eHealth Ontario
It's working for you

Certificate Implementation Package

Version: V1.1

Ontario
eHealth Ontario

1. Audience

This document is intended for clients who must leverage one or more PKI certificates for integration with eHealth Services. Readers are expected to have a general understanding of Public Key Infrastructure Certificates and an expert level of understanding of the system(s) on which the certificate(s) will be installed.

2. Introduction

PKI Certificates are used to secure communications between eHealth Ontario and client systems and are required for many eHealth service implementations.

Client organizations are responsible for installing certificates onto their infrastructure and for establishing internal processes to support certificate maintenance. While some installation instructions are included in this package to support this task, these instructions cannot cover all steps in all cases. eHealth Ontario may be able to provide additional support in such scenarios upon request.

For background information on PKI Certificates, please read the ***PKI Certificate Overview.***

Pre-requisites

Prior to the certificate request and issuance process, the following pre-requisites must be met:

- The organization must have signed a PKI Services Schedule with eHealth Ontario.
- An Application Owner (AO) should be nominated by the sponsoring organization and be registered and enrolled in the ONE® ID System. The AO is accountable for the certificate(s) issued and will be the first point of contact for issuance, management and renewal purposes. Additional information can be found in the ***Application Owner Role Overview***
- PKI Certificates are leveraged as part of the eHealth Service integration and respective service(s) may have additional requirements that are not described in this document. Please contact your service deployment representative for further details.

PKI Certificate Request & Issuance Process

This section summarizes the eHealth Ontario PKI Certificate Implementation process. For complete details, please refer to the ***Certificate Process Guide***.

1. Complete and Submit the Computer Application Registration Form or System Registry Form

The Application Owner completes the Computer Application Registration Form or System Registry From and submits via email to REGISTRATION.AGENTS@EHEALTHONTARIO.ON.CA.

For instructions on how to complete the form, please click ***here***.

2. Generate and Return the Certificate Signing Request (CSR)

eHealth Ontario issues a reference number to the Application Owner to generate a CSR and returns it to eHealth Ontario via email.

Note: eHealth Ontario has developed utilities that can be used for CSR generation. Please refer to eHealth Ontario Utilities for further details.

3. Merge Undersigned Certificate and Private Key

eHealth Ontario organization returns the new undersigned certificate via email. The Application Owner merges it with their private key prior to installation. Refer to eHealth Ontario Utilities for assistance with this step.

4. Install the Certificate(s)

The Application Owner installs the certificate in the appropriate certificate store and notifies eHealth Ontario upon successful installation.

3.1 Computer Application and System Registry Form

One of two forms must be submitted to initiate the PKI Certificate Request and Issuance Process. The form used is dependent on the service implementation.

Computer Application Form: This form register and enrolls client systems as whole, without visibility into their component parts, and is used for issuing PKI Certificates for point-to-point authentication..

For detailed information about each field, please refer the instruction guide

System Registry Form: This form registers and enrolls client systems based on their component parts and is used for issuing PKI Certificates for authentication via the eHealth HIAL.

For detailed information about each field, please refer the instruction guide.

4. eHealth Ontario Utilities

Clients are encouraged to use their organization's established tools and processes for creating CSR files and installing/managing certificates. In the absence of such tools and processes, eHealth has created utilities that can be leveraged for this purpose. Note that these utilities may not be compatible with all platforms.

CSRCreate

CSRCreate is an OpenSSL based utility for use in CSR generation and key merger for most certificate implementations.

CDR Data Contribution

CDR Data Contribution is a Java Key tool-based set of scripts specifically developed to assist in CSR generation and key merger for CDR contribution certificates for Connecting Ontario.

5. Instructions for 3rd Party Utilities

Clients may refer to the instructions below as a quick reference for common scenarios while leveraging their own processes / software:

How to create a Certificate Signing Request (CSR) and install on a MAC OX Tiger Server

Create a Keystore and Certificate Signing Request using the key tool utility

How to generate Certificate Signing Request for Apache HTTP Server

If additional support is required, clients should contact their vendor.

6. Service-specific Guides

Service-specific guides that cover common eHealth implementation scenarios are provided below:

One Mail Guides

- ONE® Mail Partnered – Client Deployment Guide for MS Exchange Server 2000/2003
- ONE® Mail Partnered – Client Deployment Guide for MS Exchange Server 2007
- ONE® Mail Partnered – Client Deployment Guide for MS Exchange Server 2010

7. Certificate Maintenance

Beyond initial installation of certificates, client organizations are responsible for establishing internal processes related to their maintenance. The Application Owner must be able to support such processes, either directly or by engaging appropriate resources.

PKI Certificate Renewal

Certificates by eHealth Ontario expire after of 3 years and must be renewed to ensure that there is no interruption to services.

In advance of a certificate's expiry date, eHealth will notify the Application Owner via email and provide a new reference number. From this point, renewal follows the same process as certificate issuance (steps 3 -7). Refer to the ***PKI Certificate Process Guide*** for complete details**.** If renewal is not required, the AO can instead request that that the renewal process be cancelled.

PKI Certificate Revocation

The Application Owner must notify eHealth Ontario in the event that a PKI Certificate is no longer required by emailing registration.agents@ehealthontario.on.ca and indicating:

- The CN of the certificate
- The Name of the Organization
- The reason for the revocation

Revocation requests may be driven by technical changes to the client's infrastructure and/or the respective eHealth Service.

Change Management

PKI certificates must be considered when implementing changes to related systems. It is the responsibility of the Application Owner to be aware of such changes and assist with an impact assessment. In the event that the change requires a new or replacement certificate to be issued, the Application Owner should email registration.agents@ehealthontario.on.ca, providing the CN of the existing certificate and a summary of the change. eHealth Ontario will work with the AO to ensure certificate requirements are met..

Application Owner Changes

The client organization is responsible for transitioning the Application Owner role in response to staff turnover and/or organization restructuring. A new Application Owner should be registered and enrolled and a request submitted to registration.agents@ehealthontairo.on.ca to transition ownership of the certificates. Refer to ***Application Owner*** for more details.