



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


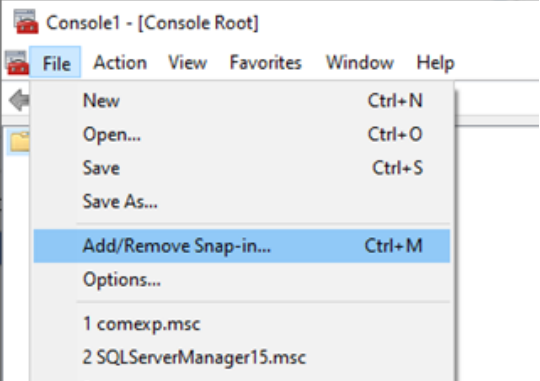
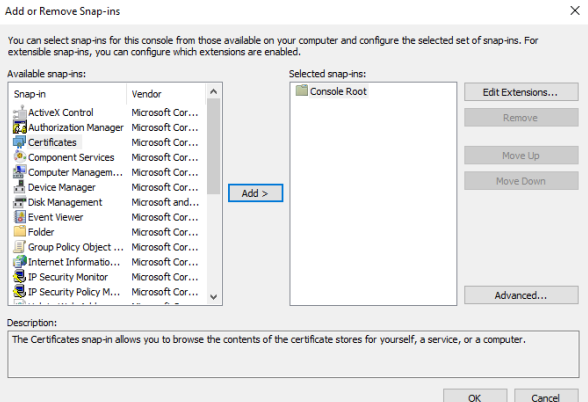
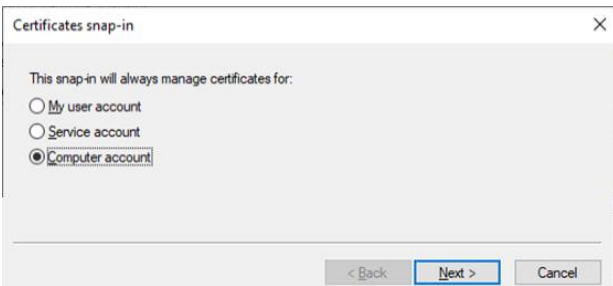
There are two passwords mentioned in this document, one is used to setup the certificate while the other is to connect/login to the webservice:

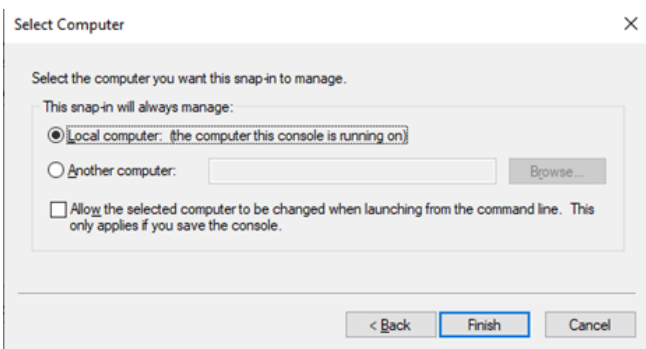
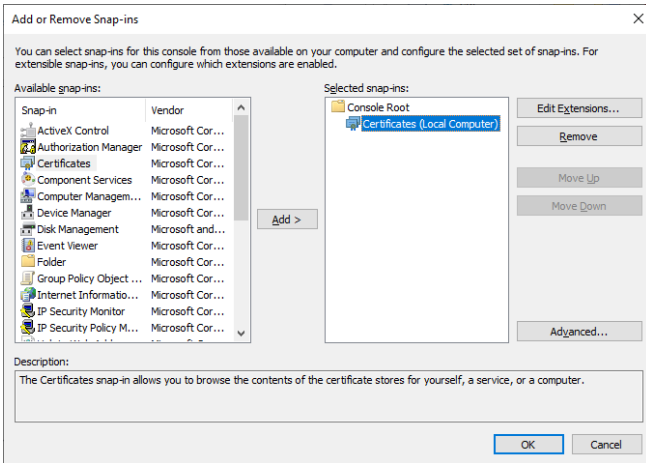
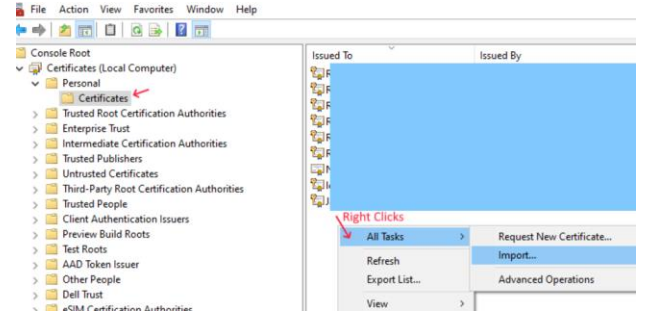
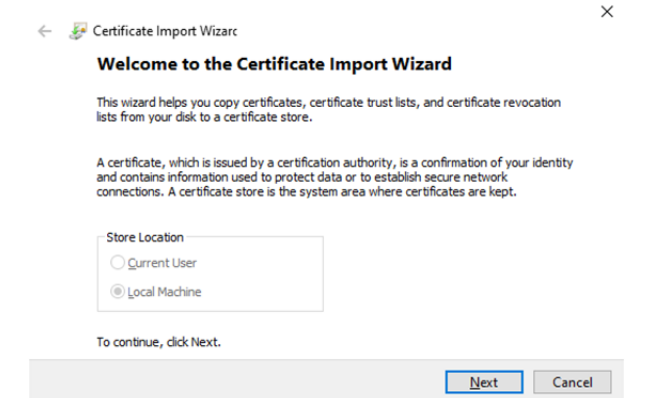
#	Description	Example
1	The Client Certificate file (pfx) requires a Password to import/install it.	<i>*aic</i>
3	The service endpoint credentials. Required “ Service Login Password ” related to the “ Service Login Account ” within the certificate	<i>ending with *</i>

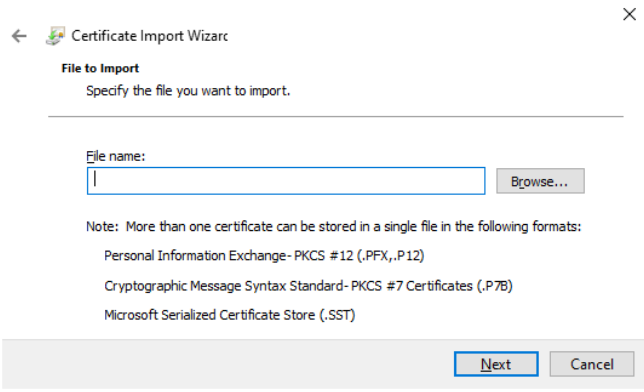
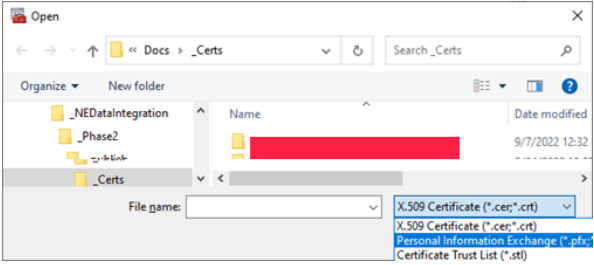
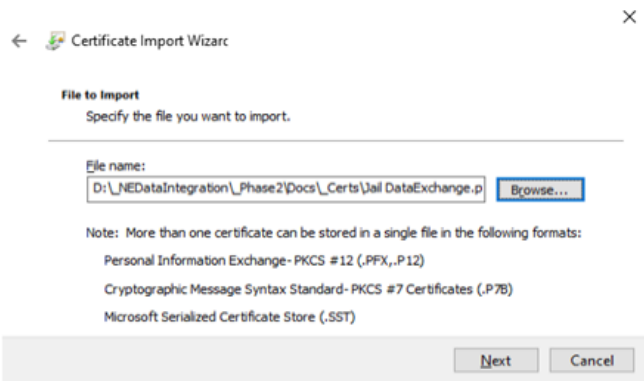
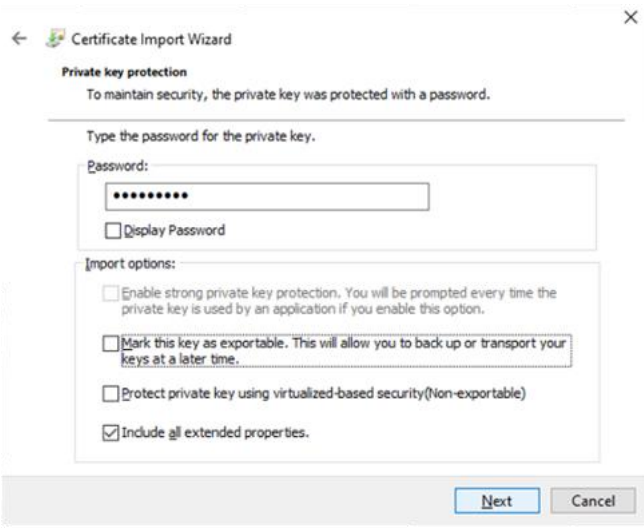
The same credentials can be used for both, TEST URI and Production URI after successful TEST.

