CDX Vendor Certificate Process

Document Version Control

Release Date	Version	Status / Comments
13 January 2014	0.01	Initial document creation
15 January 2014	0.02	Edits
10 June 2014	0.03	Edits

AUTHORS

- Jay Martens, Interior Health

EDITORS

- Cindie Robertson, Interior Health

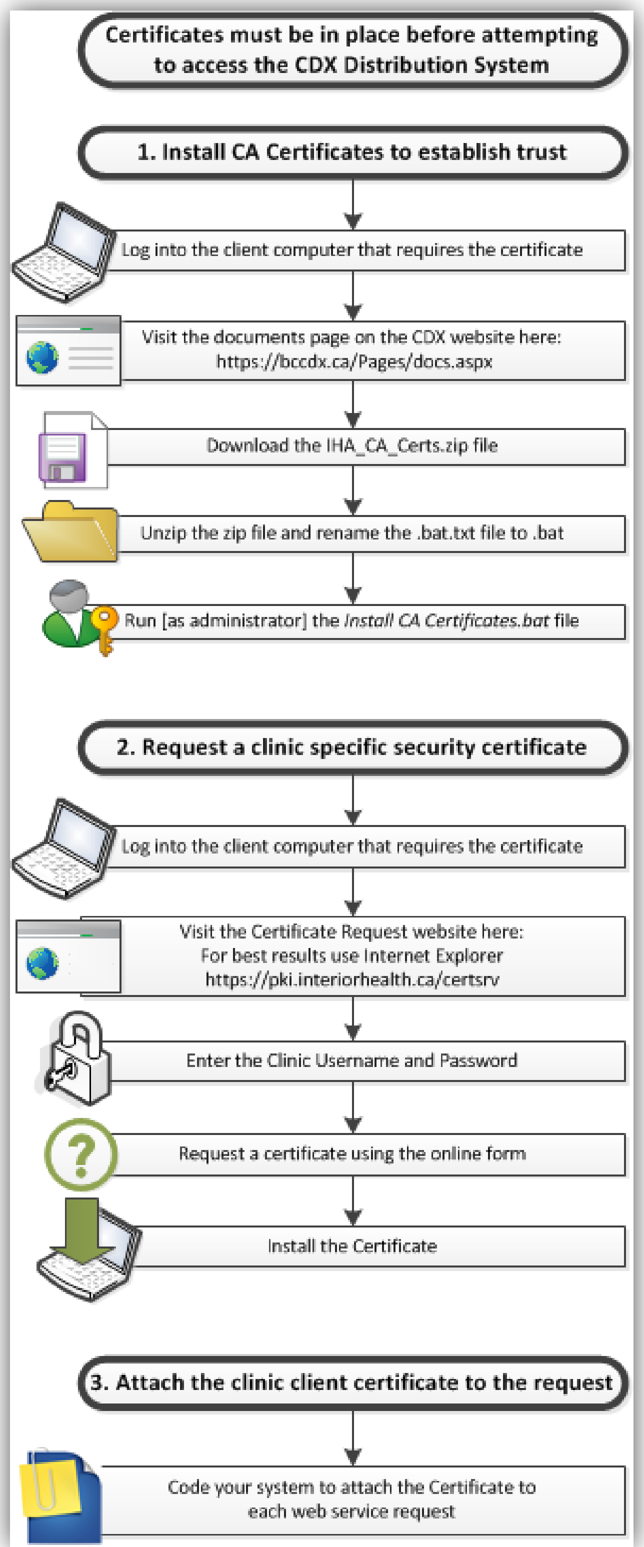
Contents

Process Overview

Business Context

The purpose of this document is to outline the process for EMR vendors to request and install security certificates for the Clinical Document eXchange (CDX) distribution system.

Process Diagram



Certificates must be in place before attempting to access the CDX Distribution System

1. Install CA Certificates to establish trust

Log into the client computer that requires the certificate

Visit the documents page on the CDX website here:
https://bccdx.ca/Pages/docs.aspx

Download the IHA_CA_Certs.zip file

Unzip the zip file and rename the .bat.txt file to .bat

Run [as administrator] the *Install CA Certificates.bat* file

2. Request a clinic specific security certificate

Log into the client computer that requires the certificate

Visit the Certificate Request website here:
For best results use Internet Explorer
https://pki.interiorhealth.ca/certsrv

Enter the Clinic Username and Password

Request a certificate using the online form

Install the Certificate

3. Attach the clinic client certificate to the request

Code your system to attach the Certificate to each web service request

Implementation Steps

Complete the following steps in order.

Precondition: Some steps require that you are logged in the target computer with local administrator permissions.

1. Install CA certificates to establish trust

This step will guide you through the download and installation of the IHA Certification Authority (CA) Certificates, this is necessary to establish the trust in the CA servers.

The .bat file is used to install Root and Intermediate CA certificates on the local host.

1. Log on to the client computer that requires the certificate
2. Go to https://bccdx.ca/Pages/docs.aspx
3. From the Vendor Information Category download and save IHA_CA_Certs.zip
4. Unzip the “IHA_CA_Certs.zip” file into a local folder
5. **Change the extension on the “Install CA Certificates” from .bat.txt to .bat**

Note: you will need to run the following batch file with an account that has local *administrator permissions* on the host:

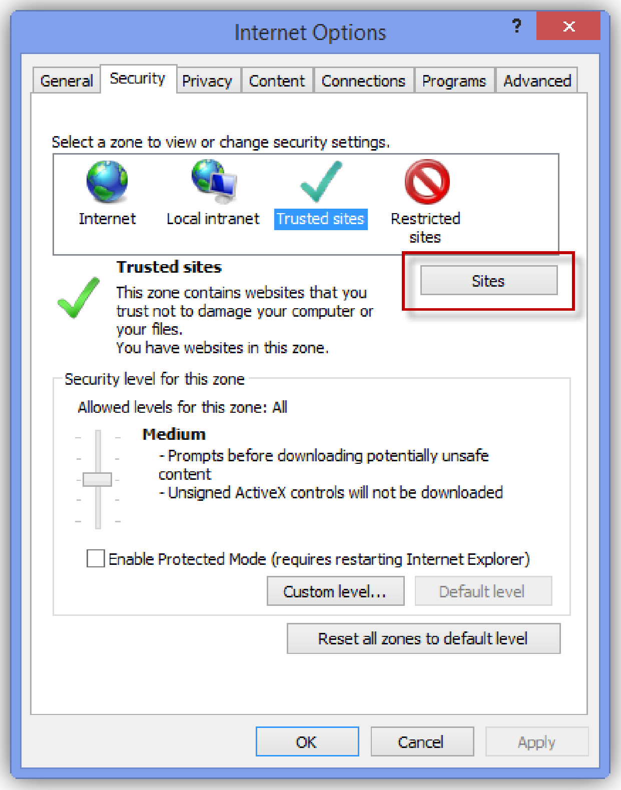
6. Run the “Install CA certificates.bat” file

2. Request a clinic specific security certificate

This step will guide you through the requesting and installation of the clinic specific security certificate.

1. Log on to the client computer with an account that requires the certificate
2. Open your web browser (for best results use Internet Explorer) and navigate to https://pki.interiorhealth.ca/certsrv

3. Add this site to the list of Trusted sites on this computer
    - Internet options > Security tab > Trusted Sites > Sites button



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

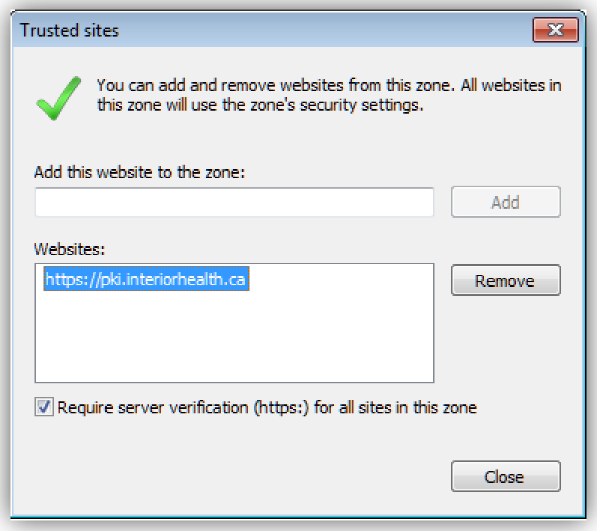
Security level for this zone

Allowed levels for this zone: All

Medium
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

- Click the Add button to add the site to the list of trusted sites.



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

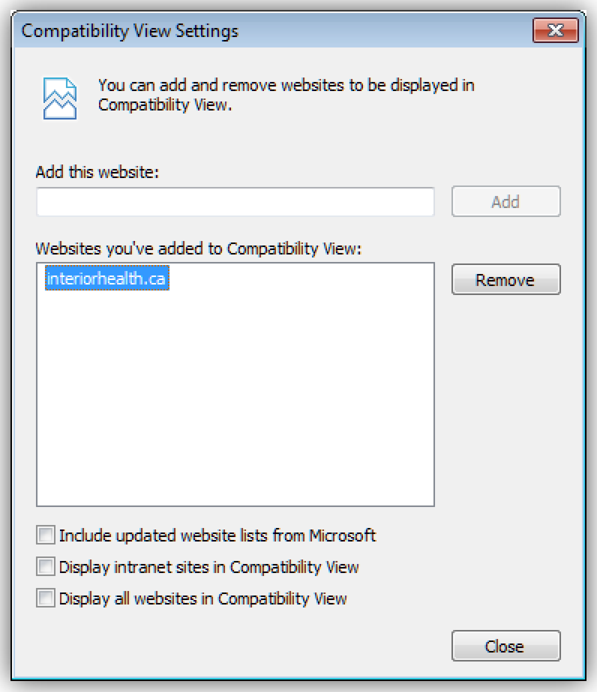
Add this website to the zone:

Websites:

https://pki.interiorhealth.ca

☑ Require server verification (https:) for all sites in this zone

4. Ensure that you are viewing this website in compatibility view
    - Tools > Compatibility View Settings > Add



Compatibility View Settings

You can add and remove websites to be displayed in Compatibility View.

Add this website:

Websites you've added to Compatibility View:

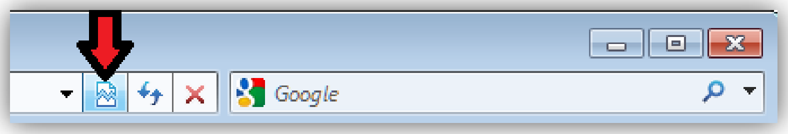
interiorhealth.ca

□ Include updated website lists from Microsoft

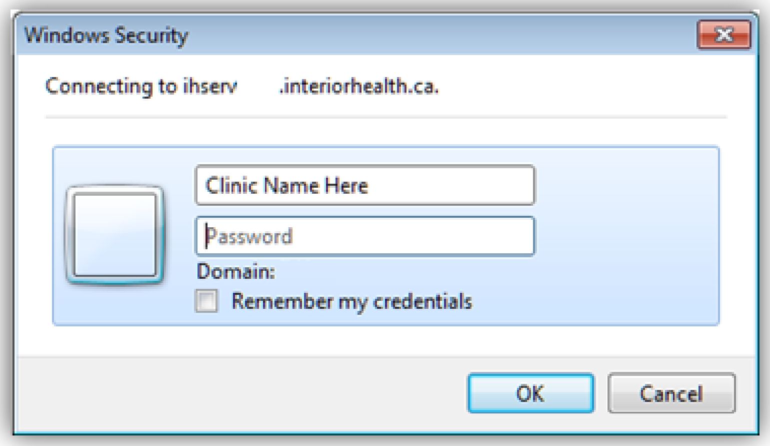
□ Display intranet sites in Compatibility View

□ Display all websites in Compatibility View

    - Click this icon to use compatibility view.



