www.ehealthontario.on.ca

eHealth Ontario

PKI Certificate Installation Guide

Instructions for Windows Platforms

Version: 2.1

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Revision History

Date	Version	Revision
March 2007	2.1	Minor reworking for external audiences
March 2007	2.0	Updated for next version of certificate utility
November 2006	1.0	Added Application Owner and baselined document
August 2006	0.04	Revised by Ron McEwen, Marianne White, Tiffany Yim; added SSHA CA Root certificate installation instructions and other minor reworking
July 2006	0.03	Revised - Ron McEwen, Tiffany Yim
June 2006	0.02	Revised draft – add EESW
May 2006	0.01	Initial Draft

Table of Contents

List of Figures

N/A

List of Tables

N/A

1.0 Introduction

This document describes the use of the **sshacertreq.hta** executable to:

- Generate a PKCS #10 certificate signing request
- Install the created certificate

1.1 Glossary

CA	Certification Authority
CSR	Certificate Signing Request
MMC	Microsoft Management Console
PKI	Public Key Infrastructure

1.2 Intended Audience

This document is intended for technical personnel at eHealth Ontario client organizations who are involved in registering computer applications with eHealth Ontario. This includes:

- Application Owners
- Their delegates

1.3 Applicability

sshacertreq only works on a Windows platform.

2.0 Creating and Installing Certificates

2.1 Overview

The process of creating and installing certificates is as follows:

1. **Register the application for which you require a certificate with eHealth Ontario**, if this hasn't already been done.
2. **Obtain a PKI Reference Number from eHealth Ontario**. This number will be required to create and submit your request to eHealth Ontario.
3. **Create the Certificate Signing Request (CSR)** using **sshacertreq.hta** (which has been sent to you via e-mail)**.**
   - The CSR is created on the machine where the certificate is to be used.
   - The process of creating a CSR generates a matching public and private RSA key pair.
   - The private key is stored on the machine and the public key is placed in the CSR.
4. **Send the CSR (with Reference Number)** to the eHealth Ontario Deployment Team.
5. **Install the PKI Certificate created from your CSR, on the same machine where the CSR was created**, using **sshacertreq.hta**. Now a matching certificate and private key exist on the machine and the certificate can be used for digital signing, encryption, etc.
6. **Install the eHealth Ontario Certification Authority root certificate.**

This guide assumes that the computer application has already been registered and the Reference Number has been provided to you.

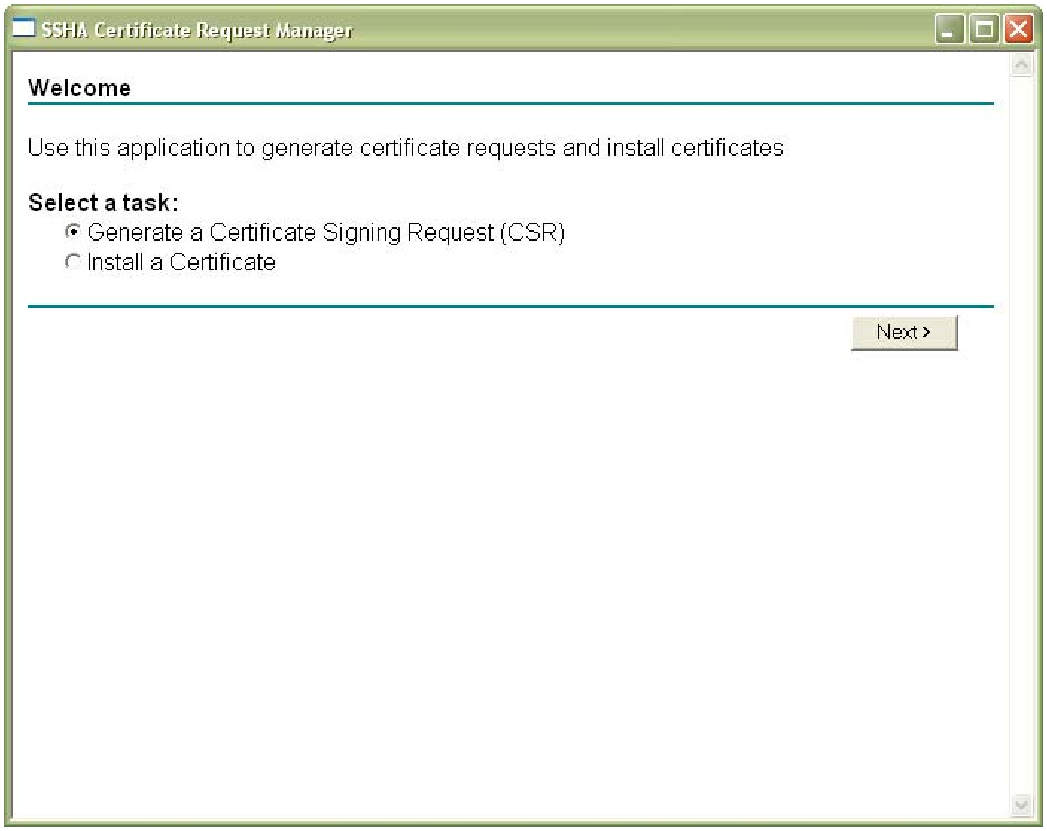
2.2 Create CSR(s)