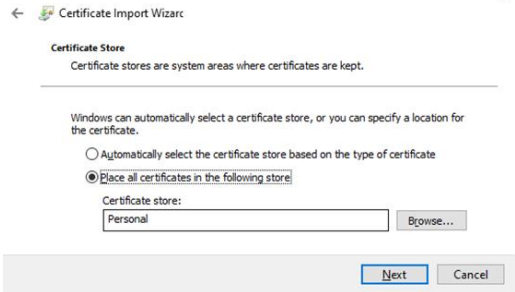
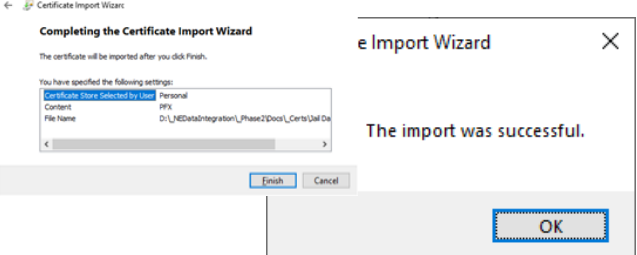
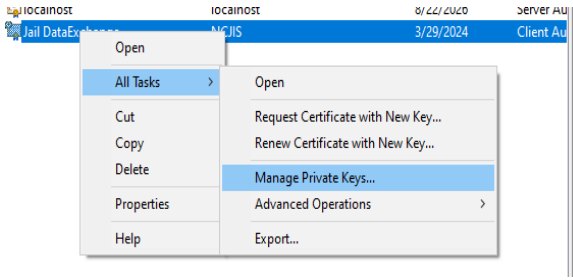
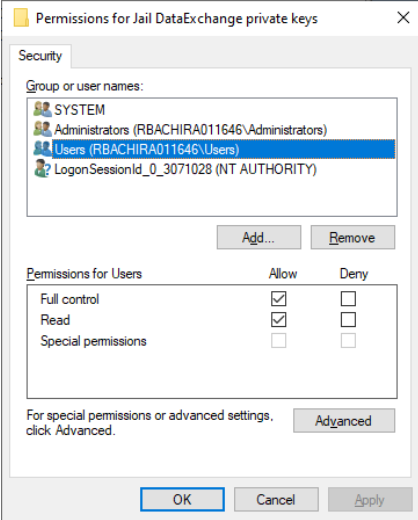
2. Client Certificate Setup

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:

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

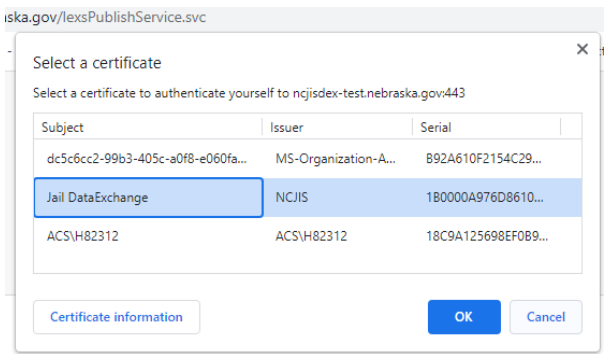
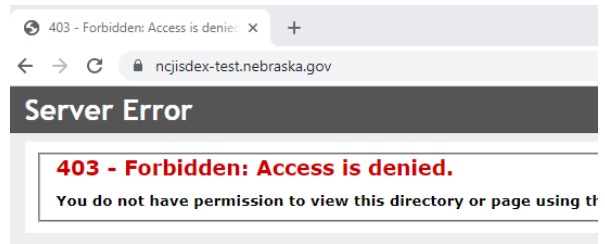
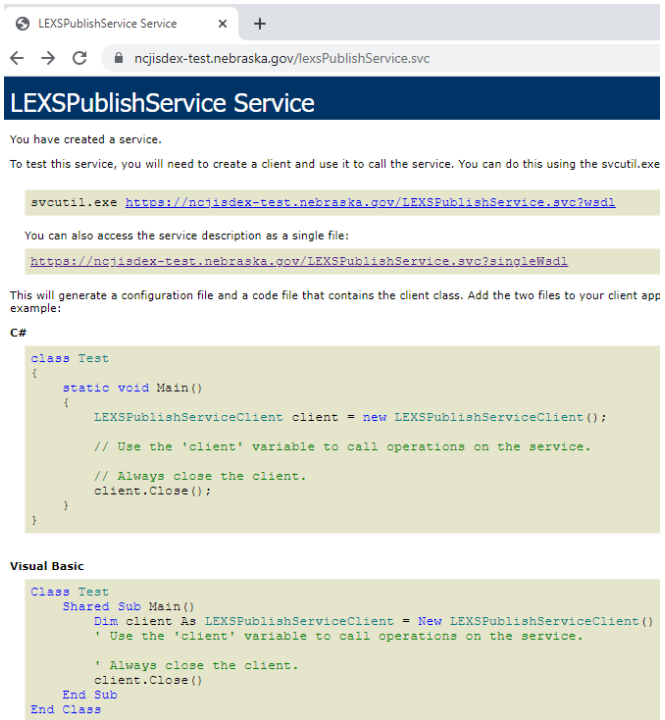
5	Click Finish Keeping Local Computer selected	 <p>Select Computer</p> <p>Select the computer you want this snap-in to manage.</p> <p>This snap-in will always manage:</p> <p><input checked="" type="radio"/> Local computer: (the computer this console is running on)</p> <p><input type="radio"/> Another computer: <input type="text"/> Browse...</p> <p><input type="checkbox"/> Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.</p> <p>< Back Finish Cancel</p>																												
6	Click OK	 <p>Add or Remove Snap-ins</p> <p>You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.</p> <p>Available snap-ins:</p> <table><thead><tr><th>Snap-in</th><th>Vendor</th></tr></thead><tbody><tr><td>ActiveX Control</td><td>Microsoft Cor...</td></tr><tr><td>Authorization Manager</td><td>Microsoft Cor...</td></tr><tr><td>Certificates</td><td>Microsoft Cor...</td></tr><tr><td>Component Services</td><td>Microsoft Cor...</td></tr><tr><td>Computer Managem...</td><td>Microsoft Cor...</td></tr><tr><td>Device Manager</td><td>Microsoft Cor...</td></tr><tr><td>Disk Management</td><td>Microsoft and...</td></tr><tr><td>Event Viewer</td><td>Microsoft Cor...</td></tr><tr><td>Folder</td><td>Microsoft Cor...</td></tr><tr><td>Group Policy Object ...</td><td>Microsoft Cor...</td></tr><tr><td>Internet Informatio...</td><td>Microsoft Cor...</td></tr><tr><td>IP Security Monitor</td><td>Microsoft Cor...</td></tr><tr><td>IP Security Policy M...</td><td>Microsoft Cor...</td></tr></tbody></table> <p>Selected snap-ins:</p> <ul style="list-style-type: none">Console RootCertificates (Local Computer) <p>Add ></p> <p>Edit Extensions... Remove Move Up Move Down Advanced...</p> <p>Description:</p> <p>The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.</p> <p>OK Cancel</p>	Snap-in	Vendor	ActiveX Control	Microsoft Cor...	Authorization Manager	Microsoft Cor...	Certificates	Microsoft Cor...	Component Services	Microsoft Cor...	Computer Managem...	Microsoft Cor...	Device Manager	Microsoft Cor...	Disk Management	Microsoft and...	Event Viewer	Microsoft Cor...	Folder	Microsoft Cor...	Group Policy Object ...	Microsoft Cor...	Internet Informatio...	Microsoft Cor...	IP Security Monitor	Microsoft Cor...	IP Security Policy M...	Microsoft Cor...
Snap-in	Vendor																													
ActiveX Control	Microsoft Cor...																													
Authorization Manager	Microsoft Cor...																													
Certificates	Microsoft Cor...																													
Component Services	Microsoft Cor...																													
Computer Managem...	Microsoft Cor...																													
Device Manager	Microsoft Cor...																													
Disk Management	Microsoft and...																													
Event Viewer	Microsoft Cor...																													
Folder	Microsoft Cor...																													
Group Policy Object ...	Microsoft Cor...																													
Internet Informatio...	Microsoft Cor...																													
IP Security Monitor	Microsoft Cor...																													
IP Security Policy M...	Microsoft Cor...																													
7	On the left pane Expand Personal->Certificates On the Right pane: - Right Click and select All Tasks Import	 <p>File Action View Favorites Window Help</p> <p>Console Root</p> <ul style="list-style-type: none">Certificates (Local Computer)<ul style="list-style-type: none">Personal<ul style="list-style-type: none">Certificates (Right Clicked)Trusted Root Certification AuthoritiesEnterprise TrustIntermediate Certification AuthoritiesTrusted PublishersUntrusted CertificatesThird-Party Root Certification AuthoritiesTrusted PeopleClient Authentication IssuersPreview Build RootsTest RootsAAD Token IssuerOther PeopleDell TrusteGSM Certification Authorities <p>Right Clicks</p> <ul style="list-style-type: none">All TasksRefreshExport List...ViewRequest New Certificate...Import...Advanced Operations																												
8	Local Machine is selected by default, Click NEXT	 <p>← Certificate Import Wizard</p> <p>Welcome to the Certificate Import Wizard</p> <p>This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.</p> <p>A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.</p> <p>Store Location</p> <p><input type="radio"/> Current User</p> <p><input checked="" type="radio"/> Local Machine</p> <p>To continue, click Next.</p> <p>Next Cancel</p>																												

