DIVISION OF TAXATION

ENCRYPTION PROCEDURES FOR W-2 AND Form 1099 DATASETS

The Employer:

Enclosed are the Central Collection Agency (CCA)'s encryption procedures for W-2 and Form 1099 datasets in tax year 2020. This document is aimed at employers or their agents, e.g., accountants and payroll services, that may have organizational policies which require sensitive taxpayer information be transmitted in a secure manner. The CCA encryption procedures for W-2 and Form 1099 datasets allow employers or their agents to securely encrypt their W-2 and Form 1099 datasets before sending them to CCA for processing.

Please read these procedures carefully. Employers who are required to electronically file W-2 and Form 1099 datasets may be subject to monetary penalties for failure to comply with these procedures. Employers submitting encrypted W-2 or Form 1099 datasets to CCA that are not encrypted using these procedures **will have their submittal rejected**.

CCA is using a common Public Key Infrastructure (PKI) called GNU Privacy Guard to securely encrypt the W-2 and Form 1099 datasets. The GNU Privacy Guard software is available for multiple operating systems, e.g., Linux, OS X and Windows and can be downloaded at:

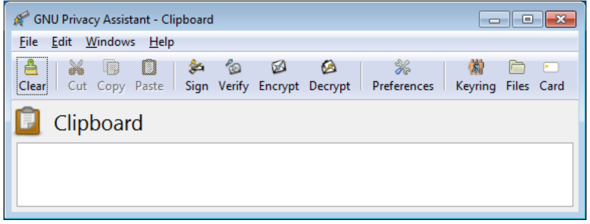
https://gnupg.org/download/#binary

Once you download and install the software, you will be asked to create a personal key (save the passphrase you use), then you will need to import CCA's public key from the public key server into your key store, see below. You will need the following information to import CCA's public key from the key server. However, **before importing** CCA's public key, insure that the **fingerprint matches** the following information:

Public Key ID:	BC48 1999 5CCA 05A5
Public Key Name:	CCA Data Format TY2020
Public Key Comment:	Andrew Houghton, Information Systems Department
Public Key Email:	ahoughton@city.cleveland.oh.us
Public Key Valid From:	11/2/2020
Public Key Valid Until:	12/31/2021
Public Key Fingerprint:	711F 8796 9C7C A046 F527 6BAB BC48 1999 5CCA 05A5

The following steps assume you have installed GNU Privacy Guard and created your personal key on **Windows**; instructions for OS X and Linux may be similar, but for those operating systems you will have to read their GNU Privacy Guard manual and use the following steps as a guide. Note in the following guide the terms key and certificate are used interchangeable.

1. Open the GPA (GNU Privacy Assistant) application.

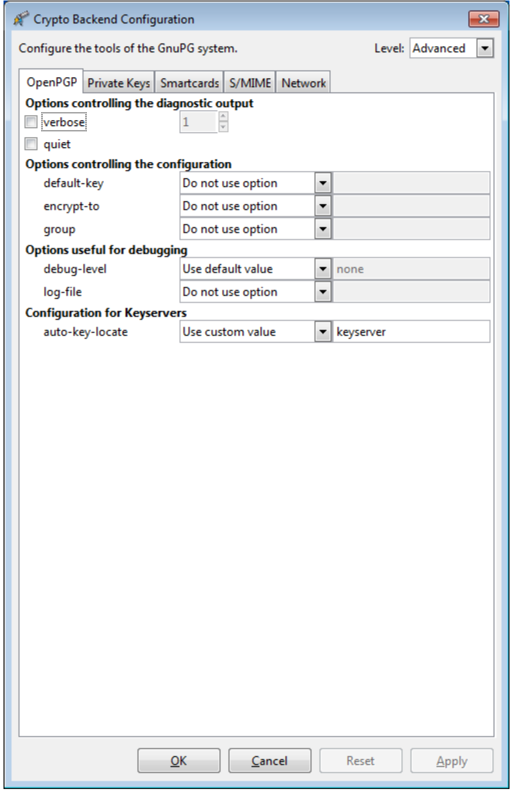


2. Select the Edit -> Backend Preferences menu choice and it will bring up the Crypto Backend Configuration dialog box.

   a. Select the Advanced choice in the Level drop down box, upper right.

   b. Select the OpenPGP tab.

   c. Select Use custom value for the auto-key-locate item under the Configuration for Keyservers section and enter keyserver for the value.



Configure the tools of the GnuPG system.

Level: Advanced

Options controlling the diagnostic output

□ verbose 1

□ quiet

Options controlling the configuration

default-key: Do not use option

encrypt-to: Do not use option

group: Do not use option

Options useful for debugging

debug-level: Use default value none

log-file: Do not use option

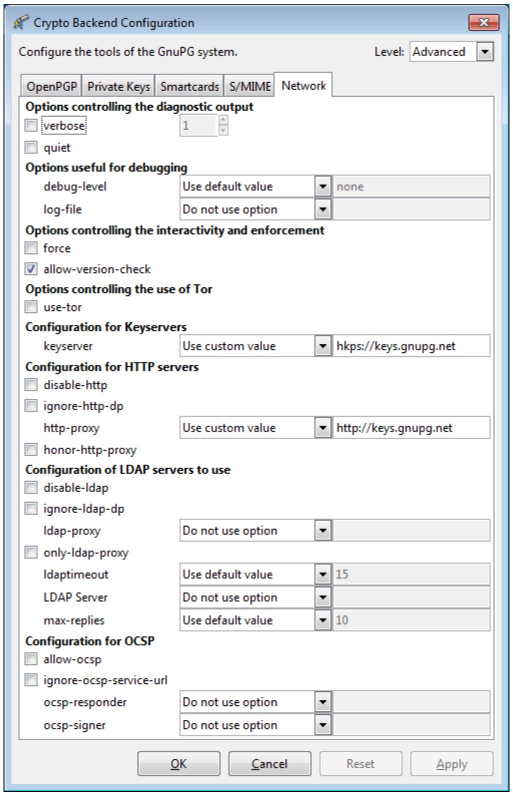
Configuration for Keyservers

auto-key-locate: Use custom value keyserver

   d. Select the Network tab.