5. When challenged for a username and password, use the *clinic* account credentials Be sure to include the IHA domain in the username (i.e. IHA\cdx-abc)



Windows Security

Connecting to ihserv .interiorhealth.ca.

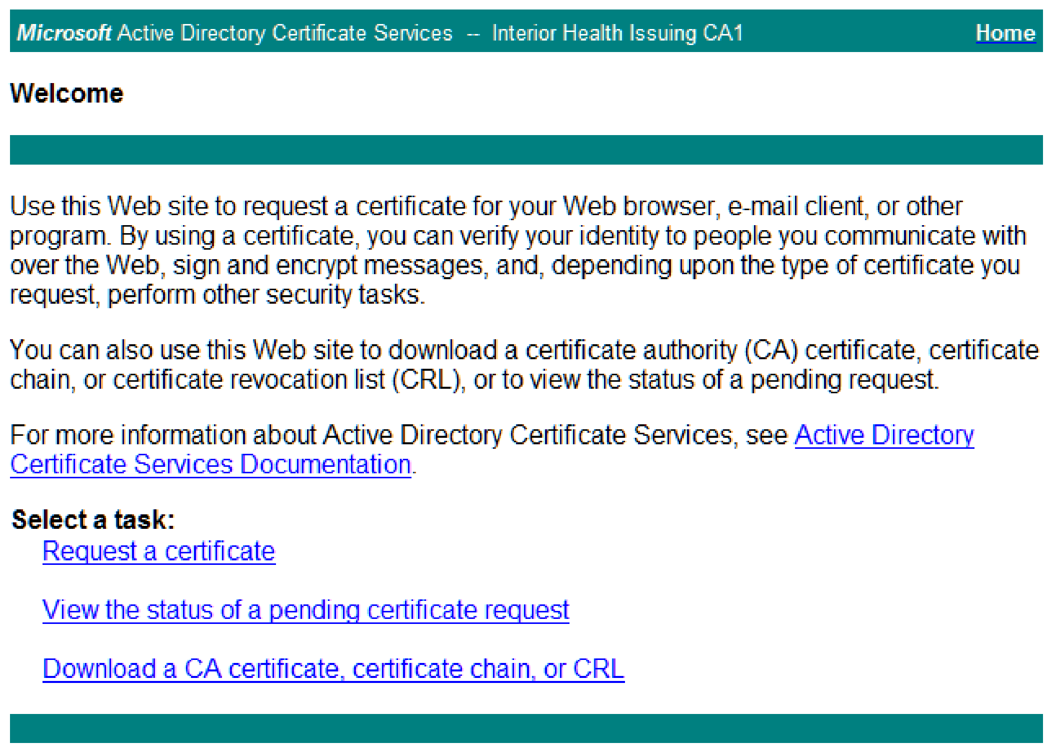
Clinic Name Here

Password

Domain:

□ Remember my credentials

6. Select “Request a Certificate”



Microsoft Active Directory Certificate Services -- Interior Health Issuing CA1 Home

Welcome

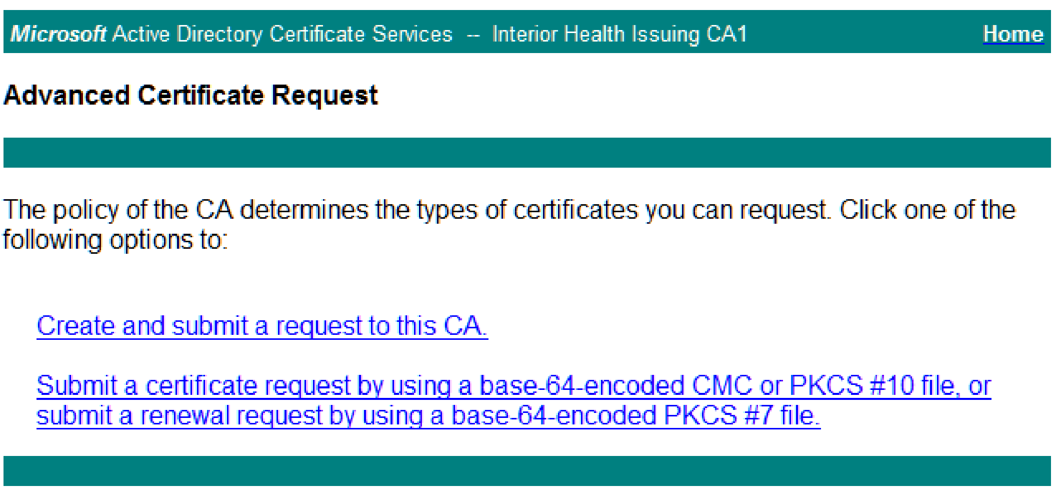
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

7. Select “Create and Submit a request”



Microsoft Active Directory Certificate Services -- Interior Health Issuing CA1 Home

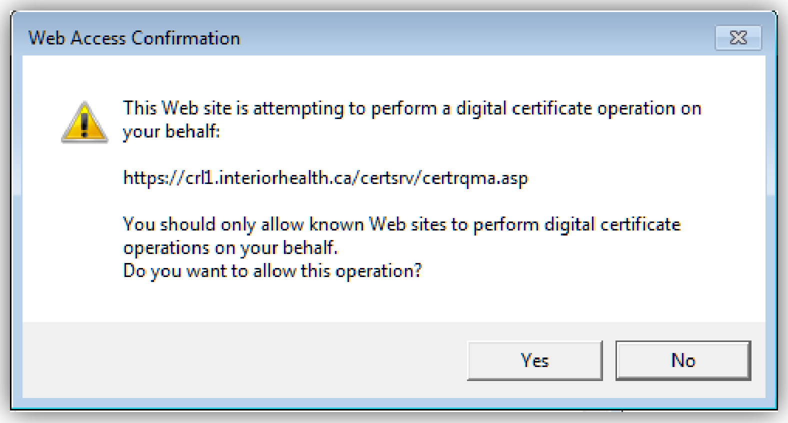
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

