



Nebraska Crime Commission

Jail Data Integration, Phase-2

Web Service Quick Setup Guide, v1.2

09-01-2026

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

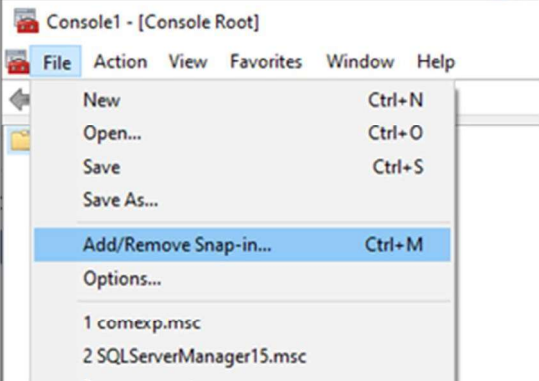
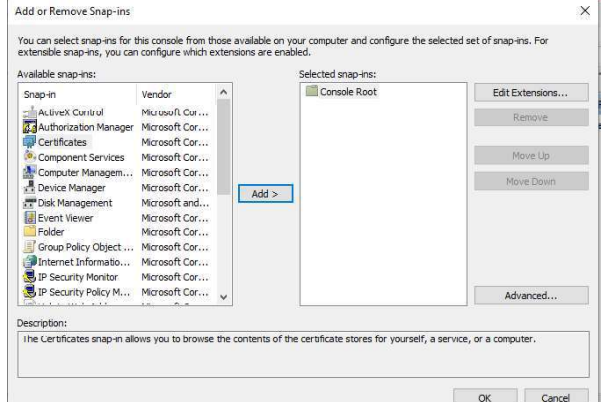
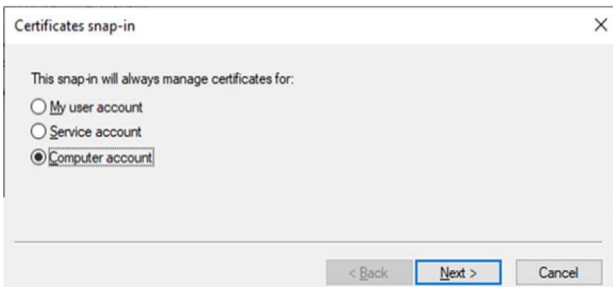
There are two passwords mentioned in this document, one is used to setup the certificate while the other is to connect/login to the webservice:

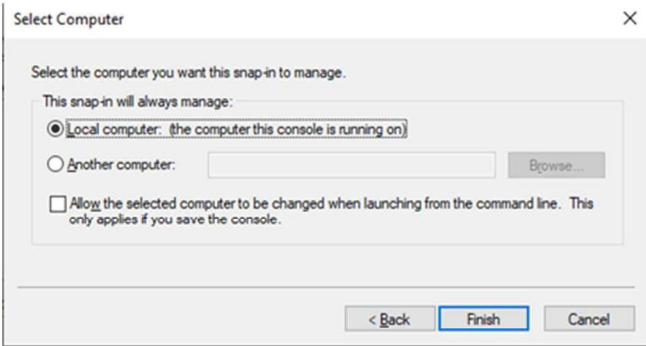
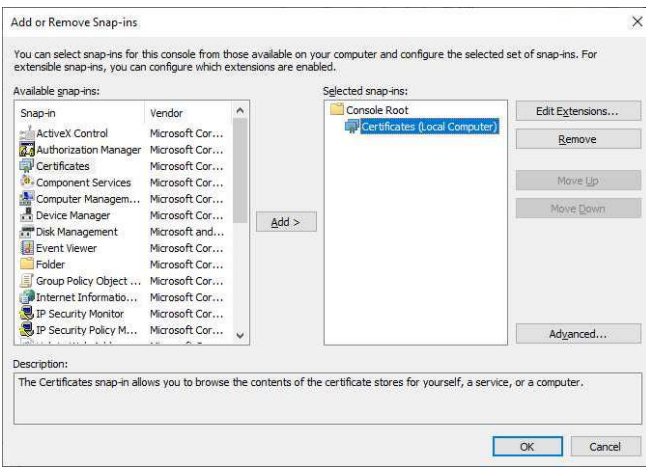
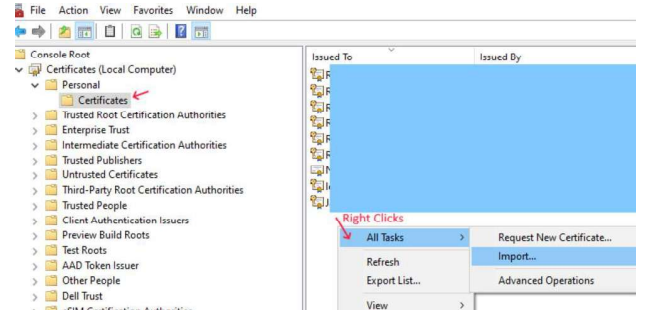
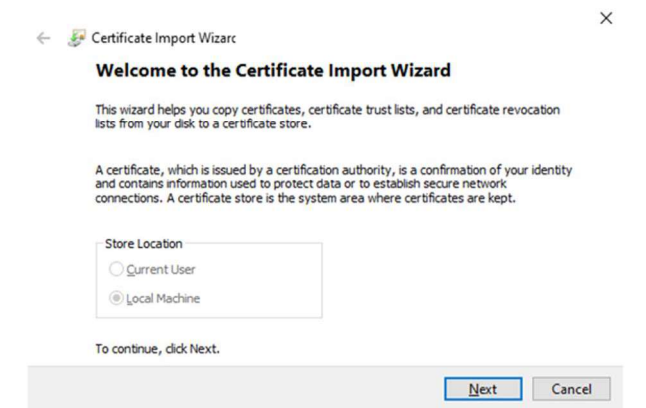
#	Description	Example
1	The Client Certificate file (pfx) requires a Password to import/install it.	<i>*aic</i>
3	The service endpoint credentials. Required “ Service Login Password ” related to the “ Service Login Account ” within the certificate	<i>ending with *</i>

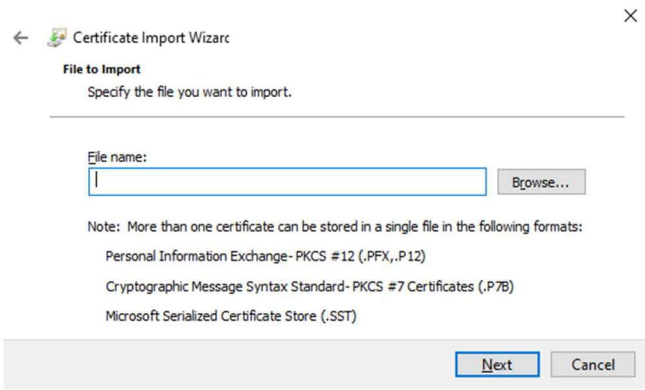
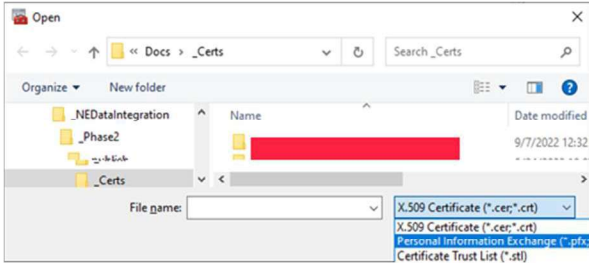
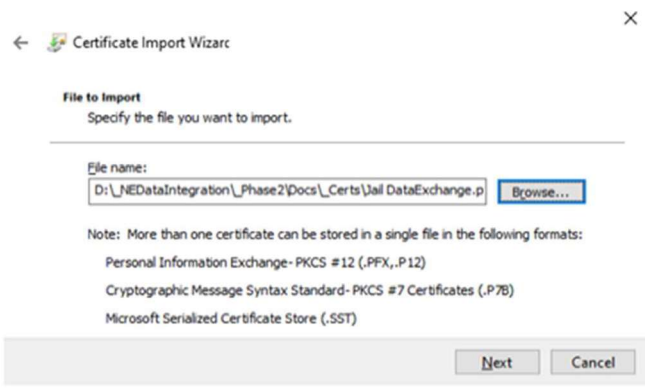
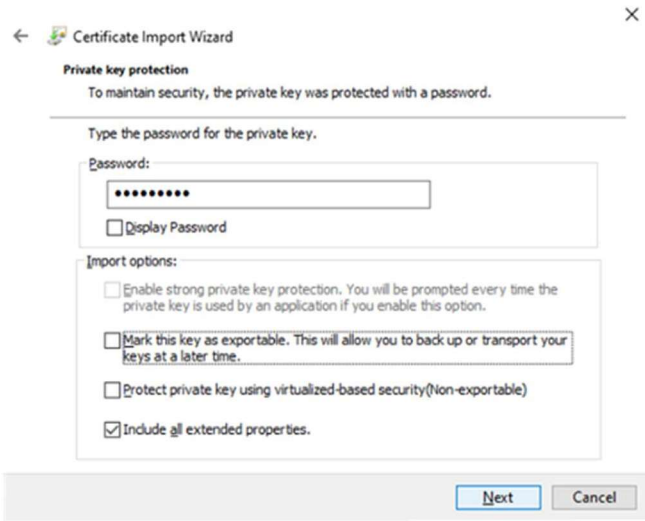
The same credentials can be used for both, TEST URI and Production URI after successful TEST.

