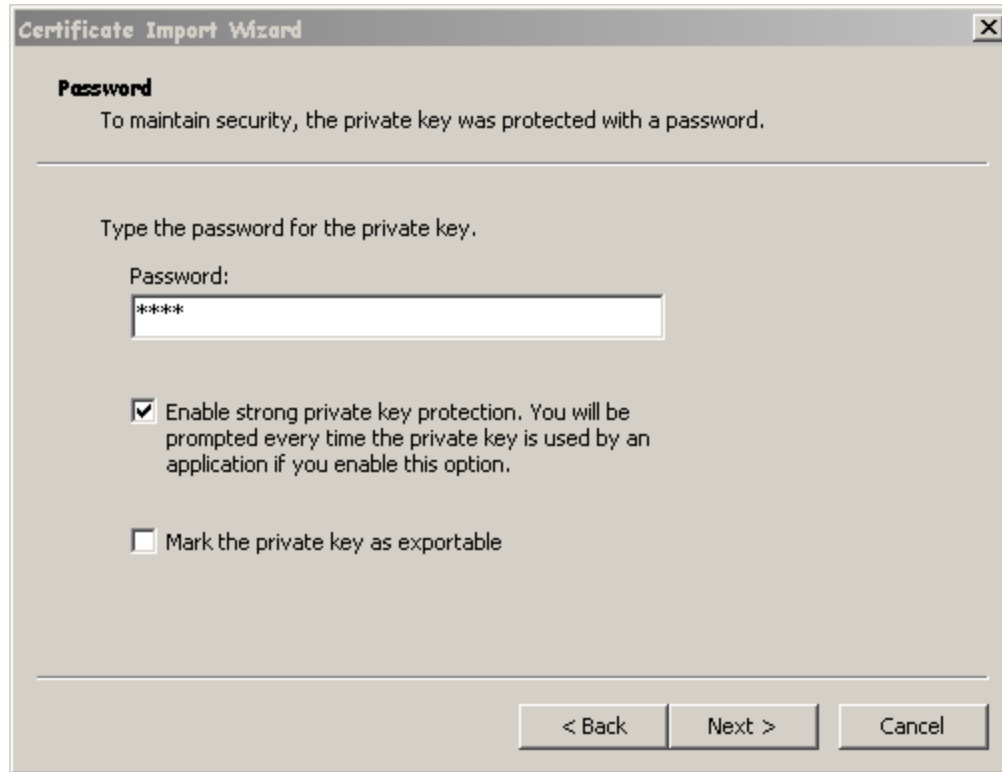
NOTE: Your Browser will present only those certificates that you have imported.



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



8. **Insert the diskette** on which you saved the 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 to highlight the file.
13. Click on the **Open** button.
14. Click on the [**N**ext >] button.

