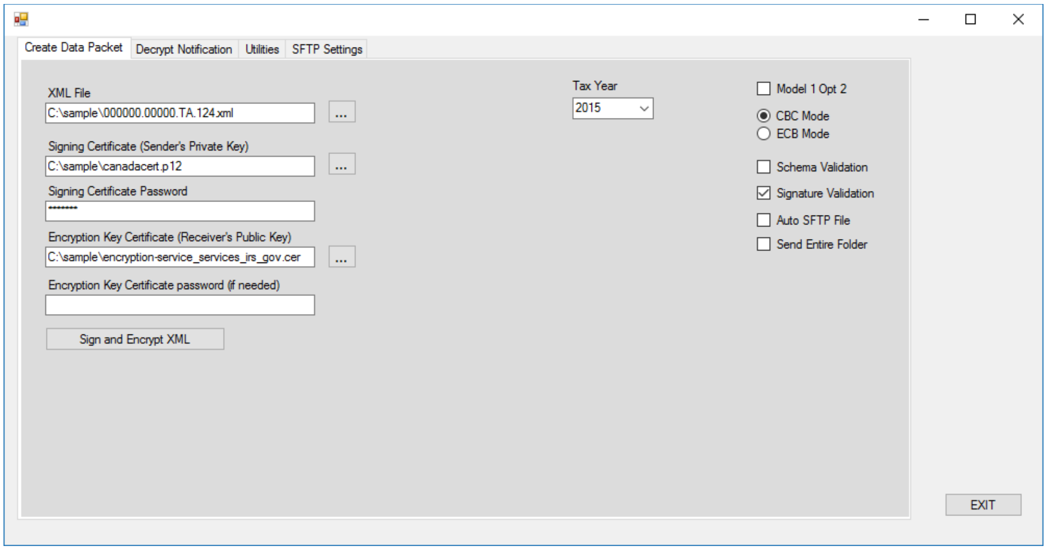
1. Validating the digital signature while creating a data packet.
   a. On the Create Data Packet tab, select the Signature Validation checkbox. This controls whether the newly created digital signature is validated or not.



XML File: C:\sample\000000.00000.TA.124.xml

Signing Certificate (Sender's Private Key): C:\sample\canadacert.p12

Signing Certificate Password: ********

Encryption Key Certificate (Receiver's Public Key): C:\sample\encryption-service_services_irs_gov.cer

Encryption Key Certificate password (if needed):

Tax Year: 2015

□ Model 1 Opt 2

● CBC Mode

○ ECB Mode

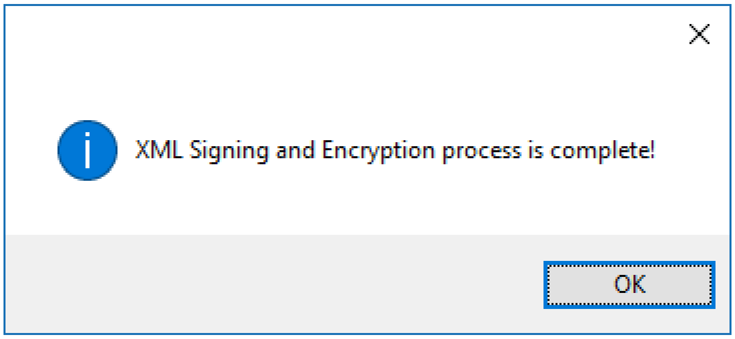
□ Schema Validation

☑ Signature Validation

□ Auto SFTP File

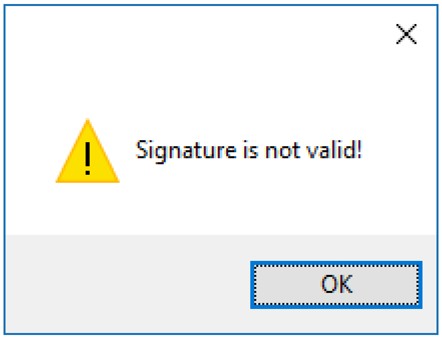
□ Send Entire Folder

   b. Enter the needed fields and click the Sign and Encrypt XML button.
   c. Successful validation and packet creation will produce a success message that the process is complete.



