Generating the Certificate Signing Request (CSR)

### Version: 1.5

### Document ID: ConnectingOntarioGenerating CSR file

### Document Owner: ConnectingOntario

#### Copyright Notice

Copyright © 2016, 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 |
|  |  | YYYY-MM-DD |
|  |  | YYYY-MM-DD |

#### Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION NO. | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2016-10-26 | Initial release | ConnectingOntario Program |
| 1.1 | 2016-11-14 | Page 3 - Added instructions to rename the L7\_key folder when the scripts are run multiple times per environment to prevent previous files from being overwritten. | ConnectingOntario Program |
| 1.2 | 2016-12-11 | Page 2 – Added process diagram | ConnectingOntario Program |
| 1.3 | 2017-05-31 | Updates to align with new scripts (V6) | ConnectingOntario Program |
| 1.4 | 2017-12-15 | Updates to align with new scripts (V9) | ConnectingOntario Program |
| 1.5 | 2018-05-1 | Updates to align with new scripts (V9) | ConnectingOntario Program |

## Document ID

ConnectingOntarioCSR generation instructions

Table of Contents

[Version: 1.5 1](#_Toc512945615)

[Document ID: ConnectingOntarioGenerating CSR file 1](#_Toc512945616)

[Document Owner: ConnectingOntario 1](#_Toc512945617)

[Document Control ii](#_Toc512945618)

[Document ID ii](#_Toc512945619)

[Overview 1](#_Toc512945620)

[Description 2](#_Toc512945621)

[Prerequisites 2](#_Toc512945622)

[Certificate Request & Installation Process 3](#_Toc512945623)

[Instructions 3](#_Toc512945624)

[Configuring the settings.cmd file 3](#_Toc512945625)

[Using the generateCSR.cmd file 5](#_Toc512945626)

[Next steps: 7](#_Toc512945627)

[Appendix A: Changing the Password (i.e. Storepass) associated to the Private Key 8](#_Toc512945628)

# Overview

Connection to ConnectingOntario infrastructure for contributing sites is secured via mutually authenticated Secured Sockets Layer (SSL) connection. For mutual authentication to work, both client and server present certificates to each other, validating them against a list of ‘trusted’ certificates. Within ConnectingOntario, PKI certificates are undersigned by the eHealth Ontario Certification Authority; eHealth issues the client (e.g. hospital) a unique PKI certificate as well as a copy of the eHealth Ontario Root CA which must both be installed in the trusted store in order for the client to authenticate.

Before a PKI certificate can be issued to the contributing site, they must first generate a Certificate Signing Request (CSR) file to eHealth Ontario.

This document will provide the steps to generate the CSR file using the custom batch scripts developed by eHealth Ontario that helps simplify and standardize this process across all contributing sites involved in this process.

# Description

The following batch scripts are included in the package in the **private certs – v9.zip** file:

* + **exportToPKCS12.cmd**
    - Exports all keys stored in the current JKS store into PKCS12 format. Password will remain the same as for JKS store
  + **generateCSR.cmd**
    - generates CSR request to get a new certificate from eHealth Ontario or renew existing one
  + **importRootCA.cmd**
    - imports root CA provided by eHealth Ontario; keystore might contain more than one root CA certificates. This is quite normal, especially when the root CA is updated / changed by the provider.
  + **importSignedCert.cmd**
    - imports undersigned site certificate chain provided by eHealth Ontario. Certificate chain must correspond to the private key used to generate CSR
  + **manageKeystore.cmd**
    - provides basic operations to manage keystore (list keys, get details for stored certificate, rename or delete the keys); users do not need to execute this file
  + **settings-pk.cmd**
    - file with all configuration settings
  + **keystoreops.cmd**
    - library file with high level commands; users do not need to execute this file
  + **signCSR.cmd**
  + **settings-rootca.cmd**
  + **generateSiteKey.cmd**
  + **tmpl folder –** with the sha1sha2\_prod\_rootca.jks embedded in the folder
  + **changePassword.cmd –** use this file to change the storepass associated to your private key (.jks)