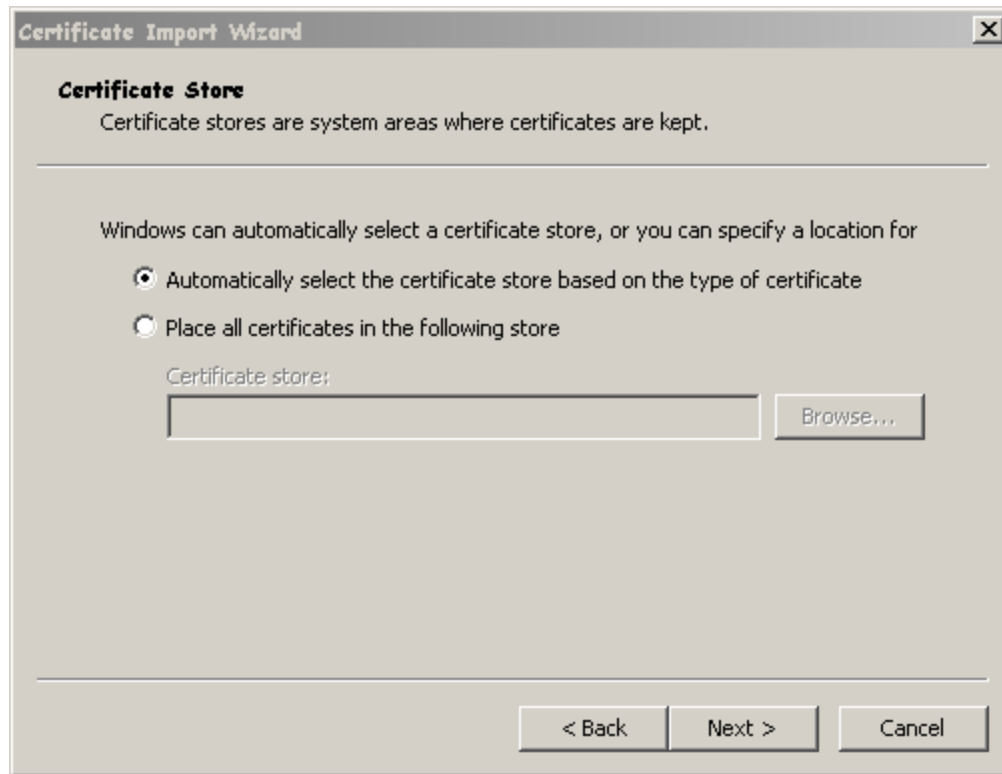


15. **Type in the certificate password** that was provided to you by the MOHP\S HelpDesk.
16. Click in the box beside **Enable strong private key protection**, to select that option.

IMPORTANT NOTE:

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

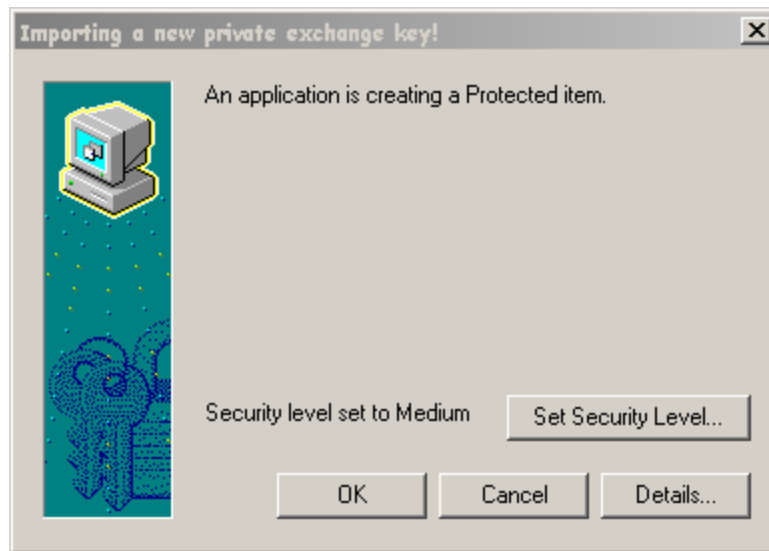
17. Click on the [**N**ext >] button.



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.

