



---

# **Nebraska Crime Commission**

**Jail Data Integration, Phase-2**

**Web Service Quick Setup Guide, v1.1**

**10-05-2022**

## CONTENTS

1. Preface	3
1.1. Intended Audience	3
1.2. Introduction	3
2. Client Certificate Setup	4
3. Test Webservice & View WSDL	8
4. Obtain the Client Certificate Thumbprint	9
5. Setup & Test Client Application	10

# 1. Preface

---

## 1.1. Intended Audience

This document is intended for use by technical staff/developers that will be setting and testing the **Nebraska Crime Commission (NCC) - Jail Data Exchange (NCJISDEx)** TEST/PROD using the “Test Client Application”.

## 1.2. Introduction

This document provides a quick step-by-step setup instruction for the **Client Certificate** (heron after, **Certificate**) and the **Test-Client-App** setup and test-run. It is recommended to test using the Test-Client-App, to be familiar with the requirements and settings needed to communicate successfully with TEST & PROD endpoints. Also covered is how to view the Webservice WSDL, obtain the certificate thumbprint and run a test request (xml file submission).

Please make sure to install the Client Certificate on the same Machine using the same Account as the one used for service test. Before proceeding, it is assumed you have the following:

1. The **Client Certificate** for the TEST endpoint “ncjisdex-test.nebraska.gov”.
2. The “**Service Login Password**” that is associated with the Test-Client Certificate.
3. A copy of the “Nebraska.JailData.Exchange.TestClient” **Test Application**.
4. A copy of the **sample xml file** (data to be submitted).

#1 & #2 are mandatory for testing (and PROD later) while the #3 & #4 are used for test to make sure the environment is setup and working. Upon successful test you can use your own tools to extract data, format xml as per the NCC shared IEPD package and submit the request.

### NOTE

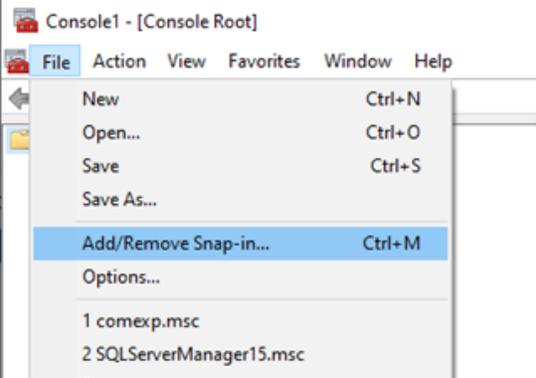
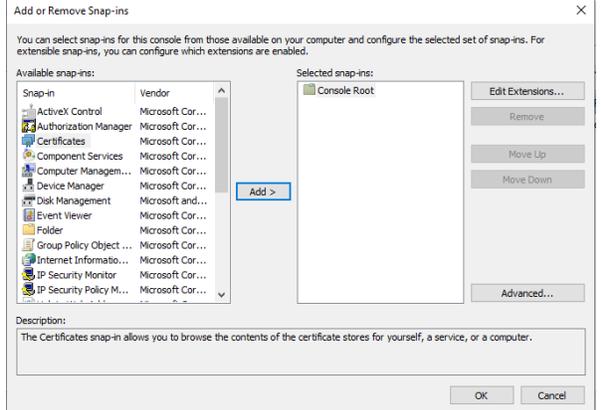
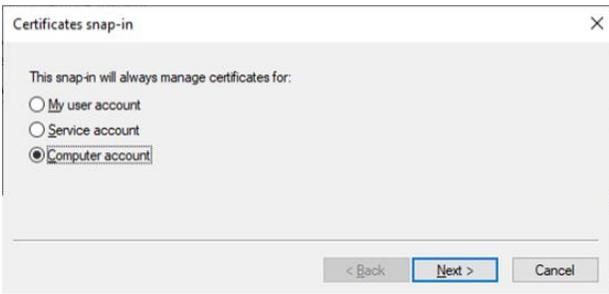
There are two passwords mentioned in this document, one is used to setup the certificate while the other is to connect/login to the webservice:

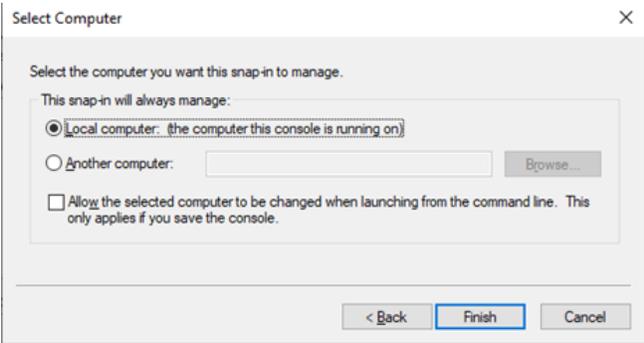
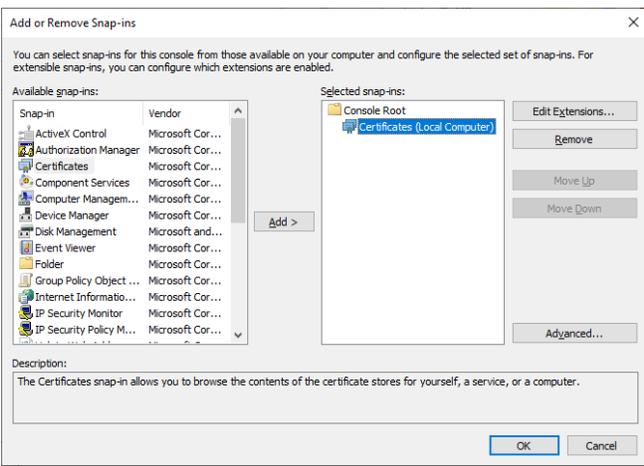
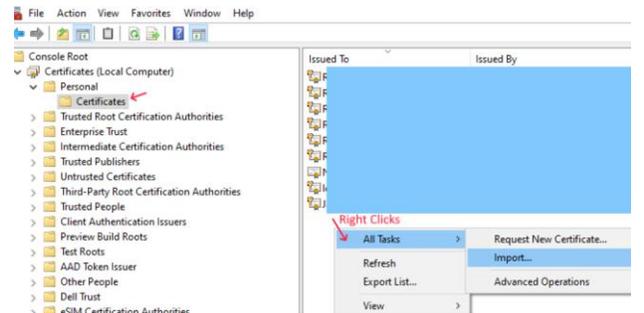
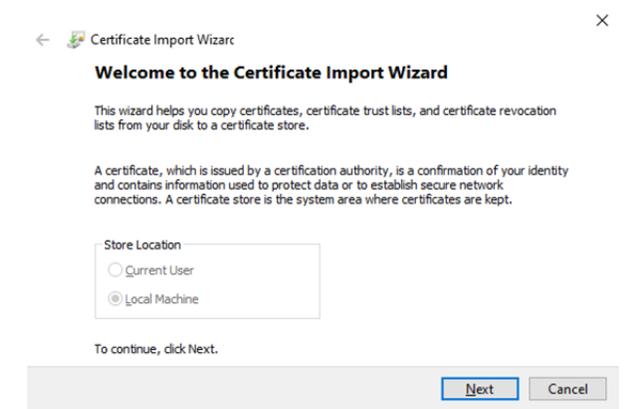
#	Description	Example
1	The <b>Client Certificate</b> file (pfx) requires a <b>Password</b> to import/install it.	<i>*aic</i>
3	The service endpoint credentials. Required “ <b>Service Login Password</b> ” related to the “ <b>Service Login Account</b> ” within the certificate	<i>ending with *</i>