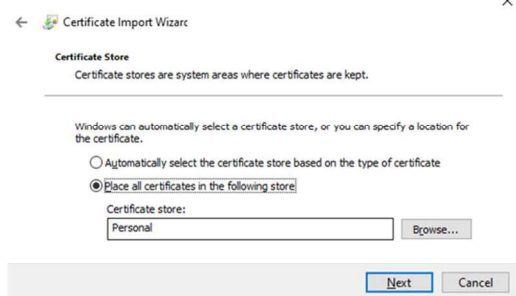
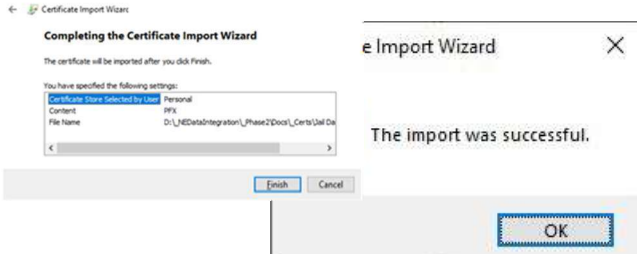
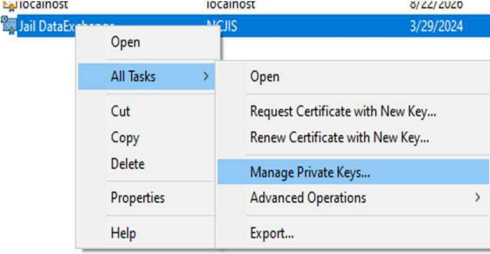
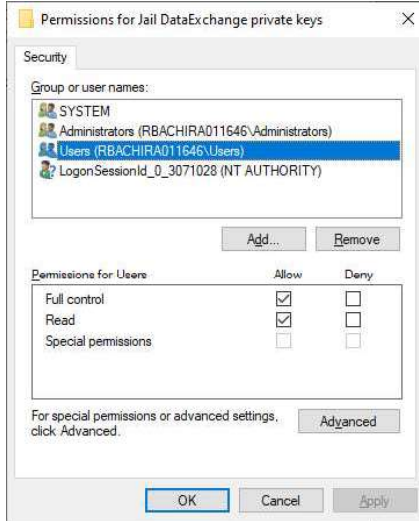
2. Client Certificate Setup

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"	