9	Click Browse and locate and select the PFX file	 <p>The screenshot shows the 'Certificate Import Wizard' window, 'File to Import' step. It prompts the user to specify the file to import. The 'File name' field is empty, and the 'Browse...' button is visible. Below the field, a note states: 'Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange - PKCS #12 (.PFX,.P12), Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B), Microsoft Serialized Certificate Store (.SST)'. The 'Next' and 'Cancel' buttons are at the bottom right.</p>
10	Make sure to select .pfx from the file type combo box.	 <p>The screenshot shows a File Explorer window titled 'Open' with the address bar set to 'Docs > _Certs'. The file list shows a folder named '_Certs' with a date modified of '9/7/2022 12:32'. The 'File name' field is empty, and the file type dropdown is set to 'All files (*.*)'. The file list shows several files, including 'X.509 Certificate (*.cer;*.crt)', 'X.509 Certificate (*.cer;*.crt)', 'Personal Information Exchange (*.pfx;*.p12)', and 'Certificate Trust List (*.stl)'.</p>
11	The pfx certificate file is selected, click [Next]	 <p>The screenshot shows the 'Certificate Import Wizard' window, 'File to Import' step. The 'File name' field now contains the path 'D:_NEDDataIntegration_Phase2\Docs_Certs\Jail DataExchange.pfx'. The 'Browse...' button is still visible. The note and buttons at the bottom are the same as in the previous step.</p>
12	Enter the certificate installation [Password] keeping default options Click [Next]	 <p>The screenshot shows the 'Certificate Import Wizard' window, 'Private key protection' step. It prompts the user to type the password for the private key. The 'Password' field is empty, and the 'Display Password' checkbox is unchecked. Below the password field, the 'Import options' section shows several checkboxes: 'Enable strong private key protection' (unchecked), 'Mark this key as exportable' (unchecked), 'Protect private key using virtualized-based security (Non-exportable)' (unchecked), and 'Include all extended properties' (checked). The 'Next' and 'Cancel' buttons are at the bottom right.</p>