Note: If certificates and keys are to be stored in the Windows machine store, administrative privileges will be required when running **sshacertreq.hta** and the MMC certificate snap-in.

For each request to be generated you require the corresponding Reference Number (example: 8934282) for the identity of registered computer application. The Reference Number is obtained from the eHealth Ontario Deployment Team. A unique Reference Number is required for each certificate that is to be created.

To create a CSR:

1. Run **sshacertreq.hta**. The following screen is displayed:



Welcome

Use this application to generate certificate requests and install certificates

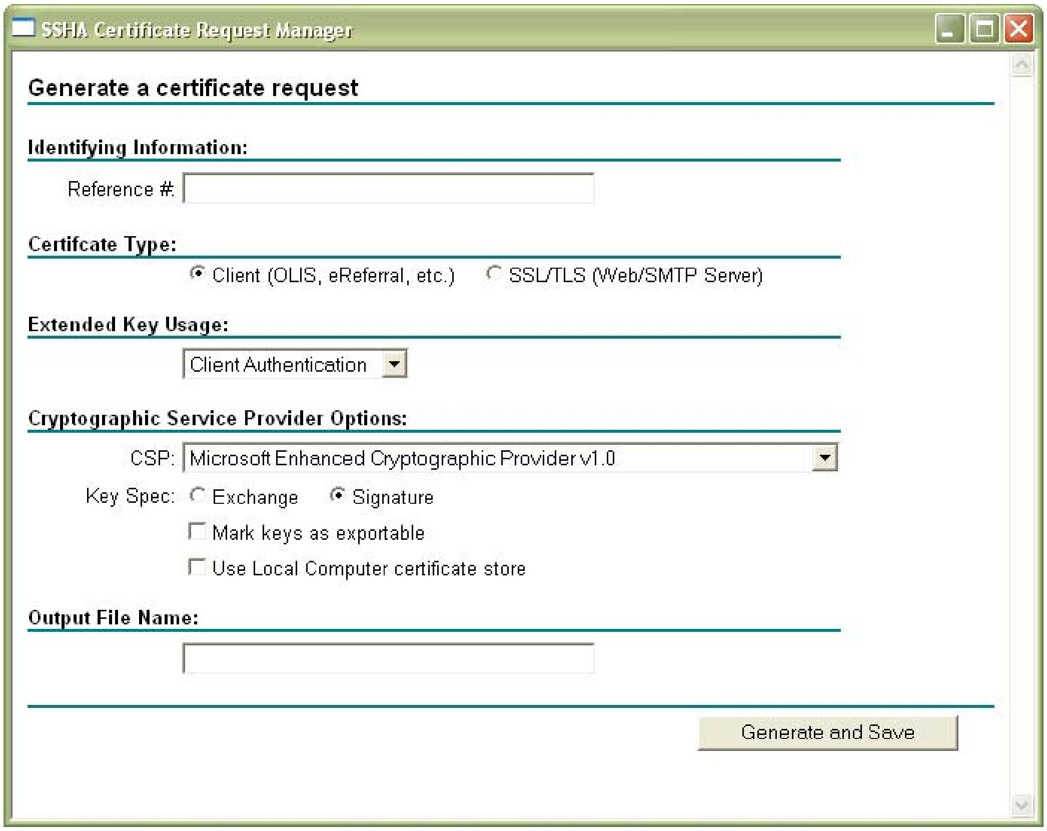
Select a task:

● Generate a Certificate Signing Request (CSR)

○ Install a Certificate

2. Choose to **Generate a Certificate Signing Request (CSR)**.

3. Click **Next**. The following screen is displayed:



SSHA Certificate Request Manager

Generate a certificate request

Identifying Information:

Reference #:

Certifcate Type:

● Client (OLIS, eReferral, etc.) ○ SSL/TLS (Web/SMTP Server)

Extended Key Usage:

Client Authentication

Cryptographic Service Provider Options:

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Spec: ○ Exchange ● Signature

□ Mark keys as exportable

□ Use Local Computer certificate store

Output File Name:

Generate and Save

4. Fill out the form fields as follows (see completed form image below):

   - **Reference #:** Enter the Reference Number given to you for this identity.