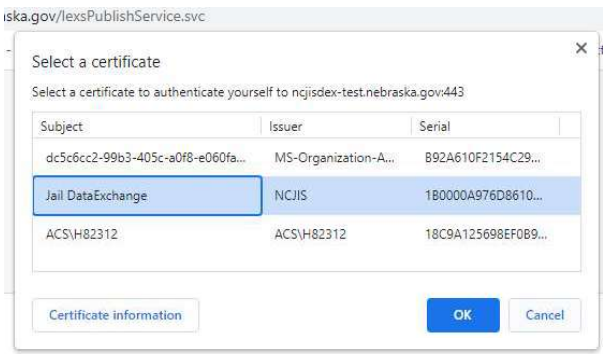
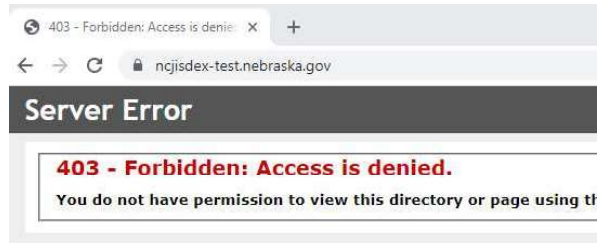
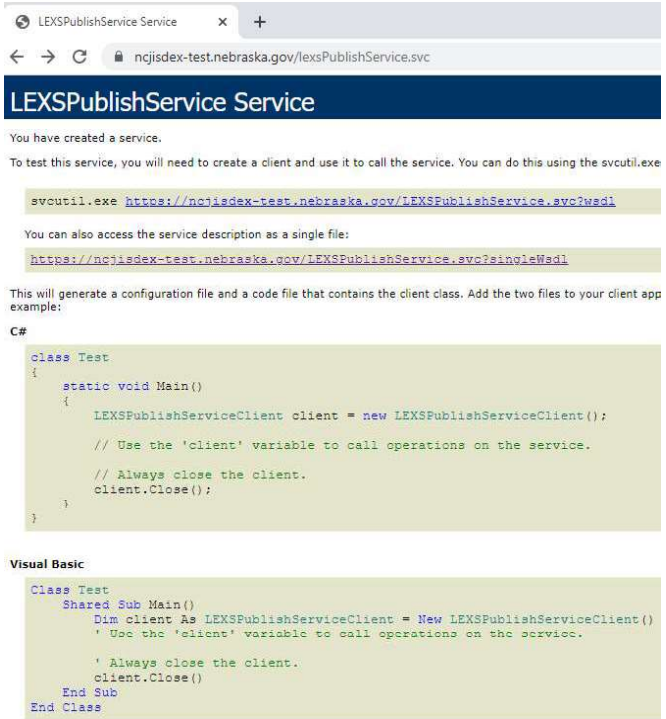
5	Click Finish Keeping Local Computer selected	 The 'Select Computer' dialog box is shown. It has a title bar 'Select Computer' and a close button. The main text says 'Select the computer you want this snap-in to manage.' Below this, it says 'This snap-in will always manage:' followed by two radio buttons. The first radio button is selected and labeled 'Local computer: (the computer this console is running on)'. The second radio button is labeled 'Another computer:' and has a text box and a 'Browse...' button next to it. Below these is a checkbox labeled 'Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.' At the bottom are three buttons: '< Back', 'Finish' (highlighted with a blue border), and 'Cancel'.
6	Click OK	 The 'Add or Remove Snap-ins' dialog box is shown. It has a title bar 'Add or Remove Snap-ins' and a close button. The main text says '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.' Below this are two panes. The left pane is titled 'Available snap-ins:' and contains a list of snap-ins with their vendors. The right pane is titled 'Selected snap-ins:' and contains a list of selected snap-ins. Below the panes is an 'Add >' button. At the bottom is a 'Description:' box with text about the Certificates snap-in. At the bottom right are 'OK' and 'Cancel' buttons.
7	On the left pane Expand Personal->Certificates On the Right pane: - Right Click and select All Tasks Import	 A screenshot of the Windows Management Console (MMC) showing the 'Certificates (Local Computer)' console. The left pane shows the tree structure with 'Personal' expanded and 'Certificates' selected. The right pane shows a list of certificates. A right-click context menu is open over the list, with 'All Tasks' selected, and a sub-menu is open showing 'Import...' highlighted.
8	Local Machine is selected by default, Click NEXT	 The 'Certificate Import Wizard' dialog box is shown. It has a title bar 'Certificate Import Wizard' and a close button. The main text says 'Welcome to the Certificate Import Wizard' and 'This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.' Below this is a section titled 'Store Location' with two radio buttons: 'Current User' and 'Local Machine' (selected). At the bottom is a 'To continue, click Next.' text and 'Next' and 'Cancel' buttons.

