Certificate Creation Tool

Version: .02

Document ID:

###### Copyright Notice

Copyright © 2015, eHealth Ontario

###### All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

###### Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

###### Document Control

The electronic version of this document is recognized as the only valid version.

###### Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| REVIEWERS | TITLE/DEPARTMENT | REVIEWED DATE |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

###### Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION NO. | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 0.1 | 2015-8-11 | Initial Draft | David Campbell |
| 0.2 | 2017-06-02 | Updated | Viorica Deretey |
|  |  |  |  |
|  |  |  |  |

###### Document ID

###### Document Sensitivity Level

Medium

Table of Contents

[1.0 About This Document 1](#_Toc484183351)

[1.1 Audience 1](#_Toc484183352)

[2.0 Certificates at eHealth Ontario 2](#_Toc484183353)

[2.1 Certificate Workflow 2](#_Toc484183354)

[2.2 Certificate Creation Tool 2](#_Toc484183355)

[2.2.1 eHealth Ontario – Create CSR 2](#_Toc484183356)

[2.2.2 eHealth Ontario – Combine Certificate and Key 3](#_Toc484183357)

[3.0 Appendix A: Glossary 6](#_Toc484183358)

# About This Document

This document provides instruction on the use of an eHealth Ontario tool to aid in the creation of PKI certificates.

## Audience

This document is intended for eHealth Ontario clients who require a certificate for use in the consumption of eHealth services protected by eHealth Ontario.

# Certificates at eHealth Ontario

PKI client certificates are leveraged as an authentication mechanism for several eHealth services that are system to system. The client requiring a certificate generates the Certificate Signing Request (CSR) on the server that will be used to consume eHealth services. CSR creation varies amongst server & application architecture, and a general Windows solution was created to aid in the process.

## Certificate Workflow

1. Client requests access to eHealth protected service that requires a PKI client certificate
2. eHealth ONE ID provisions certificate identity metadata to eHealth Certificate Authority
3. eHealth Ontario provides certificate Reference Number to client
4. Client generates CSR on system accessing eHealth protected service. Creation of CSR outputs both the CSR and a Private Key file
5. Client sends CSR to contact at eHealth
6. eHealth provides a certificate signed by eHealth to client
7. Client imports the certificate and the private key into the application consuming eHealth protected services

## Certificate Creation Tool

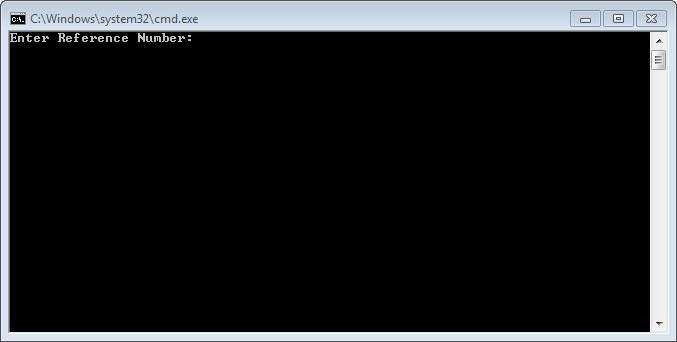
The enclosed certificate tool is intended to assist with Step 4 and Step 7 of the Certificate Workflow detailed above.

### eHealth Ontario – Create CSR

This batch file leverages the OpenSSL toolset and libraries to create a CSR and a Private Key associated with the Reference Number provided to you by eHealth Ontario.

**Usage**

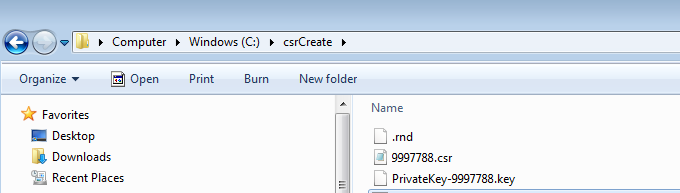
1. Double-click on eHealthOntario–CreateCSR.cmd or run it from the command prompt (cmd).



1. Enter the Reference Number provided by your eHealth Ontario contact and press Enter
2. In the folder containing the tool, two new files are created:

* *refNumber.csr*
* *PrivateKey-refNumber.key*

It is important to make a note of the location of where the *PrivateKey-refNumber.key* file was created. This key file will be needed to combine with the certificate issued back to your site later.

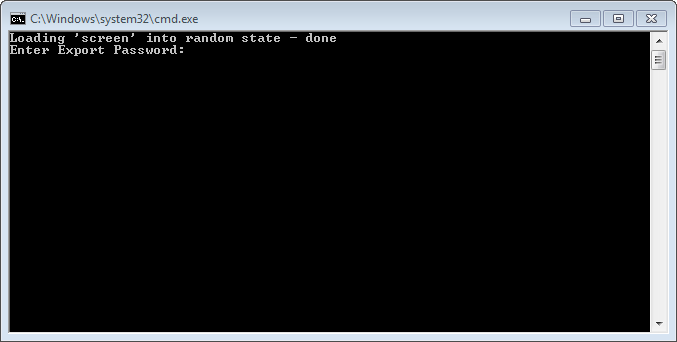


1. Email *refNumber*.csr file to your eHealth contact

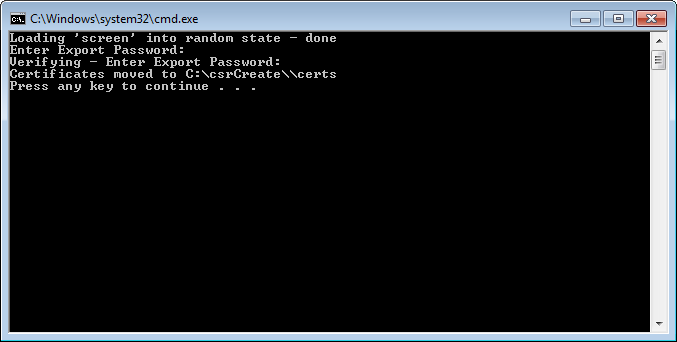
### eHealth Ontario – Combine Certificate and Key

This batch file leverages the OpenSSL toolset and libraries to combine the separate certificate and private key files (PKCS7 format) to a .pfx file (PKCS12 format) more suitable for importing into the Windows Certificate Store.