   - **Certificate Type:** If the certificate will be used to communicate with OLIS and/or eReferral, choose Client. If the certificate is for a SMTP server or web server, choose SSL/TLS.

   - **Extended Key Usage:** If the certificate will be checked against a trusted certificate list by the server (e.g., OLIS, eReferral), choose **Client Authentication**. If the certificate will be provided to a client to verify the certificate holder during the establishment of a secure session (e.g., ONE Mail), choose **Server Authentication**.

   - **CSP**: Ensure that *Microsoft Enhanced Cryptographic Provider v1.0* is selected.

   - **Key Spec**: If the certificate will be used to encrypt a symmetric key to establish an encrypted session, choose **Exchange**. If the certificate will be used to sign a message, choose **Signature**.

   - **Mark Keys as Exportable:** Check **Mark Keys as Exportable** if you require the portability of the keys/certificates.

     It is safer and preferable to **not** allow key export. This gives a higher assurance that the identity (certificate and private key) is only available on the machine on which the certificate request was generated on, thereby minimizing the risk of compromise or misuse. **Certificates for Production**

systems should not be exportable.

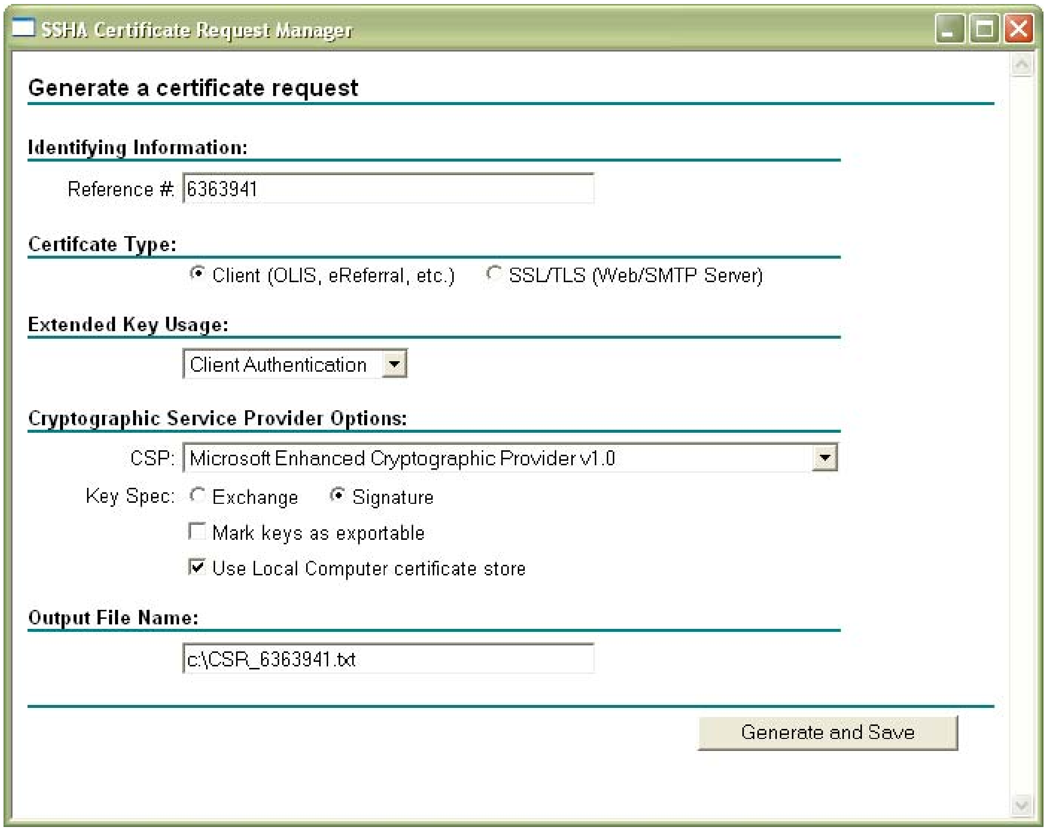
There may be situations where key export might be desirable for pre-Production or testing purposes; e.g., testing the secure connection with eHealth Ontario using non-PHI data on several developers' machines may warrant the use of a common certificate and exportable keys, or some situations may warrant the need to back-up the certificate. Proper safeguards, however, must be in place to prevent to unauthorized disclosure or misuse of keys when the keys and certificate are marked exportable.