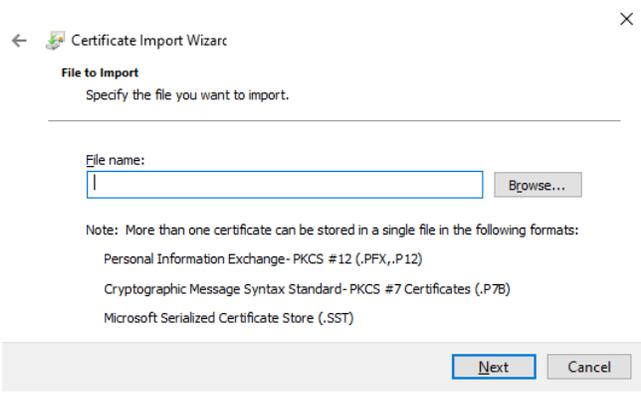
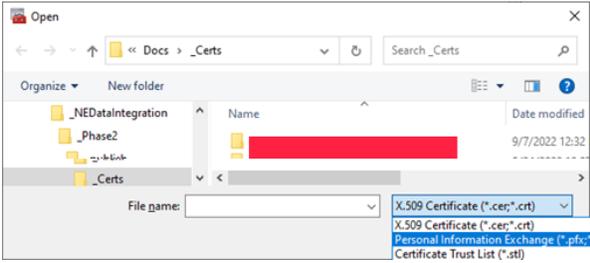
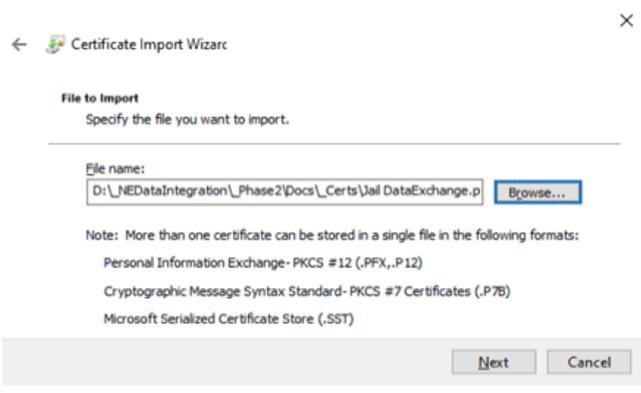
The same credentials can be used for both, TEST URI and Production URI after successful TEST.

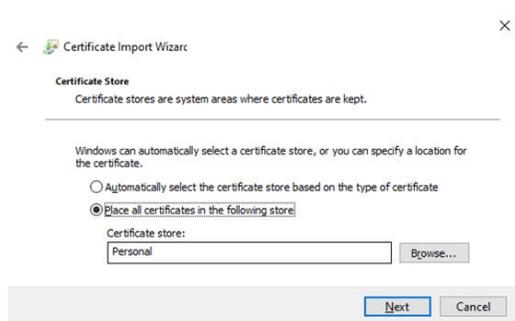
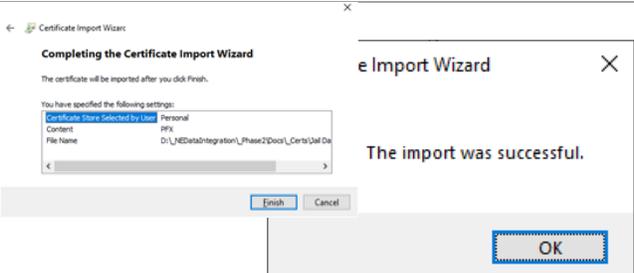
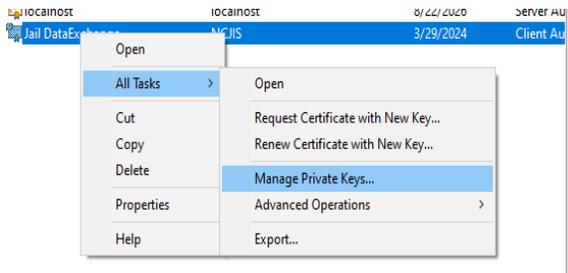
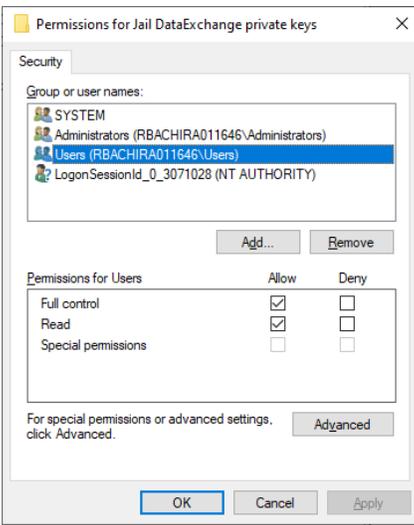
## 2. Client Certificate Setup