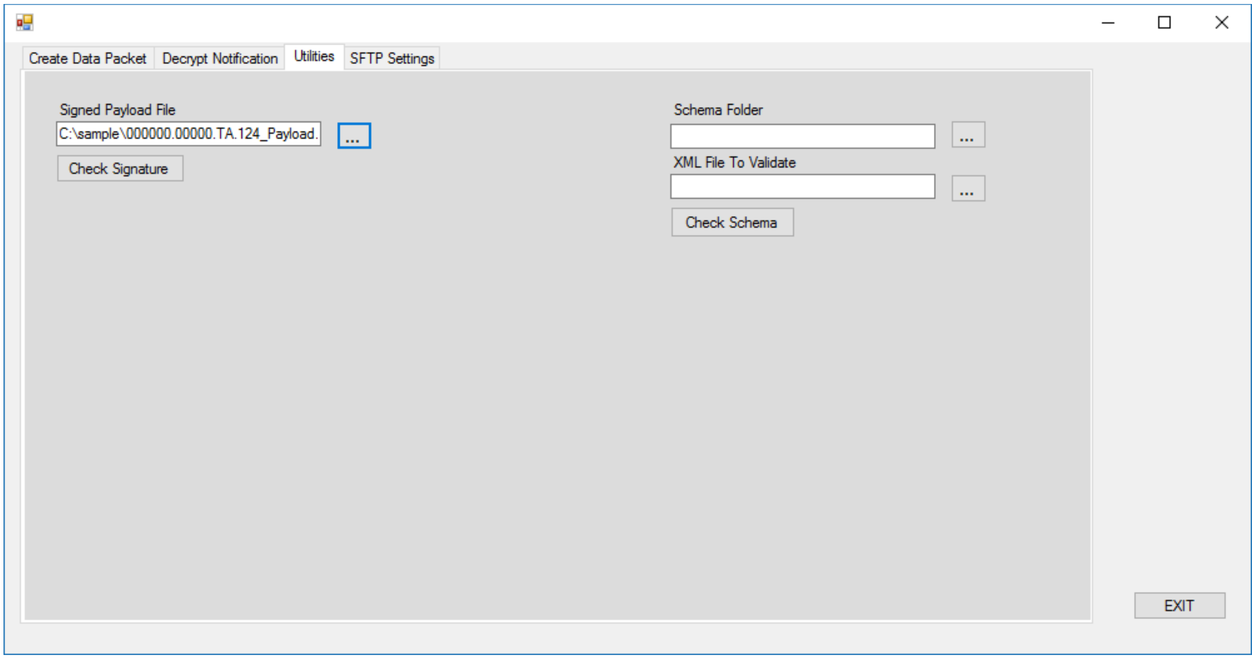
XML Signing and Encryption process is complete!

   d. A validation error will produce a failure message and the data packet will not be created.



Signature is not valid!

2. Validating the digital signature while not creating a data packet.
   a. Select the Utilities tab. Select the Signed Payload File.



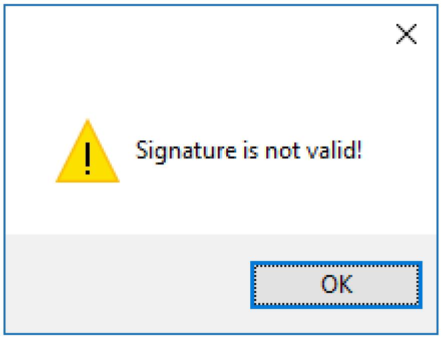
Signed Payload File: C:\sample\000000.00000.TA.124_Payload.

Schema Folder:

XML File To Validate:

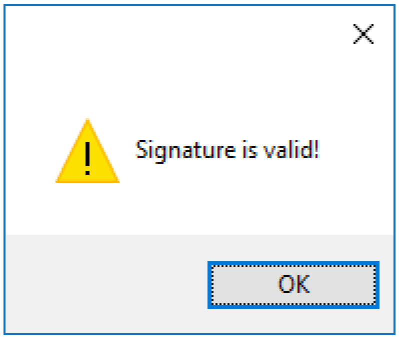
b. Click the Check Signature button. This will validate the digital signature on the selected XML file.

c. A validation failure will present a failure message.



Signature is not valid!

d. If the digital signature is valid, a success message will be presented.



Signature is valid!