13	Keep Place certificate in Personal store. Click [Next]	 <p>The screenshot shows the 'Certificate Store' step of the Certificate Import Wizard. It explains that certificate stores are system areas where certificates are kept. It offers two options: 'Automatically select the certificate store based on the type of certificate' (unselected) and 'Place all certificates in the following store:' (selected). The 'Certificate store' dropdown is set to 'Personal'. The 'Next' button is highlighted.</p>												
14	Click [Finish] “The import was successful” click [OK]	 <p>The screenshot shows the 'Completing the Certificate Import Wizard' screen. It states 'The certificate will be imported after you click Finish.' It lists the specified settings: Certificate Store (Personal), Content (PKIX), and File Name (D:_MEDDataIntegration_Phase2\Docs\Jail Data Exchange\...). The 'Finish' button is highlighted. Below this, a separate window shows 'The import was successful.' with an 'OK' button highlighted.</p>												
15	Now that we have the certificate installed, we need to grant permission to user account													
16	Right Click on the certificate and Select All Tasks -> Manage Private Keys	 <p>The screenshot shows a right-click context menu for a certificate named 'Jail DataExchange'. The 'All Tasks' option is selected, and the 'Manage Private Keys...' option is highlighted in the submenu.</p>												
17	Add “Users” account and click OK	 <p>The screenshot shows the 'Permissions for Jail DataExchange private keys' dialog box. In the 'Group or user names' list, 'Users (RBACHIRA011646\Users)' is selected. The 'Permissions for Users' table shows 'Full control' and 'Read' permissions checked under the 'Allow' column. The 'OK' button is highlighted.</p> <table border="1"> <thead> <tr> <th>Permissions for Users</th> <th>Allow</th> <th>Deny</th> </tr> </thead> <tbody> <tr> <td>Full control</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Read</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Special permissions</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Permissions for Users	Allow	Deny	Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Special permissions	<input type="checkbox"/>	<input type="checkbox"/>
Permissions for Users	Allow	Deny												
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>												
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>												
Special permissions	<input type="checkbox"/>	<input type="checkbox"/>												

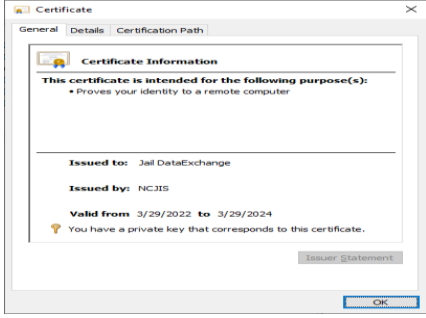
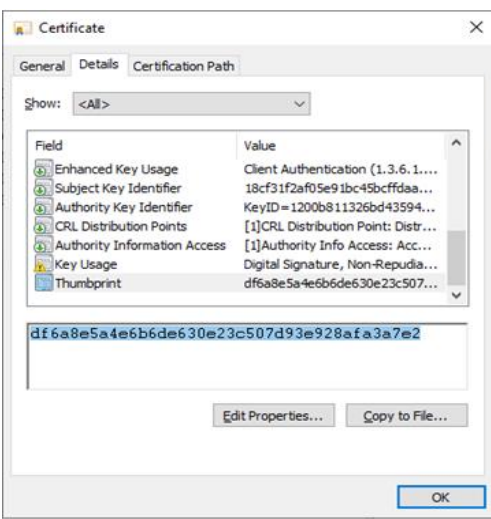
3. Test Webservice & View WSDL