Before we do anything, we need to install the client certificate on your local environment, the machine that will be used to connect with the service. Following are the steps to do that:

<p><b>1</b></p>	<p>RUN <b>MMC</b> from command prompt</p>	
<p><b>2</b></p>	<p>Click <b>FILE</b> -&gt; <b>Add/Remove Snap-in</b> OR <b>CTRL+M</b></p>	
<p><b>3</b></p>	<p>Select <b>"Certificates"</b> from the left pane And click <b>ADD&gt;</b></p>	
<p><b>4</b></p>	<p>Make sure to select <b>Computer Account</b> <b>DO NOT USE "My user Account" or "Service Account"</b></p>	

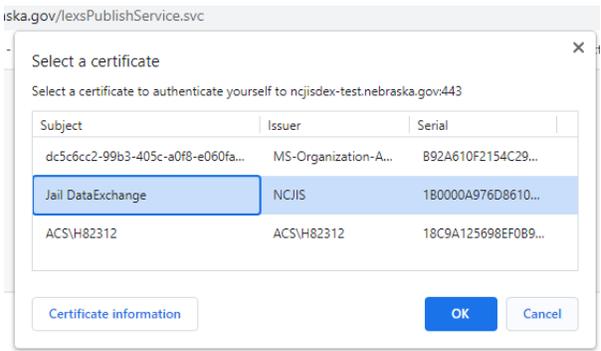
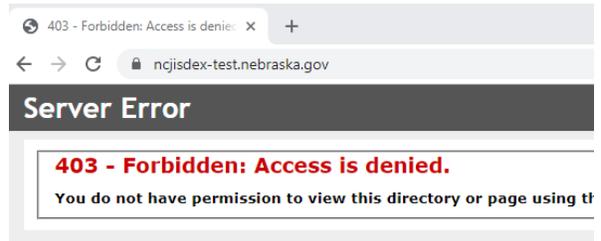
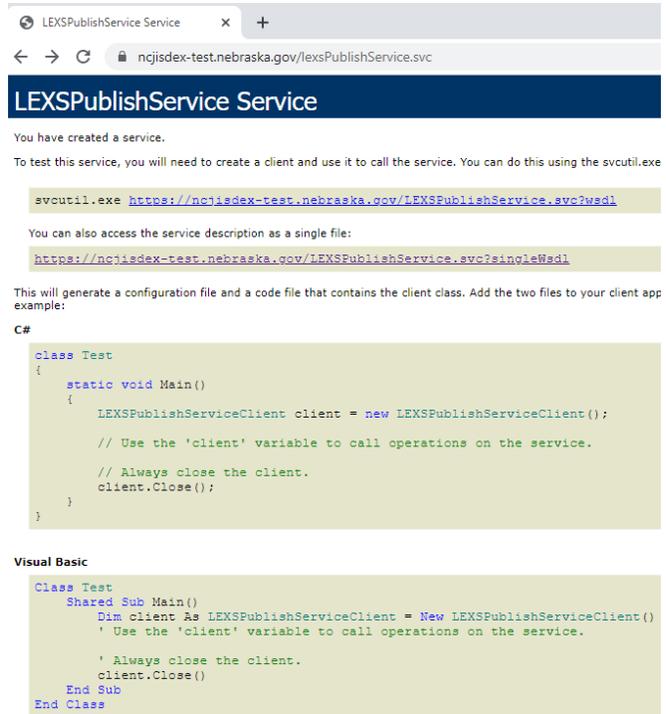
<p>5</p>	<p>Click <b>Finish</b> Keeping Local Computer selected</p>	
<p>6</p>	<p>Click <b>OK</b></p>	
<p>7</p>	<p>On the left pane Expand <b>Personal-&gt;Certificates</b> On the Right pane: - <b>Right Click</b> and select <b>All Tasks</b> <b>Import</b></p>	
<p>8</p>	<p>Local Machine is selected by default, Click <b>NEXT</b></p>	