- **Use Local Computer Certificate Store**: Windows Services (typically, long running programs that run under an identity other than the logged on user) can only access certificates in the local computer certificate store (as opposed to the User certificate store). If the certificate is to be stored in the local computer certificate store, check this box.

- **Output File Name**: Enter a file name in which to store the request. A name is automatically generated when the focus leaves the Reference # textbox. **Example:** c:\CSR_6363941.txt (default name generated).

  The output file name may be changed if desired.

  A sample of a completed screen is shown below:



Generate a certificate request

Identifying Information:

Reference #: 6363941

Certifcate Type:

● Client (OLIS, eReferral, etc.) ○ SSL/TLS (Web/SMTP Server)

Extended Key Usage:

Client Authentication

Cryptographic Service Provider Options:

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Spec: ○ Exchange ● Signature

□ Mark keys as exportable

☑ Use Local Computer certificate store

Output File Name:

c:\CSR_6363941.txt

5. Click **Generate and Save**.

Complete the above procedure for each certificate you need to create, entering a new **Reference Number and Output File Name** for each request. The result each time is a CSR file.

2.3 Send the CSR/Receive the Certificates

Forward the CSR via email to the eHealth Ontario Deployment Team. eHealth Ontario will return

- A PKI certificate created from the CSR
- The eHealth Ontario Certification Authority Root certificate

The contents of the certificate files will resemble the following:

```
-----BEGIN CERTIFICATE-----
MIIGYAYJKoZIhvcNAQcCoIIGUTCCBk0CAQExADALBgkqhkiG9w0BBwGgggY1MIIG
MTCCBRmgAwIBAgIEQA9uVDANBgkqhkiG9w0BAQUFADCBpjETMBEGCgmSJomT8ixk
ARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC1N1YnNjcmliZXJzMRUwEwYDVQQLEwxT
U0ggU2VydmljZXMxETAPBgNVBAsTCFNlY3VyaXR5MQwwCgYDVQQLEwNQS0kxOjA4
BgNVBAMTMVNtYXJ0IFN5c3RlbXMgZm9yIEhlYWx0aCBBZ2VuY3kgUm9vdCBDQSAt
IFRlc3RpbmcwHhcNMDYwMjE3MDEwNDQxWhcNMDkwMjE3MDEzNDQxWjCBkzETMBEG
CgmSJomT8ixkARkWA3NzaDEbMBkGCgmSJomT8ixkARkWC3N1YnNjcmliZXJzMRQw
EgYDVQQLEwtTdWJzY3JpYmVyczESMBAGA1UECxMJSG9zcGl0YWxzMQ8wDQYDVQQL
EwZPTFNUU1QxFTATBgNVBAsTDEFwcGxpY2F0aW9uczENMAsGA1UEAxMESElTNjCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwmVaRaRrPLO+ZY44H2ZIX1s6jpA3
H24UDEOKYfaZ1gZesltzYDphXOMp/7ZnP350TnbiZQqpNFLqqckFOWskJSC83PEU
xMa5jJU1xTfdpGWtnYrvT+mi0q3x+KGQ4y7DDtD4KSAWXkkIKndiYH9mvPBQ+q4X
aqHqmFN/DZw/kTECAwEAAaOCAvowggL2MAsGA1UdDwQEAwIHgDArBgNVHRAEJDAi
gA8yMDA2MDIxNzAxMDQ0MVqBDzIwMDgwMzI1MDUzNDQxWjCBxQYIKwYBBQUHAQEE
gbgwgbUwgbIGCCsGAQUFBzAChoGlbGRhcDovL3NzaHBraTJhMDAwMXUuc3Vic2Ny
aWJlcnMuc3NoL2NuPVNtYXJ0IFN5c3RlbXMgZm9yIEhlYWx0aCBBZ2VuY3kgUm9v
dCBDQSAtIFRlc3RpbmcsIG91PVBLSSwgb3U9U2VjdXJpdHksIG91PVNTSCBTZXJ2
aWNlcywgZGM9U3Vic2NyaWJlcnMsIGRjPXNzaD9jQUNlcnRpZmljYXRlMIIBigYD
VR0fBIIBgTCCAX0wgcGggb6ggbukgbgwgbUxEzARBgoJkiaJk/IsZAEZFgNzc2gx
GzAZBgoJkiaJk/IsZAEZFgtTdWJzY3JpYmVyczEVMBMGA1UECxMMU1NIIFNlcnZp
Y2VzMREwDwYDVQQLEwhTZWN1cml0eTEMMAoGA1UECxMDUEtJMTowOAYDVQQDEzFT
bWFydCBTeXN0ZW1zIGZvciBIZWFsdGggQWdlbmN5IFJvb3QgQ0EgLSBUZXN0aW5n
MQ0wCwYDVQQDEwRDUkwyMIG2oIGzoIGwhoGtbGRhcDovL2NybHUuc3NoYS5jYS9j
bj1TbWFydCUyMFN5c3RlbXMlMjBmb3IlMjBIZWFsdGglMjBBZ2VuY3klMjBSb290
JTIwQ0ElMjAtJTIwVGVzdGluZyxvdT1QS0ksb3U9U2VjdXJpdHksb3U9U1NIJTIw
U2VydmljZXMsZGM9U3Vic2NyaWJlcnMsZGM9c3NoP2NlcnRpZmljYXRlUmV2b2Nh
dGlvbkxpc3QwHwYDVR0jBBgwFoAUoDjQCKRd/Fk7eTuqfcpZKT5GWRowHQYDVR0O
BBYEFDtLS1NyMiADLtzKP/vfrPTThIQVMAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EA
BAwwChsEVjcuMQMCBLAwDQYJKoZIhvcNAQEFBQADggEBAB45Jjvk7NeokO2/iy+H
X142NV7wRR1lBmcJKLxYE3YgrGw7C7kBRjBEZbjoQy8g1Mniop8m1kA6tiJreuF2
kAxElilGu1DK5IqrA+lW7S3b7G5XipgC7jF8iQ9zUhblTsfLfLKZ0r/exPX3LE/P
RYeqIUbATXfc/tuwcPm4kjRigpNIs+uEJAgkoOr73A1U2SLlGf1Q+EhSyTQ2qRI/
lIDTnEACHXbgEhU4qG8p+cN2GDcN8HJUqVLGlH6GOzfpl+6rZVeHfapUqf+hWmtX
LCjcOCVZeaS6GpzIlbBlhRLae6glPUNQUqfX0P8dxCitvY20w0mePuikS1dFsAMz
MGYxAA==
-----END CERTIFICATE-----
```

