

Client Certificate Installation Guide

Creation Date: December 15, 2008 Last Updated: September 10, 2021 Revision: Version 1.2

1. TABLE OF CONTENTS

	Certreq.exe Installation Steps	10
	OpenSSL Installation Steps	10
4.	CONTACT INFORMATION	11

Alberta

2. INTRODUCTION

This document provides information on how to install an issued/approved certificate from Alberta Education.

3. INSTALLING AN ISSUED CERTIFICATE

Note: This process is only applicable for certificates which have been issued/approved by Alberta Education.

Once the certificate request is approved it will be sent via email to the account provided during the request. The following steps can be used in order to complete the process. The first step is to install the Certificate Authority Certificates and then complete the installation of the certificate sent to you.

Note: Windows Server 2016 – If you are installing certificates on Windows Server 2016 or higher you may need to install the Alberta Education root and Issuing authority certificates in the Machine certificate store instead of the current user's store (which is default when doubling clicking a certificate to install). To access the machine certificate store use MMC.exe and add the "Computer Accounts" certificate snap-in.

After downloading the certificates from the web site highlighted in step 1 below you may right click the "Trusted Root Certificate Authorities" and select "All Tasks | Import" to import the root authority certificate. Then perform the same actions but on the "Intermediate Certificate Authorities" folder importing the Alberta Education Issuing Authority Certificate. Once this is complete you may skip to the section to import the certificate you received via email.

Classification: Protected A

Last modified: 2021/Sep/10 10:18 AM

sole Root		Name		
Factorial States		control.		
Add of Remove Shap-in				
You can select snap-ins for extensible snap-ins, you	or this console fi can configure wi	on those availab	le on your computer and configure the s re enabled.	elected set of snap-ins. For
Available snap-ins:			Selected shap-ins:	
Snap-m	Vendor	^	Console Root	Edit Extensions.
ActiveX Control	Microsoft Co	y		-
Authorization Mana	Certificates in	ap-in		>
Component Service				
Computer Managen	This snap-in	vili always mana;	ge certificates for:	
Device Manager	Otyuera	scourt		
Event Vewer	O Service a	ccount		
Folder	() Computer	account		
Group Policy Object				
19 Security Monitor				
IP Security Policy M				
Description				
The Certificates map-e				
and the second se				
a nasan manana an				

Note: The screen shots shown below are taken from Windows Server 2008 using a different version of Windows may have different screens.

berta

 Using a web browser go to: <u>https://extranet.education.alberta.ca/Ae.CertificateRequest/Home/DownloadAuthorityCer</u> <u>ts/</u>.



- 2) Click on the link "Alberta Education Root Authority Certificate"
- 3) Click open



herta

4) Click Install Certificate

Į	Certificate Information
	This certificate is intended for the following purpose(s): • All issuance policies • All application policies
5 <u>4</u>	Issued to: Alberta Education Root Authority
	Issued by: Alberta Education Root Authority
	Valid from 3/12/2009 to 3/12/2029
lea	Install Certificate Issuer Statement

5) Click Next



1berta 🗖

6) Click "Place all certificates in the following store" and Browse

rtificate Import Wizard	
Certificate Store	
Certificate stores are system are	eas where certificates are kept.
Windows can automatically selec the certificate.	t a certificate store, or you can specify a location for
Automatically select the comparison of the co	ertificate store based on the type of certificate
elace all certificates in the	following store
Certificate store:	
	Browse
Learn more allowed and the stand	
Learn more about <u>certificate stores</u>	
	< Back Next > Cancel

7) Click "Trusted Root Certification Authorities" and Click Ok



- 9) Click Next
- 10) Click Finish

berta

Classification: Protected A

Certificate Import Wizard		×
F	Completing th Wizard The certificate will be in You have specified the	e Certificate Import
	Certificate Store Sele	cted by User Trusted Root Certifica Certificate
	*	n +
	< Ba	ick Finish Cancel

11) Back on the web page Click on the link "Alberta Education Issuing Authority Certificate"

12) Click open



berta

13) Click Install Certificate

1	Certificate Information
This	 certificate is intended for the following purpose(s): All application policies
	Issued to: Alberta Education Issuing Authority
	Issued by: Alberta Education Root Authority
	Valid from 3/16/2009 to 3/16/2010

14) Click Next

Certificate Import Wizard	×
	Welcome to the Certificate Import Vizard Inis wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, dick Next.
	< Back Cancel

Alberta

Last modified: 2021/Sep/10 10:18 AM

15) Click "Place all certificates in the following store" and Click Browse...