8. A Web Access Confirmation dialog box will appear (one or more times), click Yes to continue.



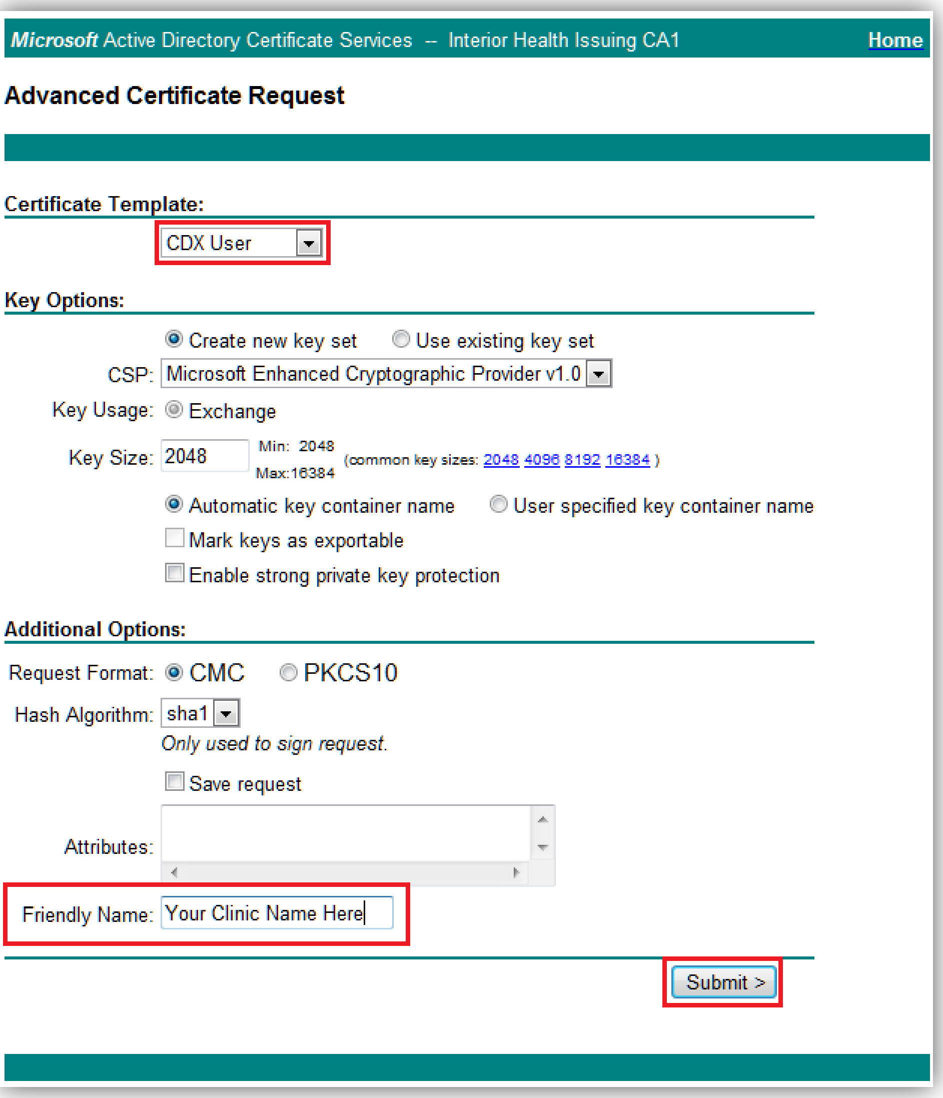
Web Access Confirmation

This Web site is attempting to perform a digital certificate operation on your behalf:

https://crl1.interiorhealth.ca/certsrv/certrqma.asp

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

9. Ensure the “CDX User” template is selected in the drop down menu
10. At the bottom of the page, enter the name of the clinic in the Friendly Name field
11. Click the Submit button.



Microsoft Active Directory Certificate Services -- Interior Health Issuing CA1 Home

Advanced Certificate Request

Certificate Template:

CDX User

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Exchange

Key Size: 2048 Min: 2048 Max:16384 (common key sizes: 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

□ Mark keys as exportable

□ Enable strong private key protection

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: sha1

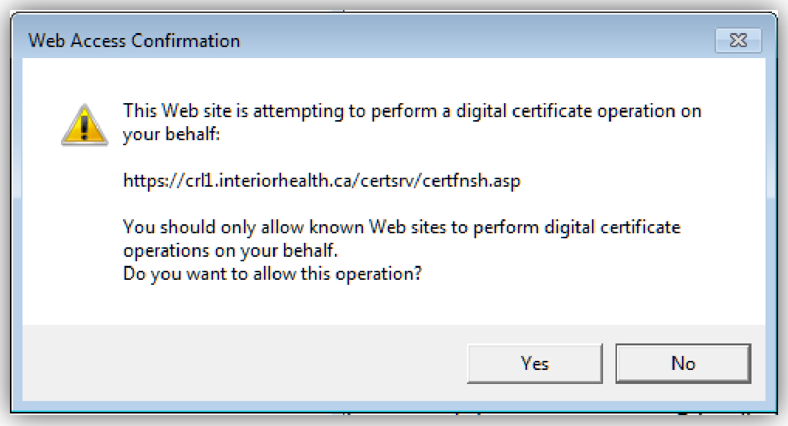
Only used to sign request.

□ Save request

Attributes:

Friendly Name: Your Clinic Name Here

12. The web page will change indicating that the request is being issued.
13. If the Web Access Confirmation dialog box appears, click Yes to continue.