<p><b>9</b></p>	<p>Click <b>Browse</b> and locate and select the PFX file</p>	 <p>The screenshot shows the 'Certificate Import Wizard' window. The 'File to Import' section is active, with the instruction 'Specify the file you want to import.' Below this is a 'File name:' text box and a 'Browse...' button. A note below explains that multiple certificates can be stored in a single file in formats like .PFX, .P7B, or .SST. At the bottom, there are 'Next' and 'Cancel' buttons.</p>
<p><b>10</b></p>	<p>Make sure to select .pfx from the file type combo box.</p>	 <p>The screenshot shows a Windows 'Open' dialog box. The current directory is 'D:\_Certs'. The 'File name' field is empty. The 'File type' dropdown menu is open, showing options: 'X.509 Certificate (*.cer;*.crt)', 'X.509 Certificate (*.cer;*.crt)', 'Personal Information Exchange (*.pfx;*.p7b)', and 'Certificate Trust List (*.stl)'. The .pfx file type is selected.</p>
<p><b>11</b></p>	<p>The pfx certificate file is selected, click <b>[Next]</b></p>	 <p>The screenshot shows the 'Certificate Import Wizard' window. The 'File name' field now contains the path 'D:\_NEDataIntegration\_Phase2\Docs\_Certs\Jail DataExchange.pfx'. The 'Browse...' button is highlighted. The rest of the screen is identical to the previous step.</p>
<p><b>12</b></p>	<p>Enter the certificate installation <b>[Password]</b> keeping default options Click <b>[Next]</b></p>	 <p>The screenshot shows the 'Certificate Import Wizard' window. The 'Private key protection' section is active, with the instruction 'To maintain security, the private key was protected with a password.' Below this is a 'Type the password for the private key.' section with a 'Password:' text box and a 'Display Password' checkbox. The 'Import options' section has three checkboxes: 'Enable strong private key protection...', 'Mark this key as exportable...', and 'Protect private key using virtualized-based security...', all of which are unchecked. The 'Include all extended properties.' checkbox is checked. At the bottom, there are 'Next' and 'Cancel' buttons.</p>

<p><b>13</b></p>	<p>Keep Place certificate in Personal store. Click <b>[Next]</b></p>	 <p>The screenshot shows the 'Certificate Store' step of the wizard. It asks where to place the certificates. The 'Personal' store is selected in the dropdown menu.</p>
<p><b>14</b></p>	<p>Click <b>[Finish]</b> "The import was successful" click <b>[OK]</b></p>	 <p>The screenshot shows the 'Completing the Certificate Import Wizard' screen. It displays the import settings and a confirmation message: 'The import was successful.' The 'Finish' button is highlighted, and an 'OK' button is shown in a separate window below.</p>
<p><b>15</b></p>	<p><b>Now that we have the certificate installed, we need to grant permission to user account</b></p>	
<p><b>16</b></p>	<p><b>Right Click</b> on the certificate and Select <b>All Tasks -&gt; Manage Private Keys</b></p>	 <p>The screenshot shows a context menu for a certificate. The 'All Tasks' option is selected, and the sub-menu 'Manage Private Keys...' is highlighted.</p>
<p><b>17</b></p>	<p>Add <b>"Users"</b> account and click <b>OK</b></p>	 <p>The screenshot shows the 'Permissions for Jail DataExchange private keys' dialog box. The 'Users' account is selected in the list of group or user names. The 'Full control' and 'Read' permissions are checked under the 'Allow' column.</p>