Note: The certificate contents include the lines that say "BEGIN CERTIFICATE" and "END CERTIFICATE".

2.4 Save the eHealth Ontario CA Root Certificate

Save the eHealth Ontario CA Root certificate to your local hard drive (it will be installed in Section 2.6).

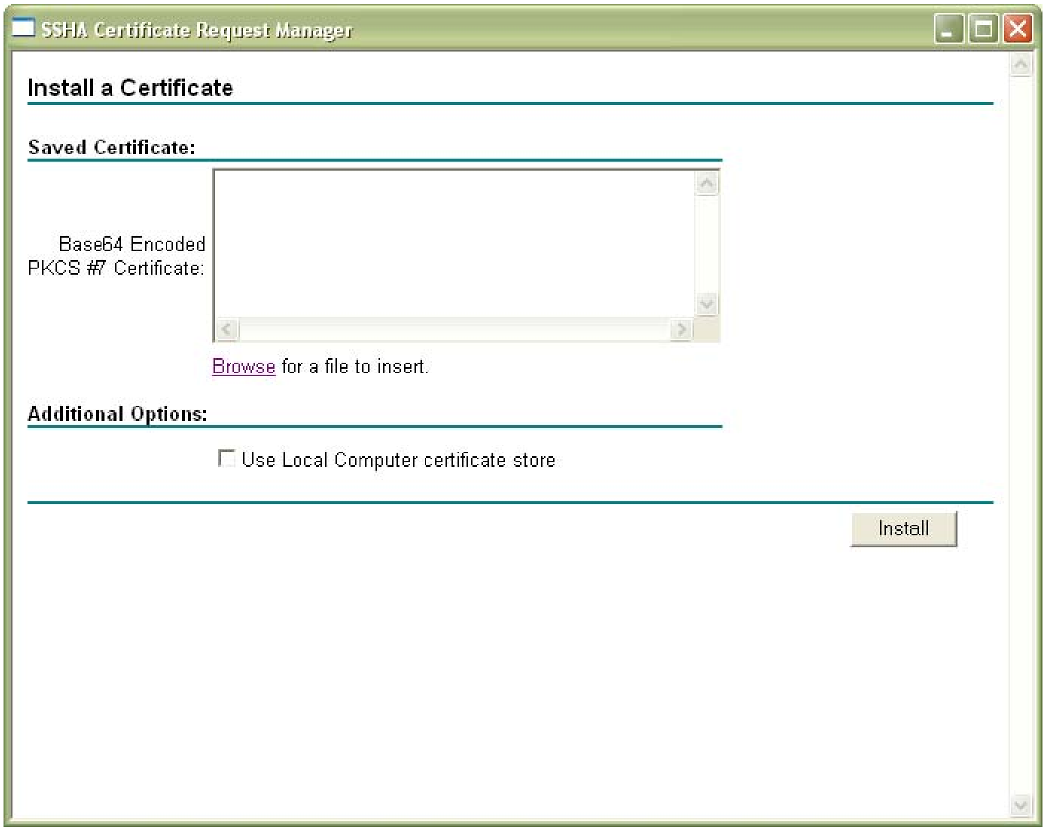
2.5 Install the PKI Certificate Created from Your CSR