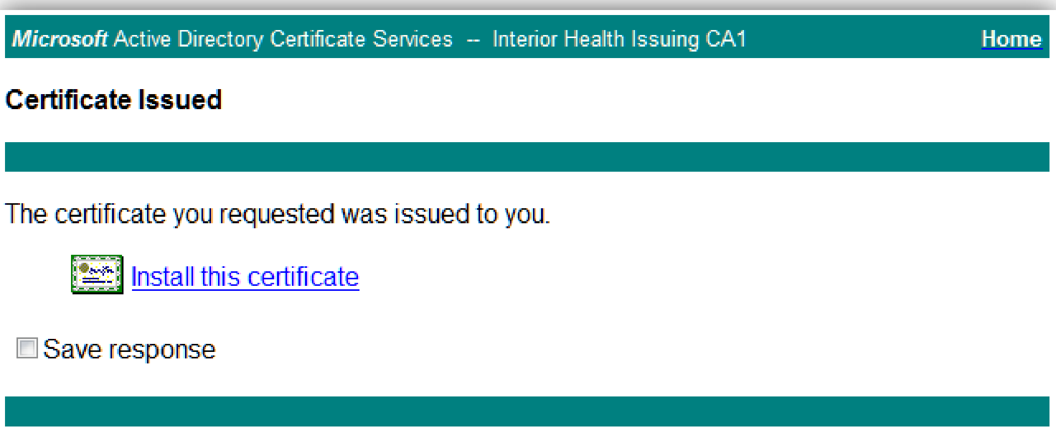


This Web site is attempting to perform a digital certificate operation on your behalf:

https://crl1.interiorhealth.ca/certsrv/certfnsh.asp

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

14. Click on the Install this certificate link.


Microsoft Active Directory Certificate Services -- Interior Health Issuing CA1
Home

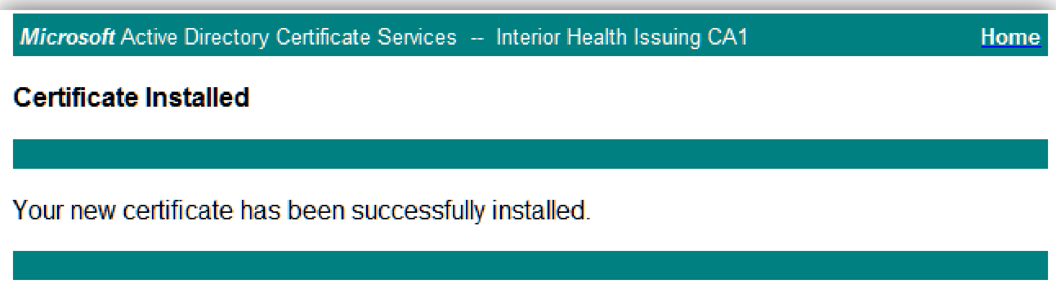
Certificate Issued

The certificate you requested was issued to you.

Install this certificate

□ Save response

15. The webpage will notify you when the Certificate has been installed.


Microsoft Active Directory Certificate Services -- Interior Health Issuing CA1
Home

Certificate Installed

Your new certificate has been successfully installed.

16. Once the certificate is installed this user account will be authorized to access the CDX system.
    - This should install the certificate in the Personal/Certificates folder in the User profile on the PC.

If you are having issues with this certificate process, please contact the CDX Analysts.

3. Attach the clinic client certificate to the request

The EMR program will need to be able to digitally attach the certificate to each web service request.

Attaching the certificate can be accomplished a few different ways and they may depend on your development language/environment.

SAMPLE ONLY (using C#)

Here is a sample tutorial that illustrates how to attach the clinic certificate to the web request:
http://www.codeproject.com/Articles/28395/Attaching-a-digital-certificate-public-key-to-an-H

Also there is a way to get the thumbprint attribute of the certificate by right clicking on the certificate (details in the troubleshooting steps below).
Then input the thumbprint into a line of code similar to this:

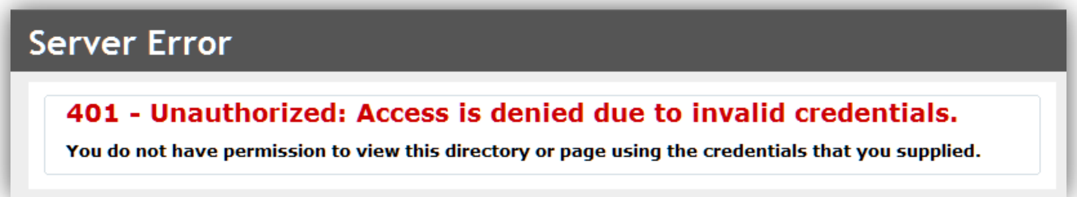
```
clientCredentials.ClientCertificate.SetCertificate (StoreLocation.CurrentUser, StoreName.My,
X509FindType.FindByThumbprint, "6D0DBF387484B25A16D7E3E53DBB978A366DA954");
```

There are a number of other great tutorials and code examples on the internet.

Troubleshooting Steps

I can’t log into the Certificate Request website

If you receive the screen below when attempting to connect to the Certificate Request website (https://pki.interiorhealth.ca/certsrv) please ensure you have installed the CA Certificates and that the credentials you have for the clinic/client device are correct.



Server Error

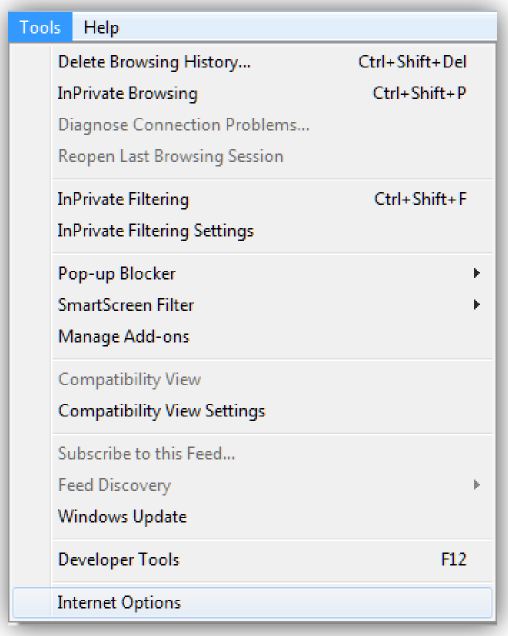
401 - Unauthorized: Access is denied due to invalid credentials.