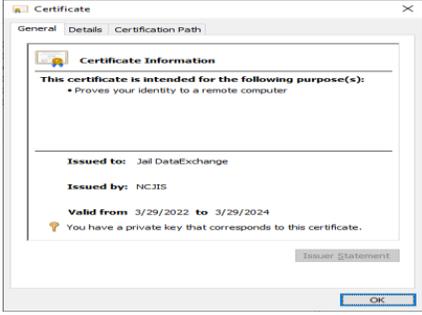
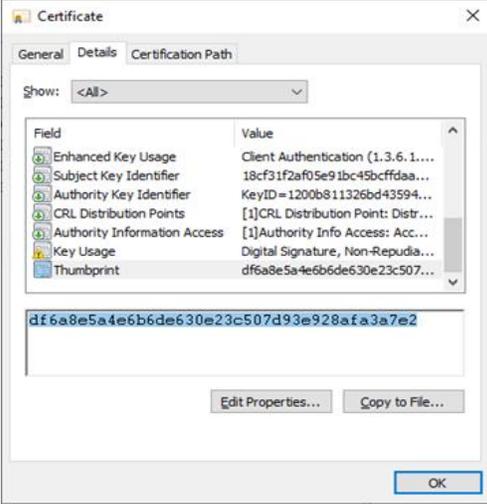
### 3. Test Webservice & View WSDL

Test the webservice to validate the certificate and the setup is accurate:

<p><b>1</b></p>	<p>Go to:  <a href="https://ncjisdex-test.nebraska.gov/lexspublishservice.svc">https://ncjisdex-test.nebraska.gov/lexspublishservice.svc</a></p> <p>You'll be prompted to select a certificate to use. Select the installed certificate.</p>	
<p><b>2</b></p>	<p>If you get this image instead of the WSDL Then check the complete URL as show above.</p>	
<p><b>3</b></p>	<p>You should get this WSDL page if all the setup is accurate.</p>	

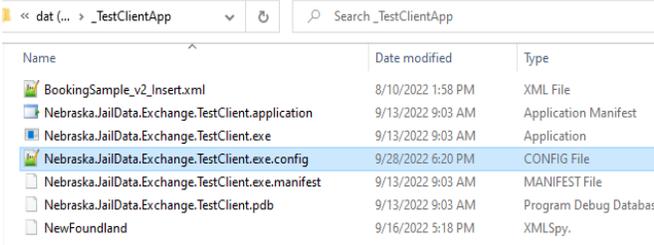
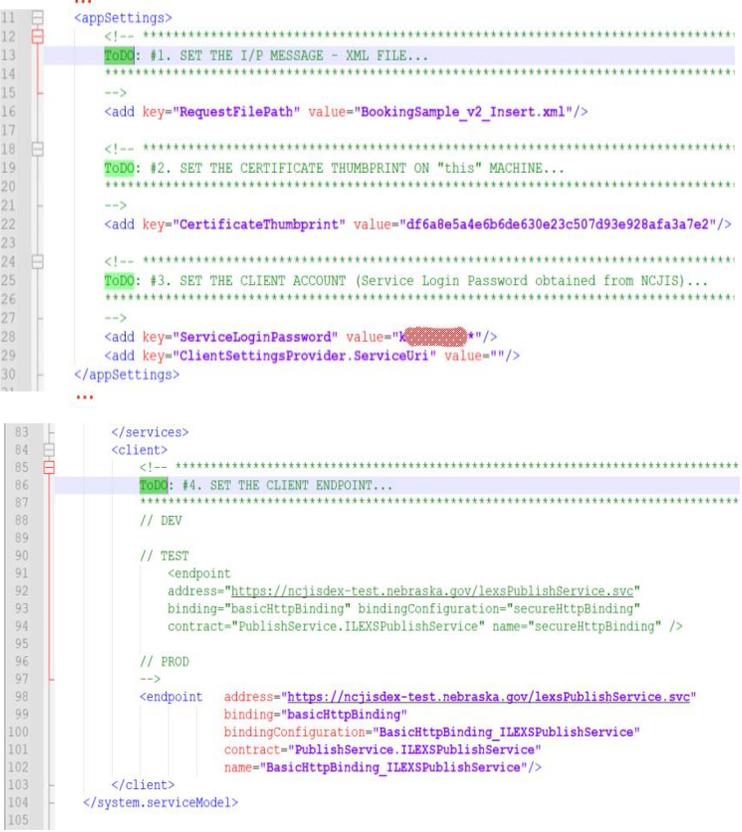
## 4. Obtain the Client Certificate Thumbprint