# Prerequisites

The site needs to fulfill the following prerequisites before attempting to generate the CSR:

1. Windows 7 or higher
2. Oracle Java v7 or higher
3. Computer Application Form (CAF) has already been submitted
4. eHealth Ontario has issued the site a Reference ID and Common Name (CN) following the submission of the CAF

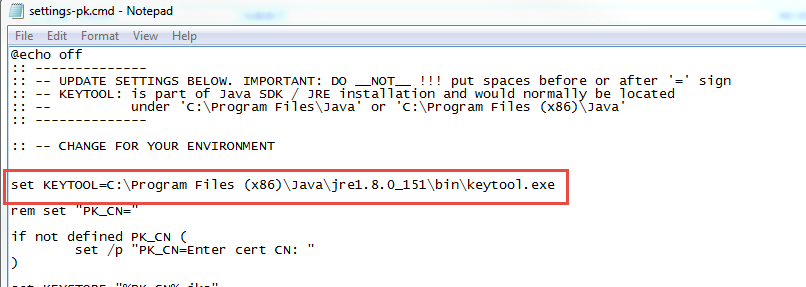
# Certificate Request & Installation Process



# Instructions

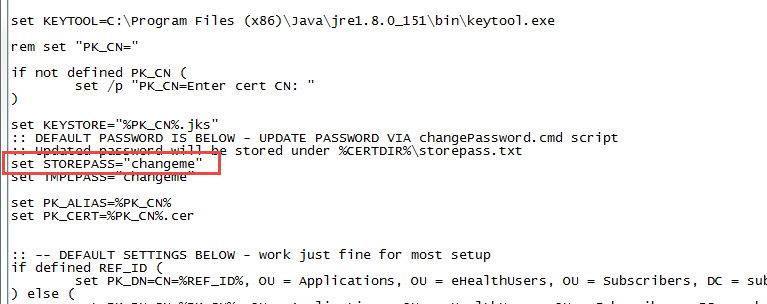
## Configuring the settings.cmd file

* 1. Unzip the **private certs – v9.zip** script package into a separate directory on a secured computer (preferably on the same computer the integration feed software resides on); this directory will be used to maintain your certificates for integration with eHealth Ontario applications
  2. Open the **settings-pk.cmd** file by right clicking and selecting the ‘edit’ button
  3. Enter the location of your keytool.exe utility. It will be located in your Java installation directory (by default – under ‘C:\Program Files\Java’ folder). In our test machine, we set the value for *KEYTOOL=C:\Program Files (x86)\Java\jre1.8.0\_101\bin\keytool.exe*



* 1. Change keystore password associated to your private key if needed (STOREPASS). Use only alpha-numeric characters

**Note:** the default STOREPASS = ***changeme | Do NOT update the password associated to “TMPLPASS” as they are for the root certificate files and cannot be altered.***



* 1. Save the changes

## Using the generateCSR.cmd file

To generate the CSR file, follow these steps:

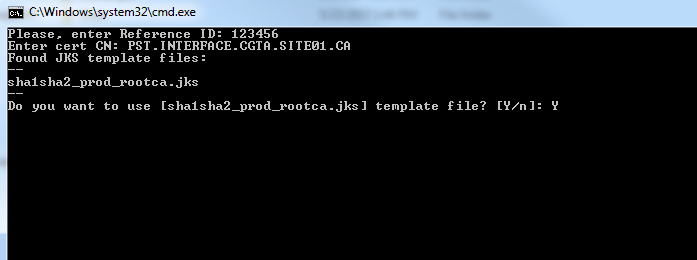
1. Double-click on the **generateCSR.cmd** script
2. At the prompt, type in reference ID provided by eHealth Ontario and click the ‘enter’ key



