Alberta Government

Alberta Education

CLIENT CERTIFICATE REQUEST AND REGISTRATION GUIDE

Creation Date: December 15, 2008

Last Updated: December 19, 2021

Revision: Version 1.1

1. Table of contents

2. Introduction

This document provides detailed information on how to Request, Register and Obtain issued Client Certificates from Alberta Education.

The following are functions which Software Provider, School, School Authority and Ministry can perform from the Certificate Registration site:

1. **Request for a new Certificate**: Client who doesn't have a certificate yet and would like to request for a free Certificate from Alberta Education.
2. **Use Existing Certificate**: Client already has certificate issued from another Certificate Authority (CA) such as VeriSign.
3. **Download a Certificate Authority Certificates**: Once the certificate is issued from Alberta Education, the Certificate Authority Certificates also need to be installed on the system that will use them. .

3. How To Request and/or Register Certificate

3.1 Getting Started

- Visit Certificate Registration site and you should see a screen like the one below:

Certificate Registration site: https://extranet.education.alberta.ca/Ae.CertificateRequest/

For School and School Authority, select:

- Submit Client certificate request and registration for School or School Authority

For Software Provider, select:

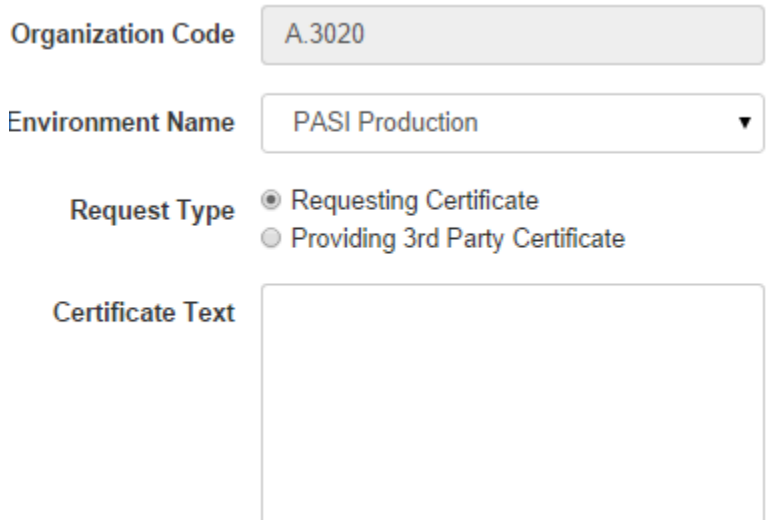
- Submit Client certificate request and registration for Software Provider

For Ministry connected systems, select:

- Submit Client certificate request and registration for Ministry Systems

3.2 Requesting a Certificate

Regardless of what type of user your system represents the there are two options for registering your certificate: Request a new Certificate or Providing and Existing Certificate. This section will focus on how to request a client certificate to be issued by Alberta Education. If you have an existing 3rd party certificate (e.g. Verisign) that you would prefer to use please refer to the section titled "Registering an Existing Certificate".



To request a new certificate you must ensure the "Requesting Certificate" option is selected as show above.

There are multiple applications that can be used to generate the Certificate Text. This document will show two examples. Regardless of the tool chosen the certificate request must meet the following requirements

3.3 Certificate Requirements

The Subject must be formed using the following format:

Software Provider

CN=SP:*Software Provider Company Name*;OU=*Product Name*,O=*AuthorityCodeOrSchoolCode*;L=*City*;S=*ProvinceOrState*;C = *Country*

Example:
CN=SP:Fake Company;OU=Fake Product;O=A.9999;L=Edmonton;S=AB;C = CA

School Authority

CN=SA:*School Authority Legal Name (A.####)*; O=*School Authority Legal Name (####)*;L=*City*,S=*ProvinceOrState*;C = *Country*

Example:
CN=SA:Authority Name (A.9999);O=Authority Name (A.9999);L=Edmonton;S=AB;C = CA

School

CN=SC:*School Name (S.####)*;OU=*School Name (####)*;O=*School Authority Legal Name (####)*;L=*City*;S=*ProvinceOrState*;C = *Country*

Example:
CN=SC:School Name (S.9999);O=School Name (S.9999);L=Edmonton,S=AB;C = CA

Ministry

CN=M:Application Name *(O.1)*; O=*GOA*;L=*City*;S= *ProvinceOrState*;C = *Country*

Example:
CN=M:Ministry Client (O.1);O=GOA;L=Edmonton;S=AB;C = CA

In all cases the Organization code in the Certificate Request subject must match the Organization code entered on the web site when submitting the request.

The 'CN' and 'O' elements can be at most 64 characters each. The 'OU' element can be at most 60 characters. If the name is too long for these elements it must be truncated to leave room for the organization code.