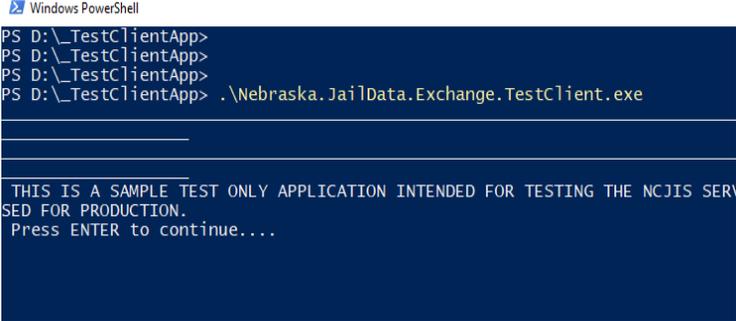
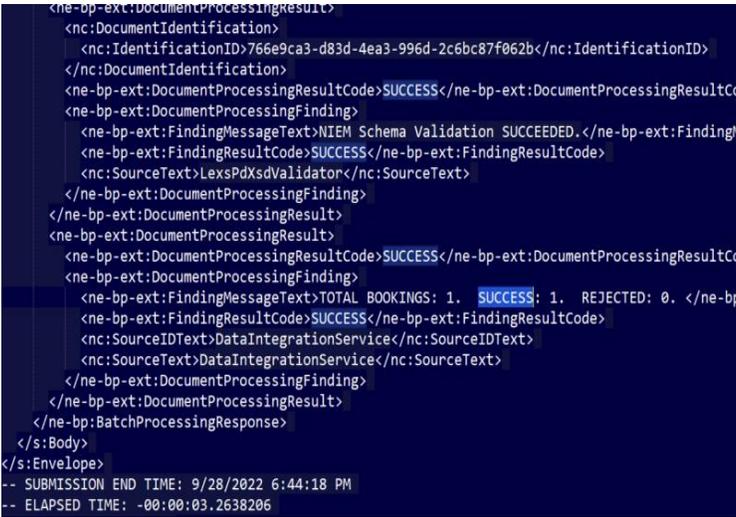
We need the Client Certificate Thumbprint to be submitted in the SOAP Message Header section to for authentication at the service endpoint. To get the thumbprint:

<p>1</p>	<p>Double Click the certificate in MMC That will open the certificate properties window</p>	
<p>2</p>	<p>Click the <b>Details</b> tab All the way at the bottom, <b>locate</b> the certificate thumbprint. From the bottom pane, <b>copy</b> the thumbprint.  Click <b>OK</b> to close</p>	
<p>3</p>	<p>The Thumbprint is to be used on the Test Client App .config file as shown on right (detail in the next section).</p>	<pre> 11 &lt;appSettings&gt; 12 &lt;!-- ***** 13 <b>ToDo: #1. SET THE I/P MESSAGE - XML FILE...</b> 14 ***** 15 --&gt; 16 &lt;add key="RequestFilePath" value="BookingSample_v2_Insert.xml"/&gt; 17 18 &lt;!-- ***** 19 <b>ToDo: #2. SET THE CERTIFICATE THUMBPRINT ON "this" MACHINE...</b> 20 ***** 21 --&gt; 22 &lt;add key="CertificateThumbprint" value="df6a8e5a4e6b6de630e23c507d93e928afa3a7e2"/&gt; 23 24 &lt;!-- ***** 25 <b>ToDo: #3. SET THE CLIENT ACCOUNT (Service Login Password obtained from NCJIS)...</b> 26 ***** 27 --&gt; 28 &lt;add key="ServiceLoginPassword" value="k*****"/&gt; 29 &lt;add key="ClientSettingsProvider.ServiceUri" value=""/&gt; 30 &lt;/appSettings&gt; 31 ***** </pre>

## 5. Setup & Test Client Application

Now you are ready to submit a sample XML file using the “Test Client App”. Please proceed with this step to make sure the environment is setup correctly and there are no credential issues:

<p>1</p>	<p>Go to the “TestClientApp” folder where you unzipped it to. Let’s assume “TestClientApp”.</p> <p>First, edit the .config file as follows</p>	
<p>2</p>	<p>In the config file there are elements marked with “ToDo:” literal (showing in green in the image on right”. There are 4 values to check/edit/confirm they are:</p> <ol style="list-style-type: none"> <li>1. XML file name to be submitted</li> <li>2. Certificate Thumbprint (from the above section)</li> <li>3. “Service Login Password” related to the “Service Login Account” within the certificate.</li> <li>4. Service Ednpoint</li> </ol> <p>replace the values as needed.</p>	
<p>3</p>	<p><b>NOTE:</b> Testing on TEST endpoint <a href="https://ncjisdex-test.nebraska.gov/lexspublishservice.svc">https://ncjisdex-test.nebraska.gov/lexspublishservice.svc</a> is required prior to submission to PROD endpoint. After successful submission, data validation, and parallel test is coordinated. A confirmation is needed so the Agency’s Account is validated for PROD submission.</p>	

<p>4</p>	<p><b>RUN the ...TestClient.exe</b></p> <p><b>you should get a message saying this app is intended for testind ONLY and not to be used for PROD with a prompt to [Press ENTER to continue]</b></p>	
<p>5</p>	<p><b>After Pressing ENTER the app should communicate with the TEST service, authenticate account, and submit the request message (xml file in the referenced in the .config).</b></p> <p><b>After processing a Response shall be returned showing the result of the request. A summary at the end of the message will indicate:</b></p> <p><b>Total Booking received</b></p> <p><b>SUCCESS Booking(s) processed</b></p> <p><b>and Rejected Booking(s)</b></p>	
<p>6</p>	<p>Here is a sample of the SOAP Header showing where the Service Login Password is located in the SOAP Message Header.</p>	<pre> &lt;soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"&gt;   &lt;soap:Header&gt;     ...     &lt;AuthPassword soap:actor="http://nebraska.gov/JailDataExchange/lexs/LEXSPublishService/1.0/ILEXSP ublishService/DoPublishRequest" xmlns="https://www.ncjis.com"&gt;       "[Service Login Password]"     &lt;/AuthPassword&gt;     ...   &lt;/soap:Header&gt;   &lt;soap:Body&gt;     ... message stream ...   &lt;/soap:Body&gt; &lt;/soap:Envelope&gt; </pre>

End of document.