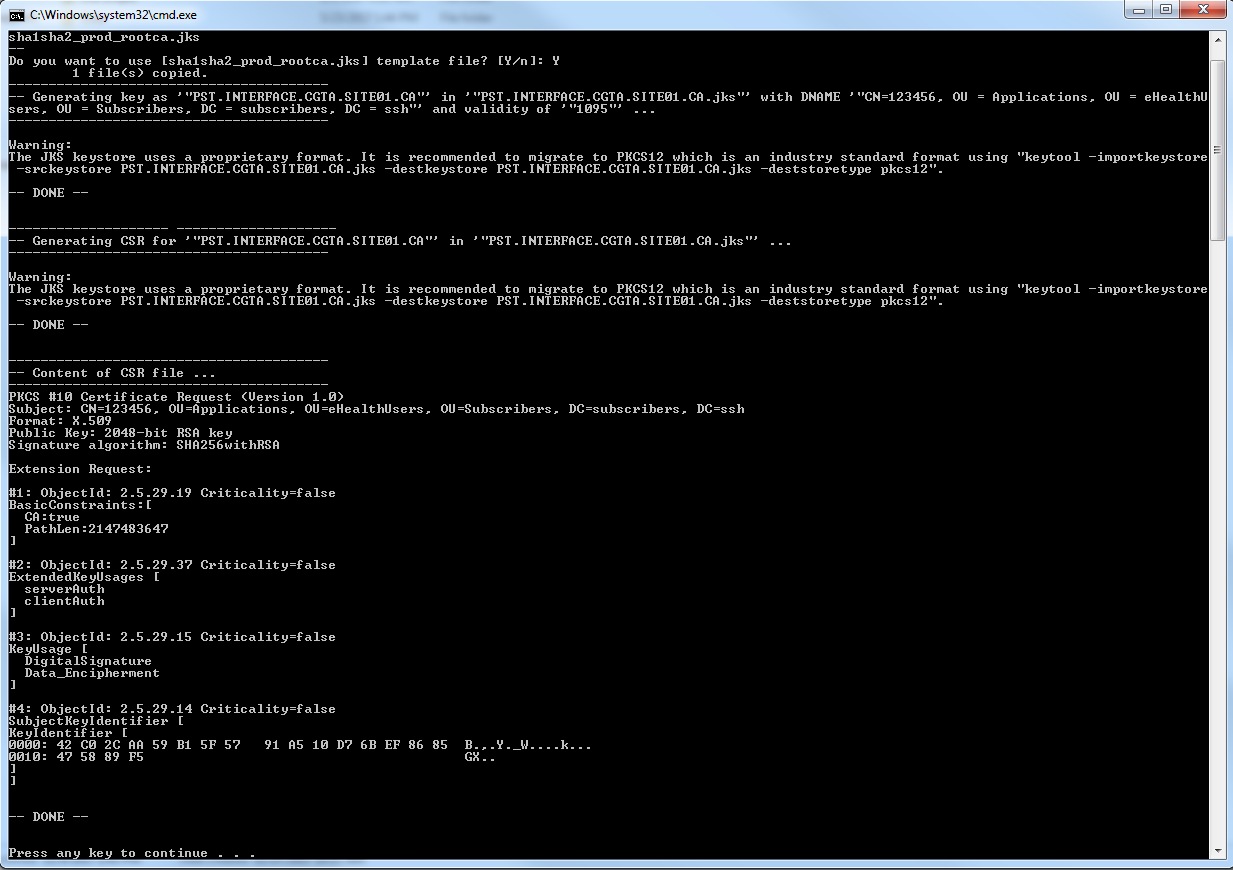
1. At the prompt, type in the Common Name (CN) provided by eHealth Ontario and click the ‘enter’ key



1. At the prompt, type “y” to the question “Do you want to use [sha1sha2\_prod\_rootca.jks] template file?” and click the ‘enter’ key



1. Once you see the information from the screenshot below, this will indicate that the CSR file was successfully created. Click the ‘enter’ key to close the window.