1. Copy the contents of the PKI certificate generated from the CSR. Using the mouse, select the entire contents of the certificate (including "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"), right-click the mouse, and click **Copy**.

2. Install the certificate generated from the CSR as follows:

   a. On the same machine on which the CSR was created, run **sshacertreq.hta**, and this time select **Install a Certificate**.

      The following screen is displayed:


SSHA Certificate Request Manager
Install a Certificate
Saved Certificate:
Base64 Encoded PKCS #7 Certificate:
Browse for a file to insert.
Additional Options:
□ Use Local Computer certificate store
Install

   b. Paste the certificate contents (which you copied in Step 1) into the **Base64 Encoded PKCS #7 Certificate** text box. Ensure this is the certificate generated from the CSR.

      If the local machine store checkbox was selected when creating the CSR (see section 2.1, step 4), check the **Use Local Computer certificate store** checkbox; otherwise, do not.

   c. Click **Install**.

2.6 Add the Certificate Snap-In to the Microsoft Management Console (MMC)

If the Certificate Snap-in is already installed on your machine, proceed to section 2.6; if not, follow these steps to add the Certificate Snap-in to MMC:

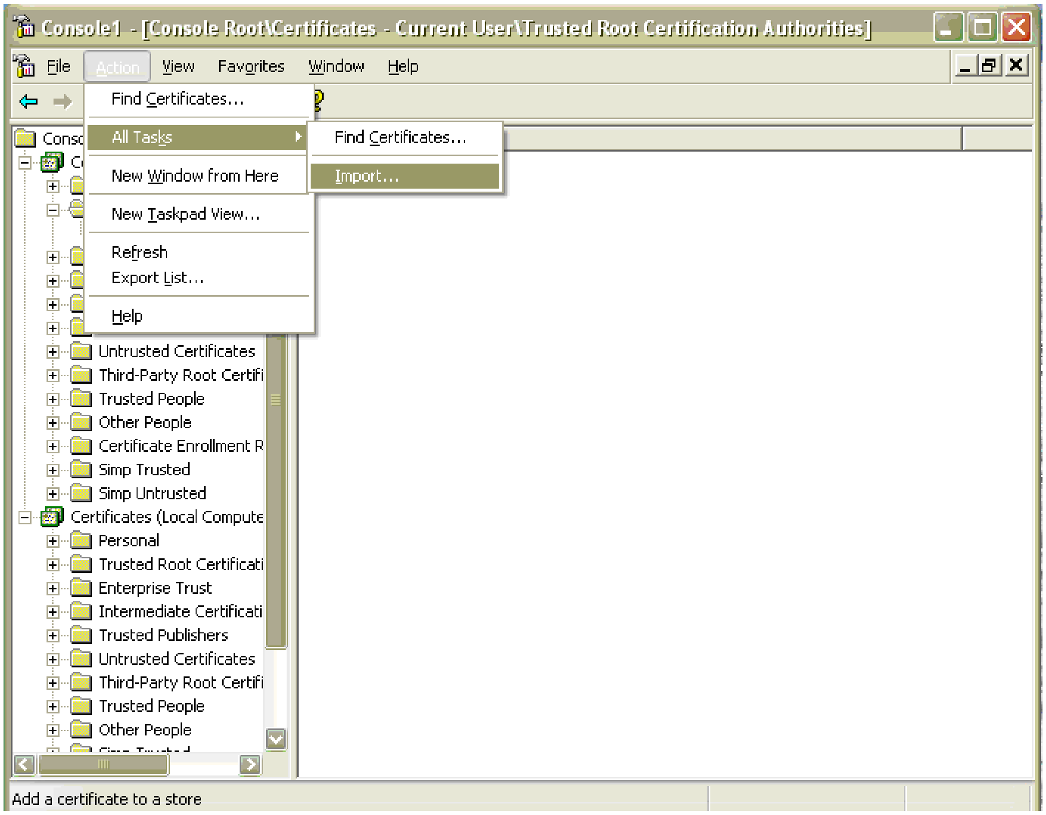
1. From the **Start** menu, select **Run**.
2. In the **Run** dialog box, type **mmc** and click **OK**. The Microsoft Management Console is displayed.
3. From the File menu, select **Add/Remove Snap-in**.
4. On the Standalone tab, click **Add**.
5. From the **Available Standalone Snap-ins** list box, select **Certificates**, and then click **Add**.
6. If you did not select the 'Use Local Computer certificate store' option when generating the CSR (see section 2.1, step 4), select **My User Account** and click **Finish**.