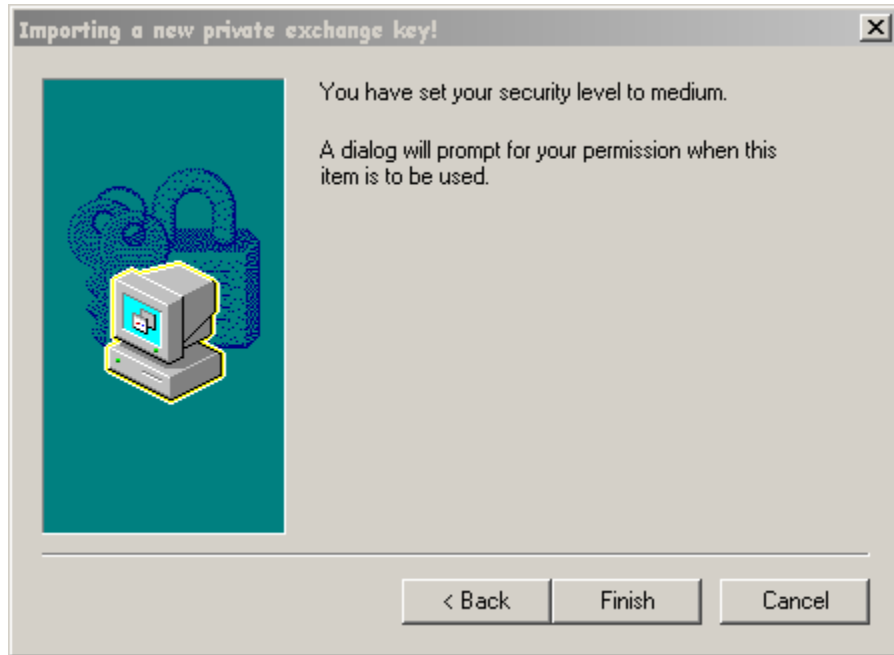


20. Click on the [**S**et **S**ecurity **L**evel...] button.

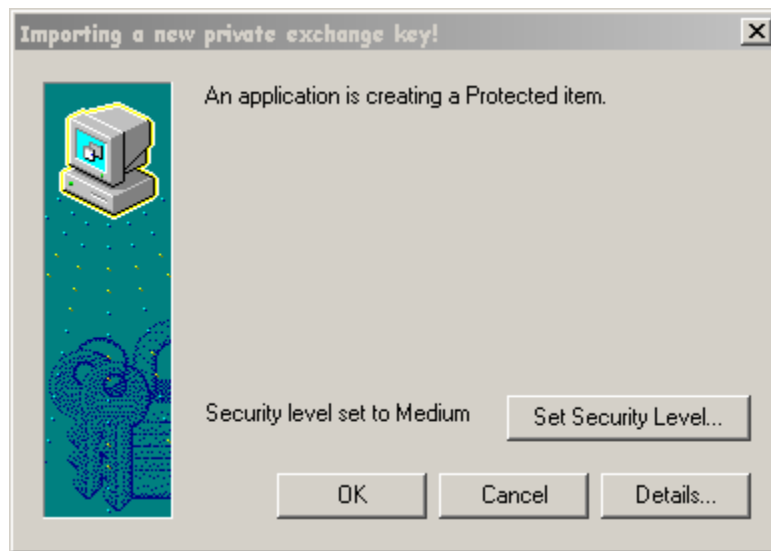


21. Click in the circle beside **M**edium, to select that security level option.

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



23. Click on the [**F**inish] button.

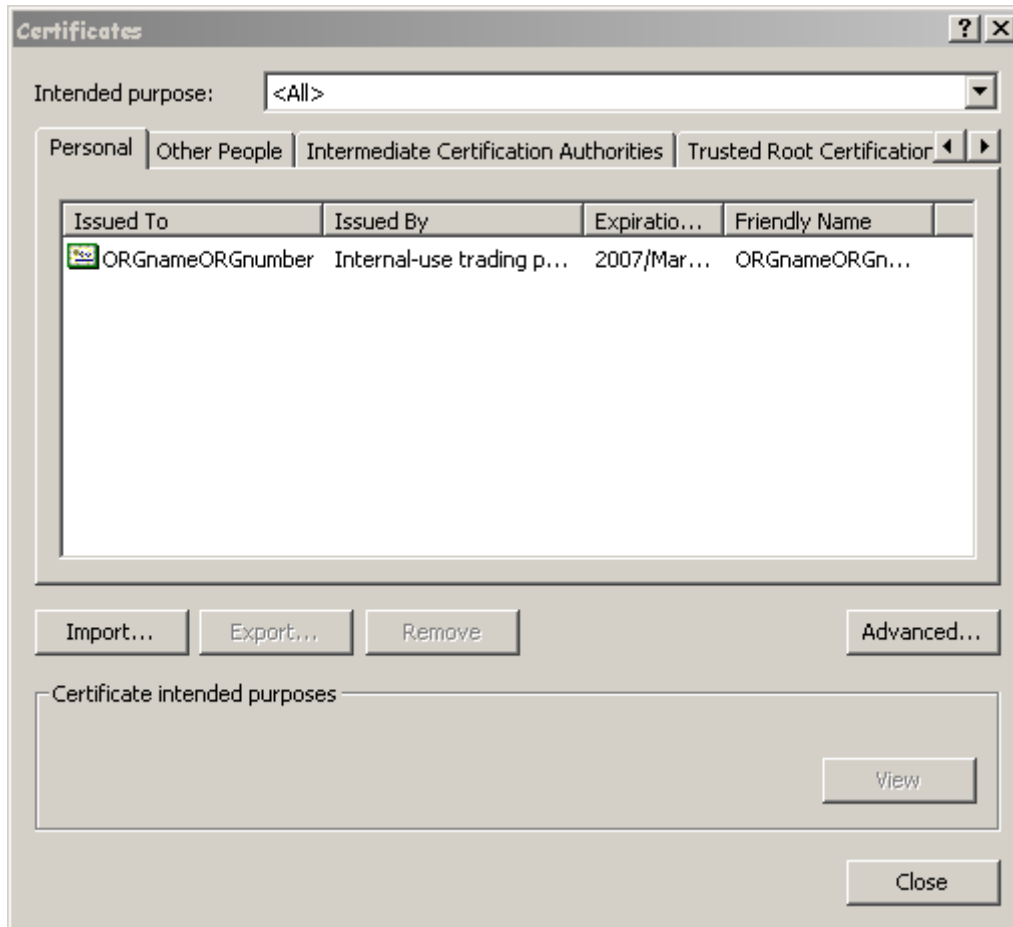


The security level has now been set, and displays on the screen to the left of [**S**et Security Level] button

24. Click on the [**O**K] button.

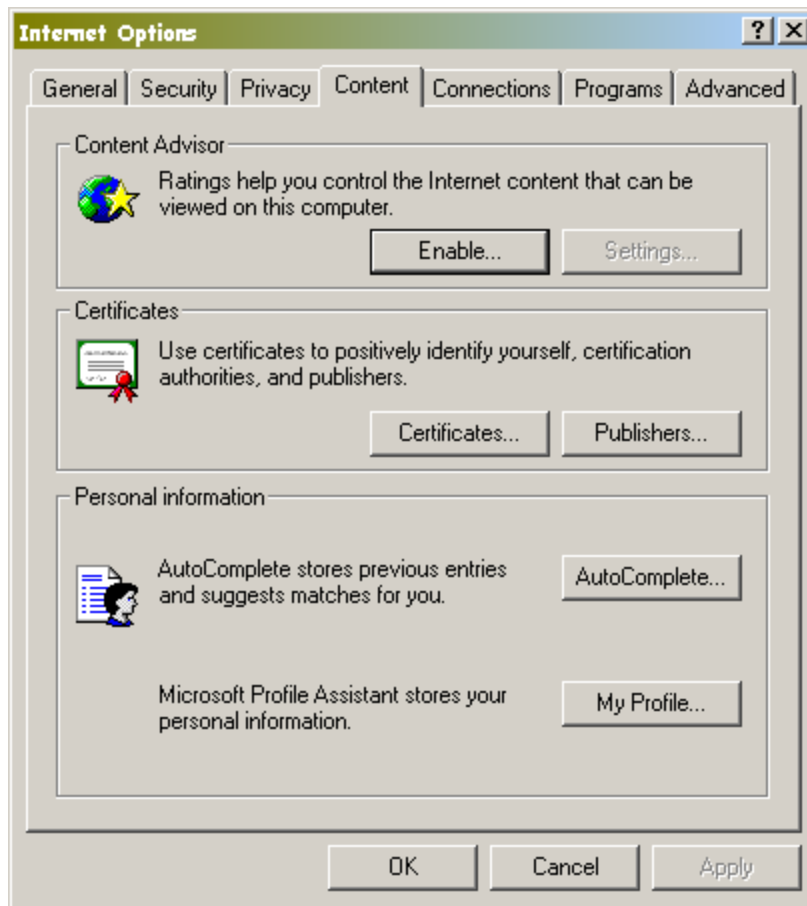


25. Click on the [OK] button.



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.

5. 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.

6. Confidentiality Undertaking Document

All users within **private sector organizations** must sign a confidentiality document prior to accessing the MOHP\S web business services.

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.

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 Services.

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



Ministry of Health Services

CONFIDENTIALITY UNDERTAKING
for private sector users who will be accessing
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 SERVICES PERMITTING ACCESS TO SPECIFIC CLIENT DATA ON CERTAIN MINISTRY 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 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.