**Results:**

* If execution is successful, two files will be generated in “keystores\<cert CN>\certs” directory (filenames below are for default PK\_CN value):
  + PST.INTERFACE.CGTA.SITE01.CA.jks (where PST.INTERFACE.CGTA.SITE01.CA.jks is the exact certificate CN provided by eHealth Ontario)
  + PST.INTERFACE.CGTA.SITE01.CA\_123456.csr (where 1234560=reference ID)
* **generateCSR.log** file will be generated under ‘keystores\<cert CN>\logs’ directory. Review the content and compare it with the sample attached below:

****

**Note:**

* The generated .jks file will contain the private key of your undersigned certificate and the root CAs you will need.

### Next steps:

* Reply to the email containing the Reference ID by attaching the generated CSR file(s) together with generateCSR.log file.

**NOTE:** Do **NOT** send the .jks file as this contain your private key. Sending this file will result in nullify your previously assigned reference ID and a new one will need to be reissued.

* eHealth Ontario will take the CSR file to generate your undersigned certificate (i.e. PKI certificate) – the request takes approx. 2-3 business days to process. Once the request is processed, eHealth Ontario will send the undersigned site PKI certificate (public key) with the full certificate chain.
* Once eHealth has provided the PKI certificate, the site will be ready to import the undersigned certificate by executing the ‘importSignedCert.cmd’ batch script to generate the Java Keystore file (i.e. JKS). This process is described in a separate document.

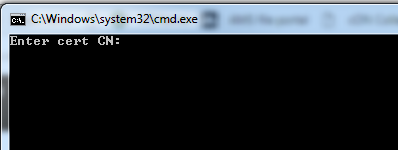
# Appendix A: Changing the Password (i.e. Storepass) associated to the Private Key

You have the option to change the password associated to the private key (i.e. jks file) after it has been generated by using the **changePassword.cmd** batch script.

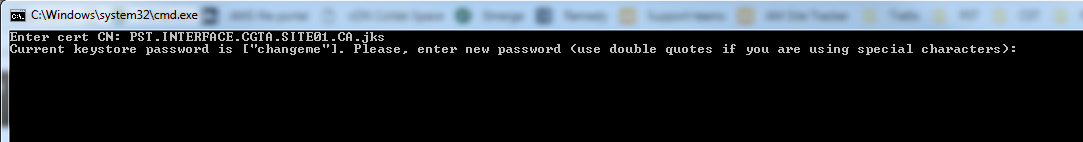
**Note:** This script can only be run after the CSR file has been generated.

To change the password, carry out these steps:

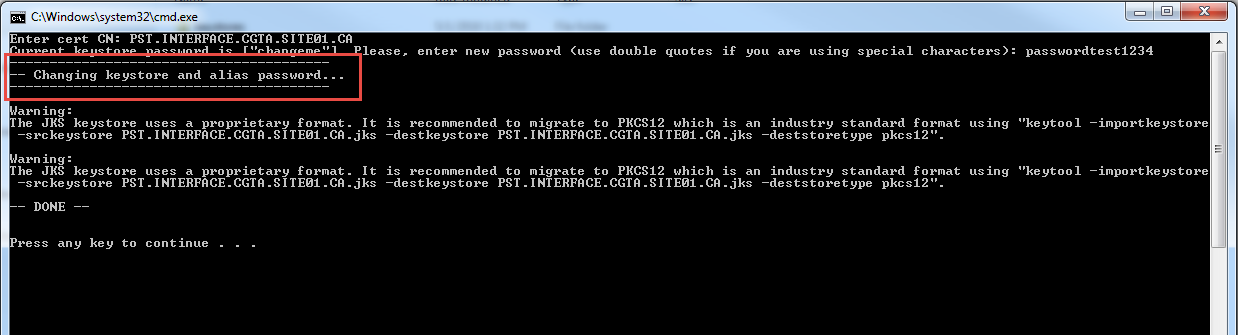
1. Click the **changePassword.cmd**
2. Enter the Certificate Common Name (CN) assigned to your site and click the ‘enter’ key



1. Enter the new password and click the ‘enter’ key



1. You will see a message of “Changing keystore and alias password” when the new password is accepted



1. The new password is stored in a file called **storepass.txt** and is located in the same directory as your private key 