Conditional Channel		
Certificate stores are system area	s where certificates are kent.	
Windows can automatically select the certificate.	a certificate store, or you can	specify a location for
Automatically select the cer	tificate store based on the typ	e of certificate
Place all certificates in the format in t	ollowing store	
Certificate store:		
		Browse
2 0 <mark>0</mark> 2 0 0		
earn more about <u>certificate stores</u> .		

17) Click "Intermediate Certification Authorities" and Click Ok

E	Personal
	Trusted Root Certification Authorities
-0	Enterprise Trust
-6	Intermediate Certification Authorities
E	Active Directory User Object
1	Trusted Publishers
	H H

- 18) Click Next
- 19) Click Finish

berta

Classification: Protected A

The next step is to install the certificate received via email.

Certreq.exe Installation Steps

If you used the Certreq.exe application to generate your request you will use Certreq.exe to complete the process with the following steps:

- Using the computer you requested the certificate from save the attachment to C:\Certificate.txt
- 2. Click Start | Run
- 3. Type cmd <Enter>
- 4. At the command line window Type **CD** \ <Enter>
- 5. Type Certreq -Accept Certificate.txt <Enter>

Note: This step must be done on the same computer and user account that created the certificate request. Using another computer or user account will result in an error. Trying to perform these steps more than once will also produce an error.

OpenSSL Installation Steps

If you used the OpenSSL application to generate your request you will use openssl.exe to complete the process with the following steps (these steps assume that openssl is set up on your system path):

- Using the computer you requested the certificate from save the attachment to C:\Certificate.txt
- 2. Click Start | Run
- 3. Type cmd <Enter>
- 4. At the command line window Type $CD \setminus <Enter >$
- 5. Type the following (once prompted set a password for the certificate file):

openssl pkcs12 -export -out certificate.pfx -inkey server2048.key -in Certificate.txt

The above statement will create a pfx file called "certificate.pfx" for the certificate

The parameter –inkey should be set to the full path where you saved the file server2048.key when creating the request.

Certificate.txt is the file sent from Alberta Education in the email.

lberta

Classification: Protected A

Last modified: 2021/Sep/10 10:18 AM

6. Once you have the pfx file you may double click this file and import into the Windows Certificate store if that is the final destination for the certificate (the reference clients provided by PASI assume the certificate has been loaded into the Windows certificate store).

Certificate.txt – The certificate returned in the Certificate.txt file is a Base64 Encoded X509 Certificate. This is described on the Microsoft website as follows.

Base64 Encoded X.509¹

This is an encoding method developed for use with Secure/Multipurpose Internet Mail Extensions (S/MIME) which is a popular, standard method for transferring binary attachments over the Internet. Base64 encodes files into ASCII text format, making corruption less likely as the files are sent through Internet gateways, while S/MIME provides some cryptographic security services for electronic messaging applications, including non-repudiation of origin using digital signatures, privacy and data security using encryption, authentication, and message integrity.

The MIME (Multipurpose Internet Mail Extensions) specification (RFC 1341 and successors) defines a mechanism for encoding arbitrary binary information for transmission by electronic mail. Because all MIME-compliant clients can decode Base64 files, this format might be used by certification authorities that are not on Windows 2000 servers, so it is supported for interoperability. Base64 certificate files use the .cer extension.

For more information, see "RFC 2633 S/MIME Version 3 Message Specification, 1999," at <u>the Internet</u> <u>Engineering Task Force (IETF) Web site</u> and "A Layman's Guide to a Subset of ASN.1, BER and DER," an <u>RSA Laboratories</u> technical note.

4. CONTACT INFORMATION

If you have any problems installing the certificate please email srbusinesssupport@gov.ab.ca

¹ http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_cmimportexport.mspx?mfr=true