The request should include the following key usage and enhanced key usage attributes (and only these attributes)

- Enhanced Key Usage

  Client Authentication (1.3.6.1.5.5.7.3.2)

- Key Usage

  Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)

3.4 Using CertReq.exe for Certificate Request Generation

Certreq.exe is a command line tool provided by Microsoft. Complete instructions on how to use this utility can be found here: http://technet.microsoft.com/library/cc725793.aspx

1) Create a Request File in a text editor with the following information

```
[NewRequest]
Subject = "Must follow the rules stated in the previous section"
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE |
CERT_KEY_ENCIPHERMENT_KEY_USAGE | CERT_DATA_ENCIPHERMENT_KEY_USAGE"
Exportable = TRUE
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.2
```

Note – Remove "Exportable = TRUE" if the certificate will not be moved to another computer.

For help generating this file use the "Generate" option on the Alberta Education Certificate Registration web site.

2) Save the above file and name it CertRequest.inf
3) From the Windows command line in the same directory as the CertRequst.inf file you created in step 1 type:
   `Certreq.exe -New CertRequest.inf CertRequestOutput.txt`
4) Open the CertRequestOutput.txt file in a text editor. This text is copied into the "Certificate Text" field of the Certificate Request web application.

3.5 Using OpenSSL for Certificate Request Generation

The following commands were based on OpenSSL 0.9.8 which was current at the time of writing. For complete documentation on OpenSSL please see: https://www.openssl.org/

1) Create an OpenSSL configuration file

```
[ req ]
distinguished_name         = req_distinguished_name
req_extensions                   = v3_ca

[ req_distinguished_name ]
commonName                 = Common Name (eg, YOUR name)
countryName                      = Country Name (2 letter code)
stateOrProvinceName              = State or Province Name (full name)
localityName                     = Locality Name (eg, city)
organizationName                    = Organization Name

commonName_default                  = Name
organizationName_default            = Organization
countryName_default                 = CA
stateOrProvinceName_default         = Alberta
localityName_default                = Edmonton
```

```
[ v3_ca ]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = 1.3.6.1.5.5.7.3.2
```

Save this file using a text editor and call it: CertRequest.inf. For help generating this file use the "Generate" option on the Alberta Education Certificate Registration web site.

2) Generate a Key

From the command line (assuming that openssl.exe is in your system path):

```
openssl genrsa -out server2048.key 2048
```

The above command will generate a new private key that is 2048 bits long and store it in a file called "server2048.key".

3) Create the Certificate Request

Based on the key just generated now create the certificate request (the following is intended to be a single line).

```
openssl req -batch -new -key server2048.key -out CertRequestOutput.txt -config
certrequest.inf
```

server2048.key – this is the key file generated in step 1

certrequest.inf – this is the full path to the configuration file used to generate the certificate. An example of the contents of this file was provided at the beginning of this section.

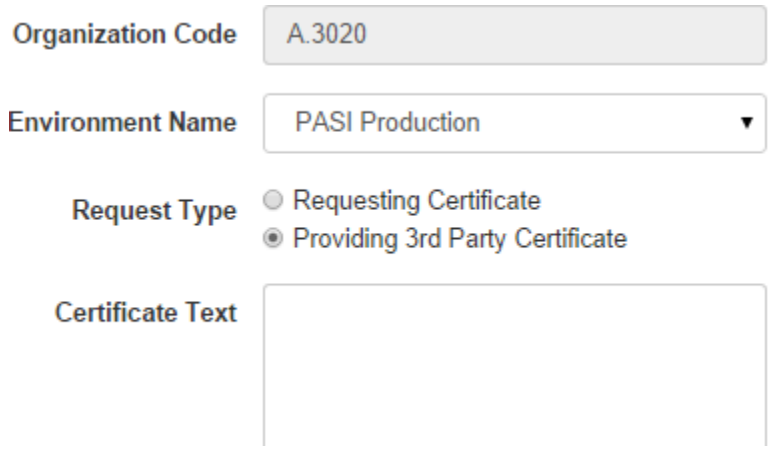
4) Open the CertRequestOutput.txt file in a text editor.

This text is copied into the "Certificate Text" field of the Certificate Request web application

3.6 Registering an Existing Certificate

If you have an existing client certificate from a recognized third part (e.g. VeriSign) you may use this certificate instead of providing a certificate request.

When sending an existing certificate it must be exported in Base64 format, copied to the Certificate Text field and the "Providing 3rd Party Certificate" option must be selected.



3.7 After Submitting

Once the certificate is successfully submitted an automated email is sent to Student Records Business Support team notifying a request has been submitted and is waiting for approval. Once the certificate request is approved it will be sent via email to the account provided.

4. Contact Information

If you have any problems with certificate request or obtaining issued certificate please email srbusinesssupport@gov.ab.ca