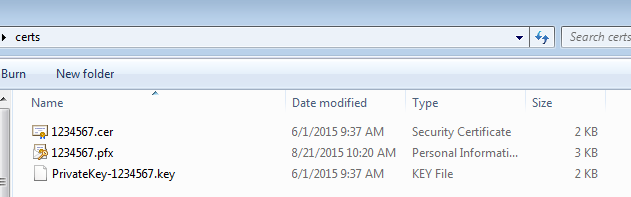
1. When you receive the certificate from eHealth, change its extension from .txt to .cer. Copy it to the folder containing the tool. This is where the private key was created during the CSR generation process.
2. Make sure the folder contains the private key generated in previous step (paragraph 2.2.1). The folder should contain only one file with extension .key (the private key) and one file with extension .cer (the certificate corresponding to the private key).
3. Double-click on eHealthOntario–CombineCertificateAndKey.cmd or run it from a command prompt (cmd)
4. Enter a password. It will be used later when importing the combined certificate



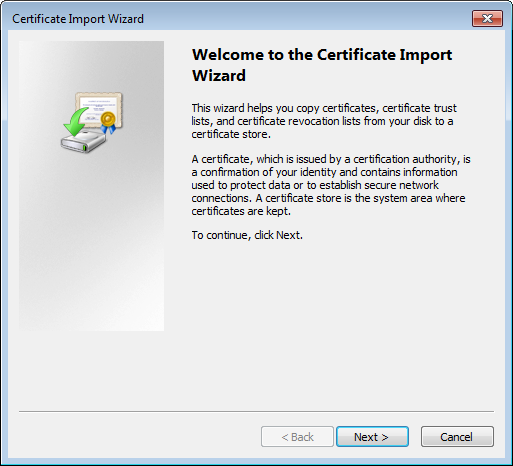
1. Verify the password
2. Note the location where certificates are saved



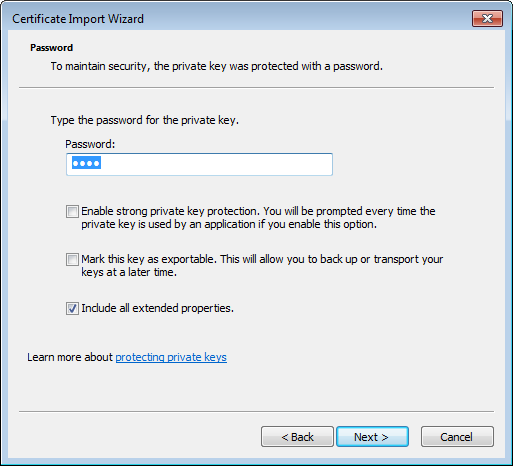
1. Verify the files exist in the folder noted in previous step, and ensure all files have a size greater than zero bytes. If the *.pfx* file has size zero, it means there is a problem with the certificates. Make sure the private key file match the certificate received from eHealth Ontario. They should both be generated from the same reference number.



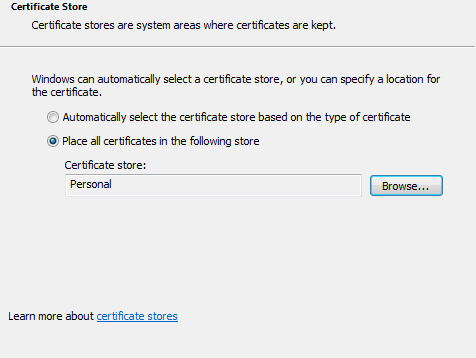
1. Double-click on the combined certificate (extension .pfx) to start the Certificate Import Wizard



1. Click Next
2. Click Next
3. Enter password specified in Step 4



1. Click Next
2. Select Place all certificates in the following store
3. Click Browse
4. Choose the appropriate store required by application



1. Click Next
2. Click Finish

# Appendix A: Glossary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Term** | | | **Definition** | |
|  |  | |
| Certificate Authority | Issuing authority for a certificate. Noted in a certificate by the Issuer attribute | |
| CSR | Certificate Signing Request is a file generated by the certificate client, and is sent to the Certificate Authority | |
| Root Certificate | Public portion of certificate authorities signing certificate | |
| PKCS7 | Certificate format often used in Apache / Tomcat application servers. Often notable in separation of certificate and private key files | |
| PKCS12 | Certificate format often used in Windows applications and servers. Often notable in .pfx extension | |
| Enrolment | Data held in ONE ID that identifies which service a user or system is authorised to access (e.g. OLIS etc.). This may also include the role the user or system is approved for, e.g. end user, administrator etc. | |
| ONE ID | Identity and Access Management System | |
|  |  | |