   Otherwise, click **Computer Account**, click **Next**, choose **Local Computer**, and then click **Finish**.
7. Click **Close**.
8. Click **OK** and proceed to step 2 in the next section.

2.7 Install the eHealth Ontario CA Root Certificate

Use the MMC Certificate Snap-in to install the eHealth Ontario CA Root Certificate:

1. In MMC, open the **Certificates** snap-in.
2. In the console tree, select the logical store where you installed the certificate.
   - If you did not select the **'Use Local Computer certificate store'** option when creating the CSR, this will be the **Certificates - Current User** store.
   - If you selected the **'Use Local Computer certificate store'** option when creating the CSR, this will be the **Certificates (Local Computer)** store.
3. In the expanded console tree under the appropriate certificate store, select **Trusted Root Certification Authorities** to ensure that the certificate is installed in the correct store.
4. From the Action menu, select **All Tasks**, and then **Import…**



Add a certificate to a store

5. The Certificate Import Wizard is displayed. Click **Next**.

6. Click **Browse...** to locate and select the eHealth Ontario CA Root certificate. Click **Next** once the eHealth Ontario CA Root certificate has been selected.

7. Select the option to **Place all certificates in the following store**. The Certificate Store displayed should be **Trusted Root Certification Authorities**, but you may need to select the Trusted Root Certification Authorities store using Browse... Click **Next** once the **Trusted Root Certification Authorities store** is specified.

8. Click **Finish**.

9. You should now see the eHealth Ontario CA Root certificate that was imported under the Trusted Root Certification Authorities Certificate folder.

2.8 Verify the Certificate Install

To verify the certificate installation:

1. In MMC, open the **Certificates** snap-in.

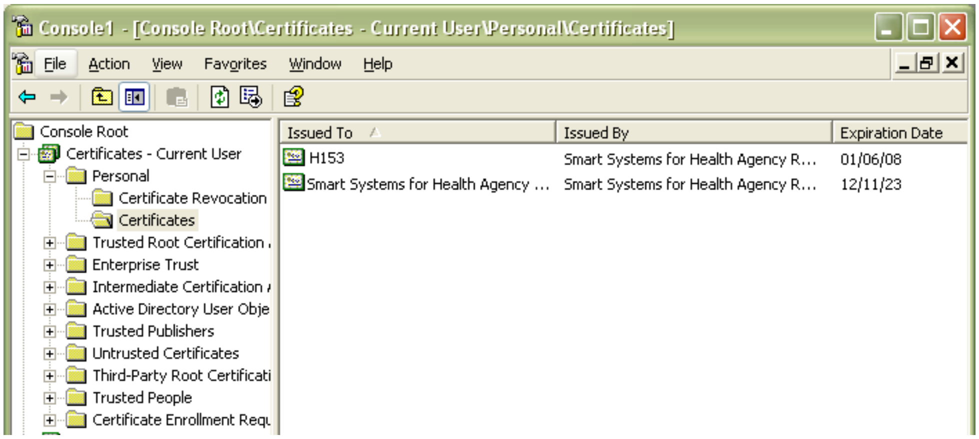
2. In the console tree, select the logical store where you installed the certificate.

   - If you did not select the **'Use Local Computer certificate store'** option when creating the CSR, this will be the **Certificates - Current User** store.

- If you selected the **'Use Local Computer certificate store'** option when creating the CSR, this will be the **Certificates (Local Computer)** store.