You do not have permission to view this directory or page using the credentials that you supplied.

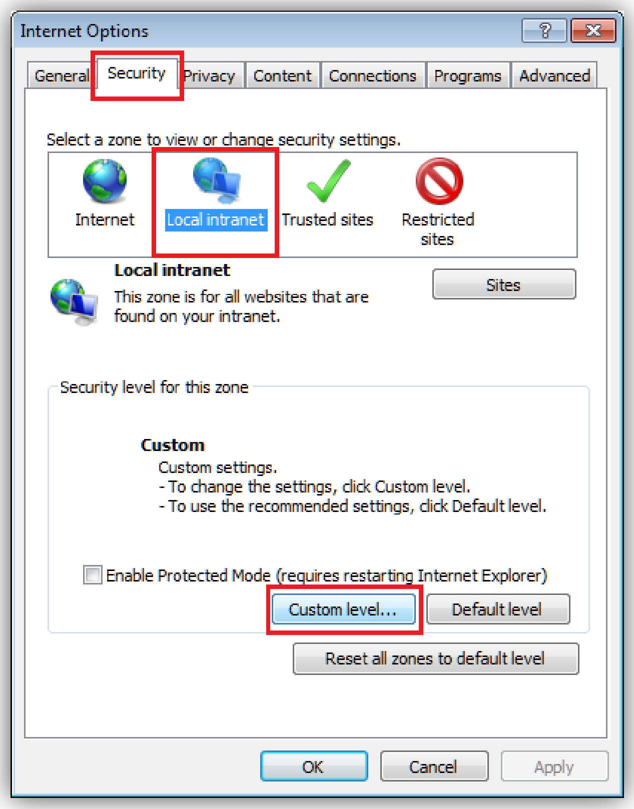
No credentials requested when accessing the Certificate Request website

If you are accessing the https://pki.interiorhealth.ca/certsrv website and no credentials are requested you will need to complete the following steps in your browser before attempting again.

Tools> Internet Options


Tools
Help
Delete Browsing History... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Diagnose Connection Problems...
Reopen Last Browsing Session
InPrivate Filtering Ctrl+Shift+F
InPrivate Filtering Settings
Pop-up Blocker
SmartScreen Filter
Manage Add-ons
Compatibility View
Compatibility View Settings
Subscribe to this Feed...
Feed Discovery
Windows Update
Developer Tools F12
Internet Options

Security Tab>Local Intranet>Custom level



Select a zone to view or change security settings.

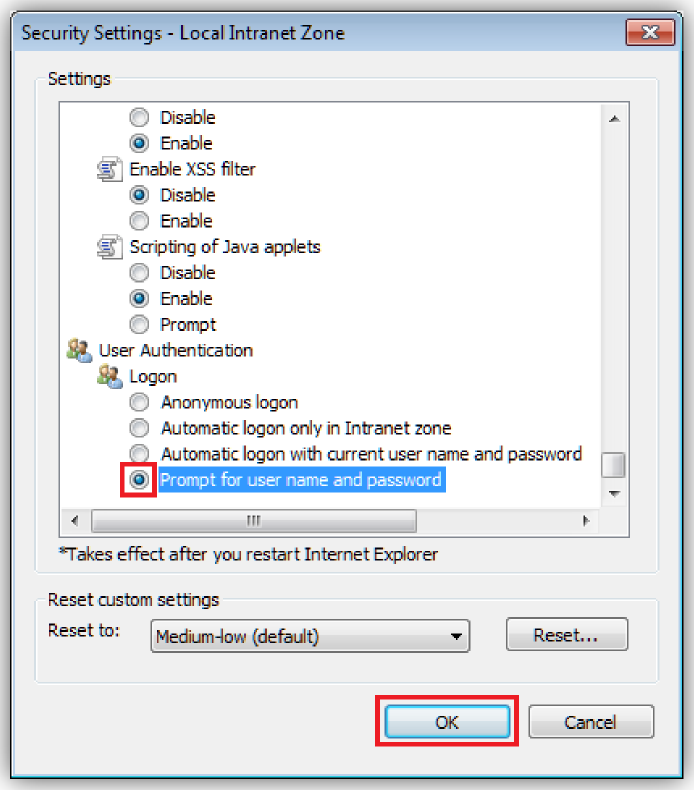
Local intranet
This zone is for all websites that are found on your intranet.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

User Authentication>Prompt for user name and password
Then click OK (you may want to set this back to the previous setting once the Certificate has been installed)



Security Settings - Local Intranet Zone

Settings

○ Disable
● Enable

Enable XSS filter
● Disable
○ Enable

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

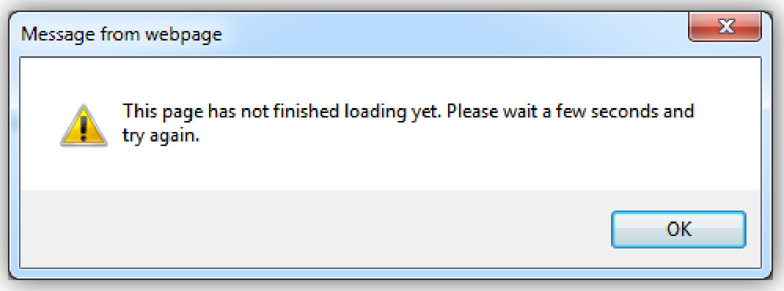
Logon
○ Anonymous logon
○ Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
● Prompt for user name and password

*Takes effect after you restart Internet Explorer

Reset custom settings
Reset to: Medium-low (default)

Website keeps loading without letting me submit

If clicking the submit button produces this message window:

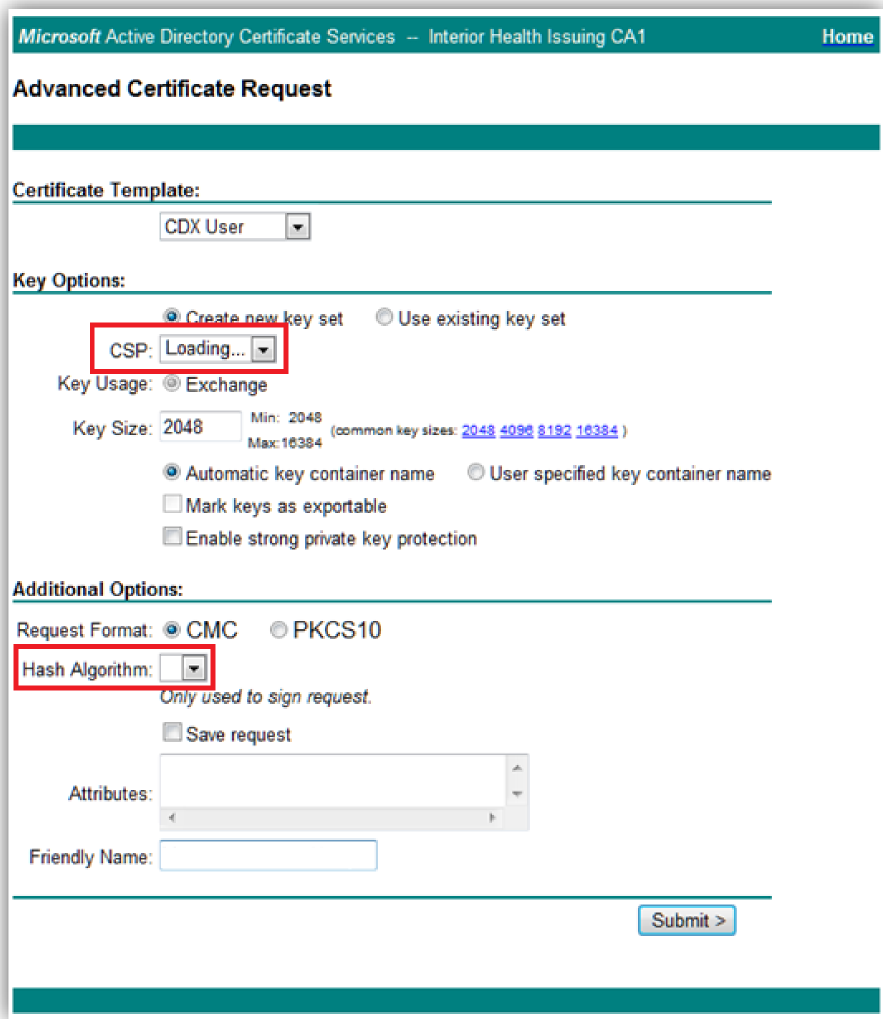


Message from webpage

This page has not finished loading yet. Please wait a few seconds and try again.

OR

If the CSP dropdown shows loading and the hash algorithm has no value for several moments – There is an issue with the trust certificates. (See example below)



Microsoft Active Directory Certificate Services -- Interior Health Issuing CA1

Advanced Certificate Request

Certificate Template:

CDX User

Key Options:

● Create new key set ○ Use existing key set

CSP: Loading...

Key Usage: ● Exchange

Key Size: 2048 Min: 2048 Max: 16384 (common key sizes: 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

□ Mark keys as exportable

□ Enable strong private key protection

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm:

Only used to sign request.

□ Save request

Attributes:

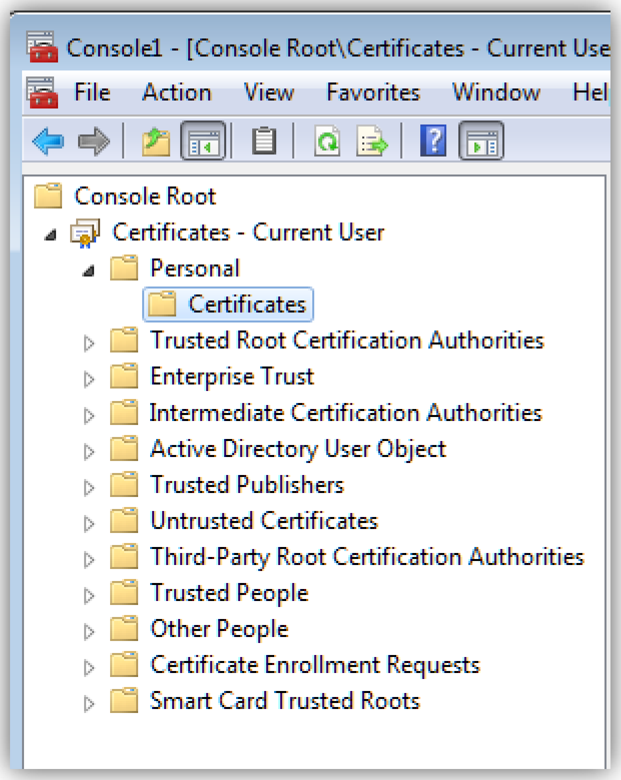
Friendly Name:

Ensure all of the CA certificates have been installed in the correct locations. Then try again to request a certificate from the website.

The CA1 and CA2 certs should be located in the Intermediate Cert Authority folder at the machine level profile.

Where does the installed clinic certificate end up?