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

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

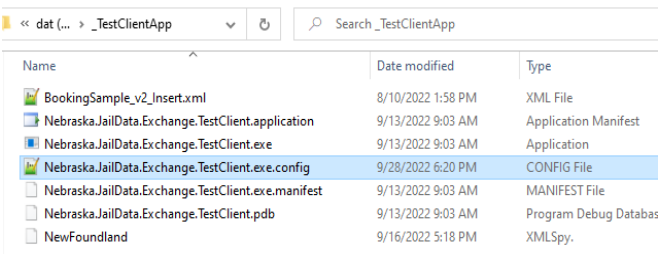
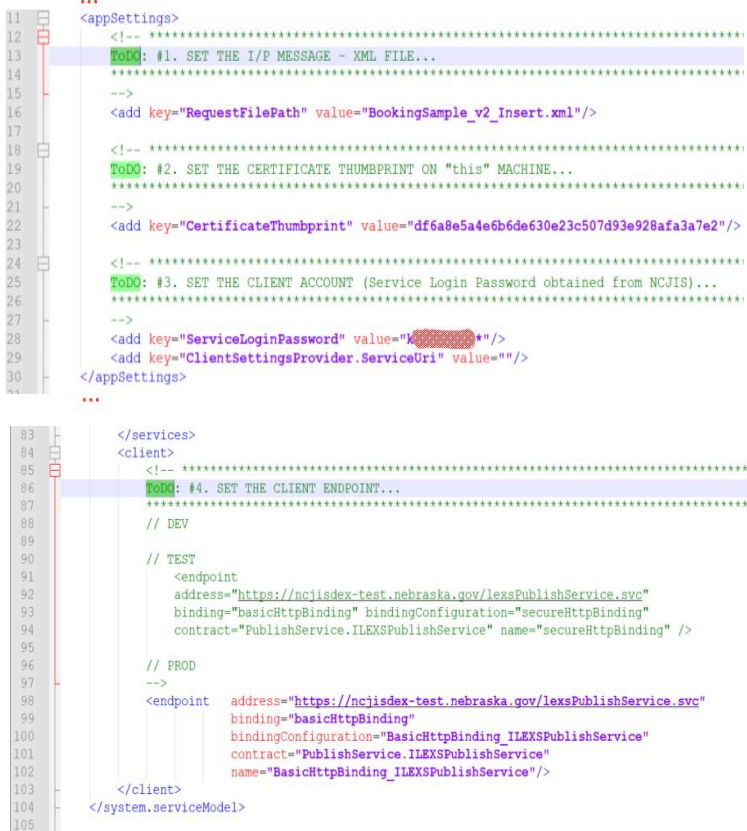
4. Obtain the Client Certificate Thumbprint