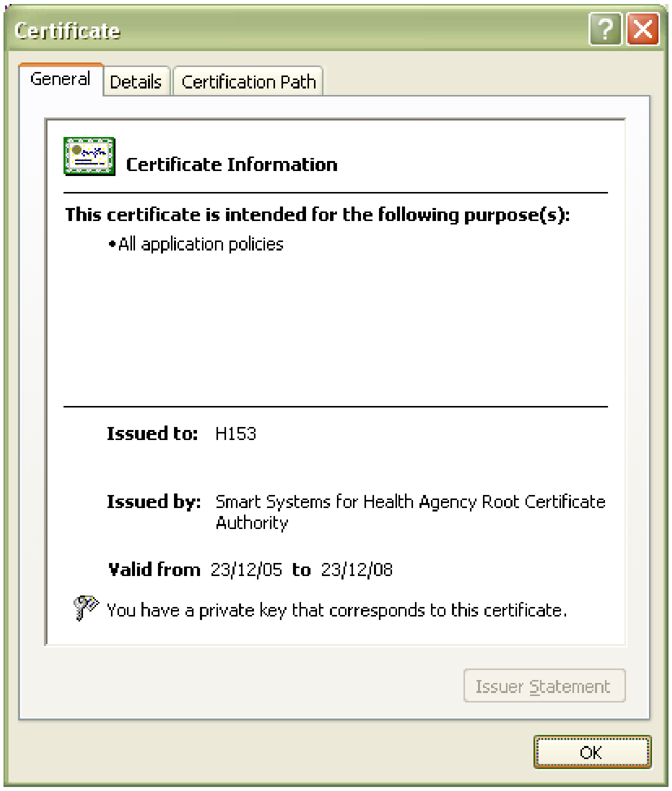
3. Open the **Personal** folder, and then open the **Certificates** folder.

   You should see the certificate that you imported using the **sshacertreq** utility.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificate Revocation
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Certificate Enrollment Requ

Issued To	Issued By	Expiration Date
H153	Smart Systems for Health Agency R...	01/06/08
Smart Systems for Health Agency ...	Smart Systems for Health Agency R...	12/11/23

4. Double-click the certificate generated from the CSR. The following dialog appears:



Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: H153

Issued by: Smart Systems for Health Agency Root Certificate Authority

Valid from 23/12/05 to 23/12/08

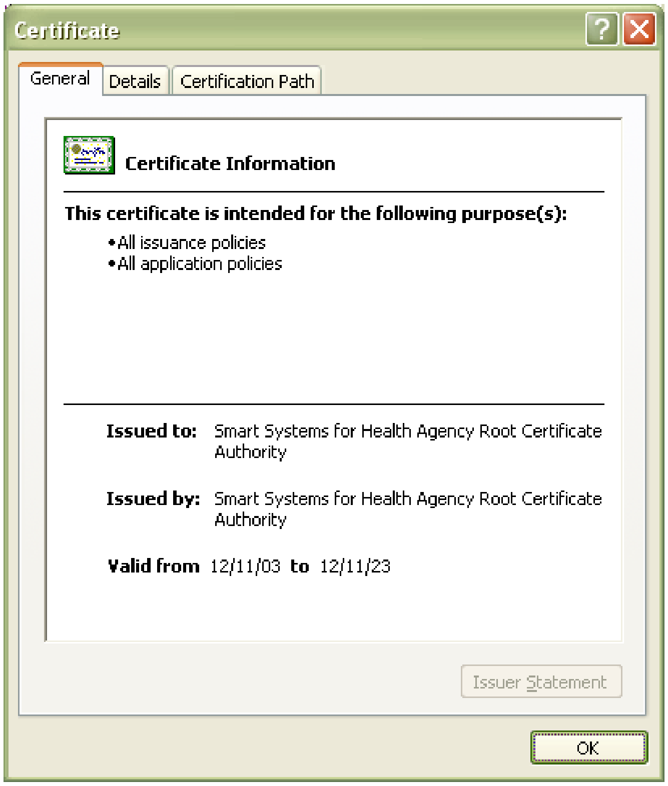
You have a private key that corresponds to this certificate.

Ensure that the message "**You have a private key that corresponds to this certificate**" is displayed.

5. In the same certificate store, open the **Trusted Root Certification Authority** folder, and then open the **Certificates** folder.

You should see the eHealth Ontario CA Root certificate that you imported using MMC.

6. Double-click the **eHealth Ontario CA Root certificate**. The following dialog appears:



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Smart Systems for Health Agency Root Certificate Authority

Issued by: Smart Systems for Health Agency Root Certificate Authority

Valid from 12/11/03 to 12/11/23

7. You have successfully installed the certificates.