The installed clinic certificate is placed here:

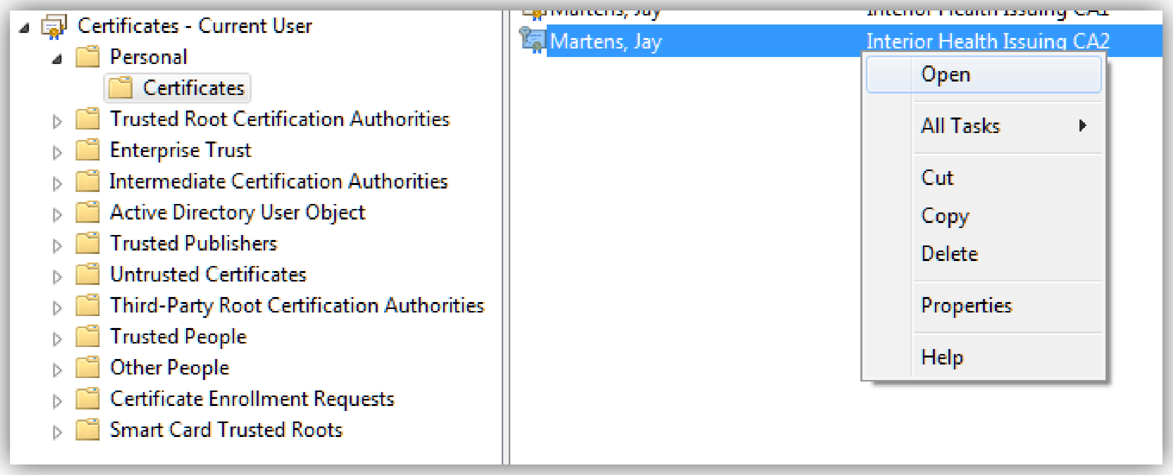

Console1 - [Console Root\Certificates - Current Use
File Action View Favorites Window Hel
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests
Smart Card Trusted Roots

*Note that it is in the Current User.

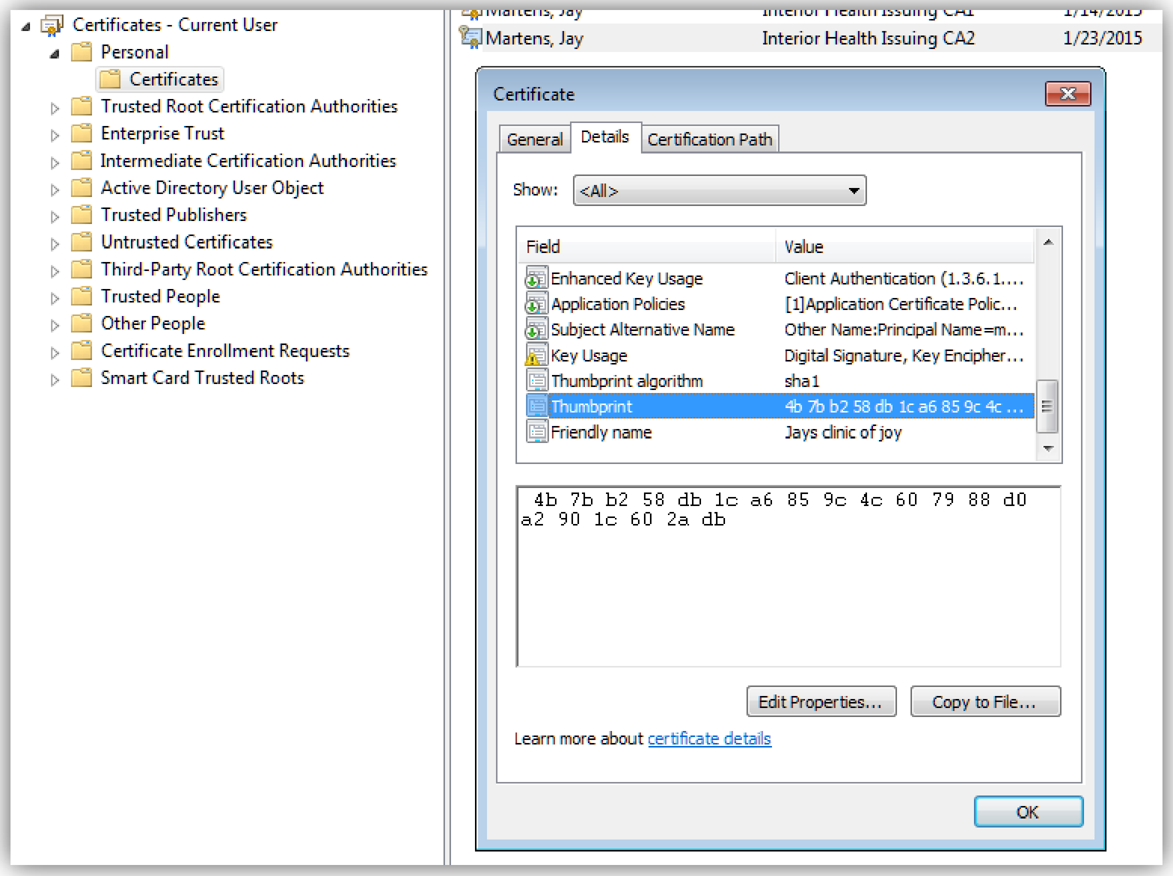
It is not enough to simply install the certificate into this location; the certificate will need to be attached to each web service request.

How to find the certificate thumbprint

If you are using the thumbprint attribute of the certificate for attaching it is found by (right clicking the certificate) Select Open.


Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests
Smart Card Trusted Roots
Martens, Jay
Interior Health Issuing CA2
Open
All Tasks
Cut
Copy
Delete
Properties
Help

In the pop up Certificate window navigate to the Details tab, Thumbprint is one of the listed attributes:


Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests
Smart Card Trusted Roots
Certificate
General
Details
Certification Path
Edit Properties...
Copy to File...
OK

Martens, Jay   Interior Health Issuing CA2   1/23/2015

Show: <All>

Field	Value
Enhanced Key Usage	Client Authentication (1.3.6.1....
Application Policies	[1]Application Certificate Polic...
Subject Alternative Name	Other Name:Principal Name=m...
Key Usage	Digital Signature, Key Encipher...
Thumbprint algorithm	sha1
Thumbprint	4b 7b b2 58 db 1c a6 85 9c 4c ...
Friendly name	Jays clinic of joy

```
 4b 7b b2 58 db 1c a6 85 9c 4c 60 79 88 d0
a2 90 1c 60 2a db
```

Learn more about certificate details