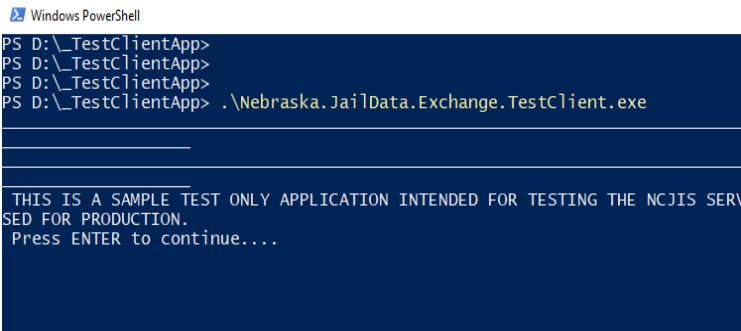
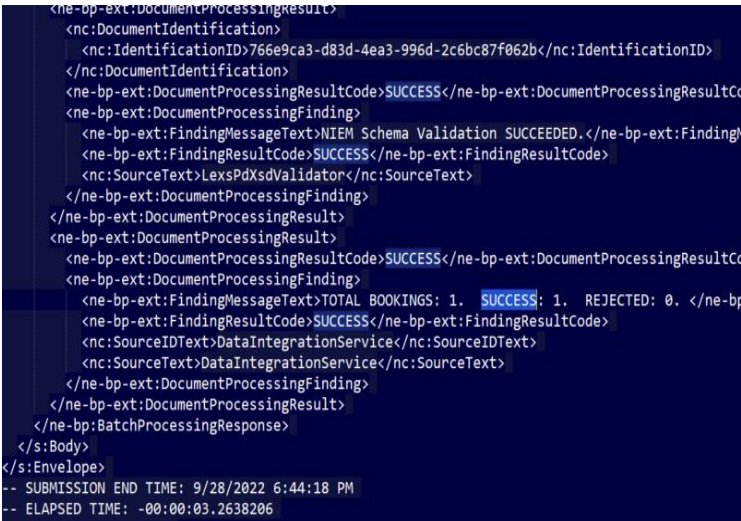
We need the Client Certificate Thumbprint to be submitted in the SOAP Message Header section to for authentication at the service endpoint. To get the thumbprint:

1	<p>Double Click the certificate in MMC</p> <p>That will open the certificate properties window</p>	
2	<p>Click the Details tab</p> <p>All the way at the bottom, locate the certificate thumbprint.</p> <p>From the bottom pane, copy the thumbprint.</p> <p>Click OK to close</p>	
3	<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 <appSettings> 12 <!-- ***** 13 ToDo: #1. SET THE I/P MESSAGE - XML FILE... 14 ***** 15 --> 16 <add key="RequestFilePath" value="BookingSample_v2_Insert.xml"/> 17 18 <!-- ***** 19 ToDo: #2. SET THE CERTIFICATE THUMBPRINT ON "this" MACHINE... 20 ***** 21 --> 22 <add key="CertificateThumbprint" value="df6a8e5a4e6b6de630e23c507d93e928afa3a7e2"/> 23 24 <!-- ***** 25 ToDo: #3. SET THE CLIENT ACCOUNT (Service Login Password obtained from NCJIS)... 26 ***** 27 --> 28 <add key="ServiceLoginPassword" value="k*****"/> 29 <add key="ClientSettingsProvider.ServiceUri" value="" /> 30 </appSettings> ... </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:

1	<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>	
2	<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"> 1. XML file name to be submitted 2. Certificate Thumbprint (from the above section) 3. “Service Login Password” related to the “Service Login Account” within the certificate. 4. Service Ednpoint <p>replace the values as needed.</p>	
3	<p>NOTE: Testing on TEST endpoint https://ncjisdex-test.nebraska.gov/lexsPublishService.svc 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>	

4	<p>RUN the ...TestClient.exe</p> <p>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]</p>	
5	<p>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).</p> <p>After processing a Response shall be returned showing the result of the request. A summary at the end of the message will indicate:</p> <p>Total Booking received</p> <p>SUCCESS Booking(s) processed</p> <p>and Rejected Booking(s)</p>	
6	<p>Here is a sample of the SOAP Header showing where the Service Login Password is located in the SOAP Message Header.</p>	<pre> <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"> <soap:Header> ... <AuthPassword soap:actor="http://nebraska.gov/JailDataExchange/lexs/LEXSPublishService/1.0/ILEXSPublishService/DoPublishRequest" xmlns="https://www.ncjis.com"> "[Service Login Password]" </AuthPassword> ... </soap:Header> <soap:Body> ... message stream ... </soap:Body> </soap:Envelope> </pre>

End of document.