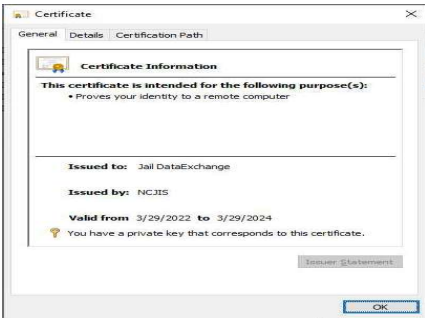
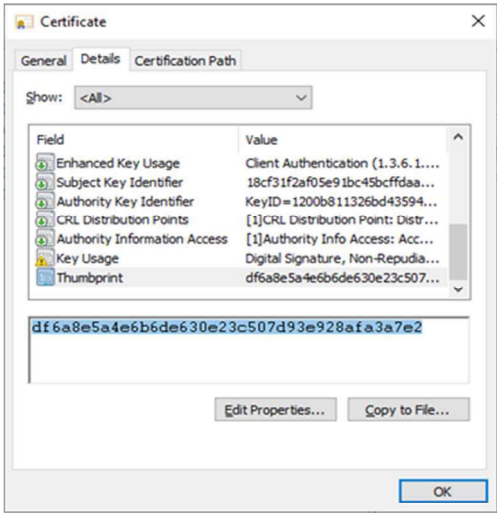
9	Click Browse and locate and select the PFX file	 The screenshot shows the 'Certificate Import Wizard' window, 'File to Import' step. It prompts the user to specify the file to import. There is a 'File name:' text box and a 'Browse...' button. Below, it lists supported formats: Personal Information Exchange - PKCS #12 (.PFX, .P12), Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B), and Microsoft Serialized Certificate Store (.SST). 'Next' and 'Cancel' buttons are at the bottom right.
10	Make sure to select .pfx from the file type combo box.	 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' selected. 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;*.p7b)', and 'Certificate Trust List (*.stl)'.
11	The pfx certificate file is selected, click [Next]	 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 highlighted. The rest of the window is the same as in step 9.
12	Enter the certificate installation [Password] keeping default options Click [Next]	 The screenshot shows the 'Certificate Import Wizard' window, 'Private key protection' step. It prompts the user to enter a password for the private key. There is a 'Password:' text box with a masked password. Below it, there is a checkbox for 'Display Password'. Under 'Import options:', there are four checkboxes: 'Enable strong private key protection...', 'Mark this key as exportable...', 'Protect private key using virtualized-based security(Non-exportable)', and 'Include all extended properties.' which is checked. 'Next' and 'Cancel' buttons are at the bottom right.

13	Keep Place certificate in Personal store. Click [Next]	 The screenshot shows the 'Certificate Store' window 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). Under the selected option, 'Personal' is entered in the 'Certificate store:' field. 'Next' and 'Cancel' buttons are at the bottom.												
14	Click [Finish] “The import was successful” click [OK]	 The screenshot shows the 'Completing the Certificate Import Wizard' window. It states 'The certificate will be imported after you click Finish.' It lists the specified settings: 'Certificate Store: Personal', 'Container: PFX', and 'File Name: D:_JailDataIntegration_Phase2\Docs\Certs\Jail Data Exchange.pfx'. 'Finish' and 'Cancel' buttons are at the bottom. A separate 'The import was successful.' dialog box with an 'OK' button is also shown.												
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	 The screenshot shows a right-click context menu for a file named 'Jail DataExchange.pfx'. The menu options include 'Open', 'All Tasks', 'Cut', 'Copy', 'Delete', 'Properties', and 'Help'. The 'All Tasks' submenu is open, showing options like 'Open', 'Request Certificate with New Key...', 'Renew Certificate with New Key...', 'Manage Private Keys...' (highlighted), 'Advanced Operations', and 'Export...'.												
17	Add “Users” account and click OK	 The screenshot shows the 'Permissions for Jail DataExchange private keys' dialog box. In the 'Group or user names:' list, 'Users (RBACHIRA011646\Users)' is selected. Below, the 'Permissions for Users' table shows 'Full control' and 'Read' permissions checked under the 'Allow' column. 'Special permissions' is unchecked. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons. <table border="1" data-bbox="915 1478 1289 1604"> <thead> <tr> <th>Permissions for Users</th> <th>Allow</th> <th>Deny</th> </tr> </thead> <tbody> <tr> <td>Full control</td> <td>☒</td> <td>☐</td> </tr> <tr> <td>Read</td> <td>☒</td> <td>☐</td> </tr> <tr> <td>Special permissions</td> <td>☐</td> <td>☐</td> </tr> </tbody> </table>	Permissions for Users	Allow	Deny	Full control	☒	☐	Read	☒	☐	Special permissions	☐	☐
Permissions for Users	Allow	Deny												
Full control	☒	☐												
Read	☒	☐												
Special permissions	☐	☐												

3. Test Webservice & View WSDL

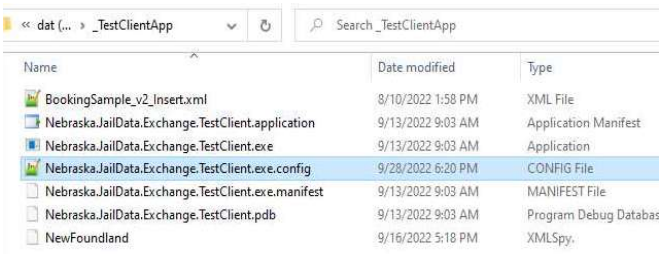
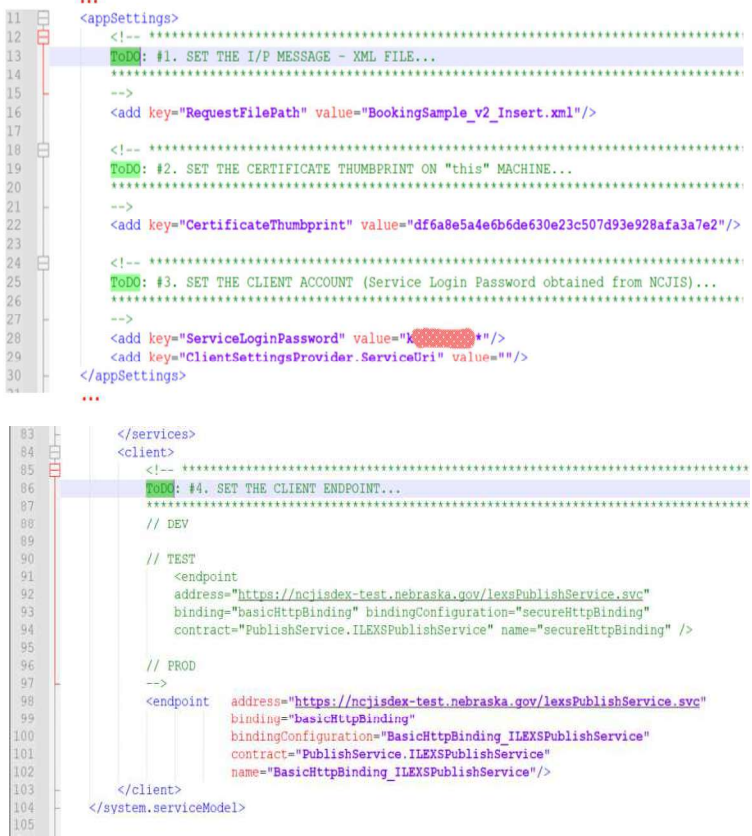
Test the webservice to validate the certificate and the setup is accurate:

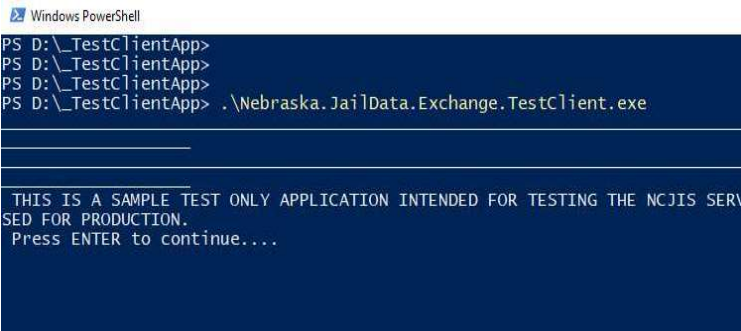
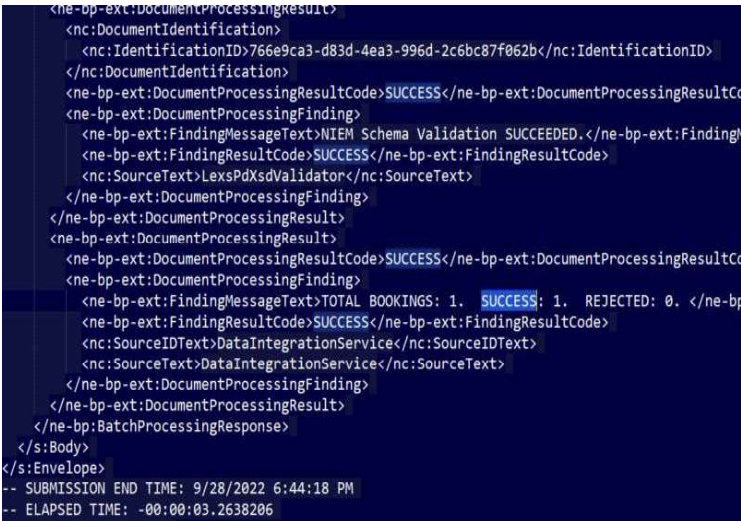
1	Go to: https://ncjisdex-test.nebraska.gov/lexspublishservice.svc You'll be prompted to select a certificate to use. Select the installed certificate.	
2	IF you get this image instead of the WSDL Then check the complete URL as show above.	
3	You should get this WSDL page if all the setup is accurate.	

1	Double Click the certificate in MMC That will open the certificate properties window	 The screenshot shows the 'Certificate' window with the 'General' tab selected. It displays 'Certificate Information' stating the purpose is to prove identity to a remote computer. It is issued to 'Jail DataExchange' by 'NCJIS' and is valid from 3/29/2022 to 3/29/2024. A note mentions a private key corresponding to the certificate.
2	Click the Details tab All the way at the bottom, locate the certificate thumbprint. From the bottom pane, copy the thumbprint. Click OK to close	 The screenshot shows the 'Certificate' window with the 'Details' tab selected. It lists various fields like Enhanced Key Usage, Subject Key Identifier, etc. At the bottom, the 'Thumbprint' is listed as 'df6a8e5a4e6b6de630e23c507d93e928afa3a7e2'. The 'Show:' dropdown is set to '<All>'. Buttons for 'Edit Properties...', 'Copy to File...', and 'OK' are visible.
3	The Thumbprint is to be used on the Test Client App .config file as shown on right (detail in the next section).	 The screenshot shows an XML configuration file snippet. The 'CertificateThumbprint' attribute is set to the value 'df6a8e5a4e6b6de630e23c507d93e928afa3a7e2'.

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	Go to the “TestClientApp” folder where you unzipped it to. Let’s assume “TestClientApp”. First, edit the .config file as follows	
2	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: 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 replace the values as needed.	
3	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.	

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

End of document.