   e. Select Use custom value for the keyserver item under the Configuration for Keyservers section and use the value hkps://keys.gnupg.net, note that the value start with hkps: not https:.

   f. Select Use custom value for the http-proxy item under the Configuration for HTTP servers and use the value http://keys.gnupg.net



Crypto Backend Configuration

Configure the tools of the GnuPG system. Level: Advanced

Options controlling the diagnostic output

☐ verbose 1

☐ quiet

Options useful for debugging

debug-level: Use default value — none

log-file: Do not use option

Options controlling the interactivity and enforcement

☐ force

☑ allow-version-check

Options controlling the use of Tor

☐ use-tor

Configuration for Keyservers

keyserver: Use custom value — hkps://keys.gnupg.net

Configuration for HTTP servers

☐ disable-http

☐ ignore-http-dp

http-proxy: Use custom value — http://keys.gnupg.net

☐ honor-http-proxy

Configuration of LDAP servers to use

☐ disable-ldap

☐ ignore-ldap-dp

ldap-proxy: Do not use option

☐ only-ldap-proxy

ldaptimeout: Use default value — 15

LDAP Server: Do not use option

max-replies: Use default value — 10

Configuration for OCSP

☐ allow-ocsp

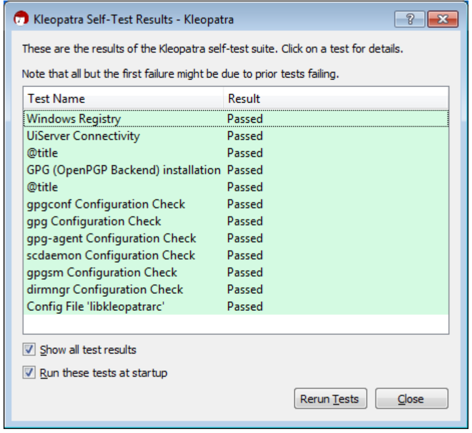
☐ ignore-ocsp-service-url

ocsp-responder: Do not use option

ocsp-signer: Do not use option

3. Open the Kleopatra application.

4. Select Settings -> Perform Self Test and it will run a self test and display the results in a dialog box. All tests should pass.



Kleopatra Self-Test Results - Kleopatra

These are the results of the Kleopatra self-test suite. Click on a test for details.

Note that all but the first failure might be due to prior tests failing.

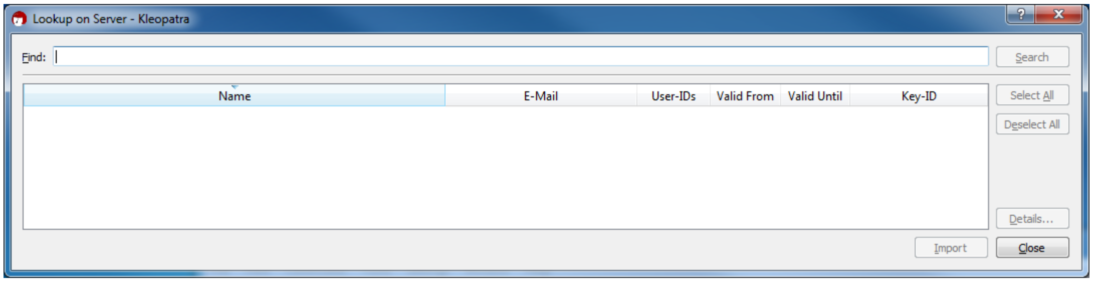
Test Name	Result
Windows Registry	Passed
UiServer Connectivity	Passed
@title	Passed
GPG (OpenPGP Backend) installation	Passed
@title	Passed
gpgconf Configuration Check	Passed
gpg Configuration Check	Passed
gpg-agent Configuration Check	Passed
scdaemon Configuration Check	Passed
gpgsm Configuration Check	Passed
dirmngr Configuration Check	Passed
Config File 'libkleopatrarc'	Passed

☑ Show all test results

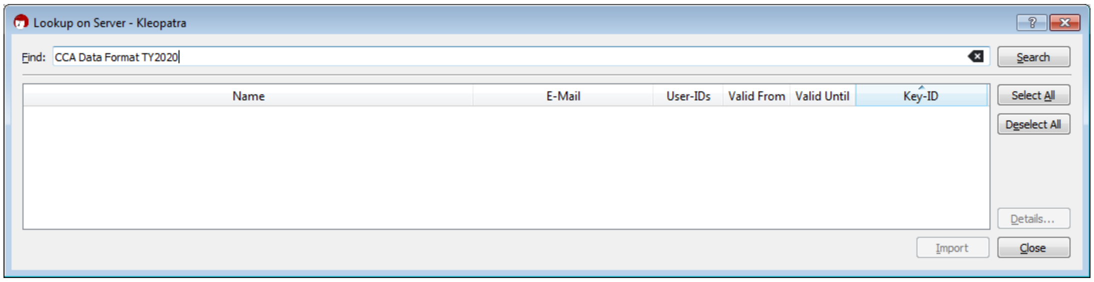
☑ Run these tests at startup

5. Click the Close button.

6. Click on the “Lookup on Server…” toolbar button or select the File->Lookup on Server… menu item or the press the Ctrl-Shift-I keys to open the Lookup on Server dialog box.

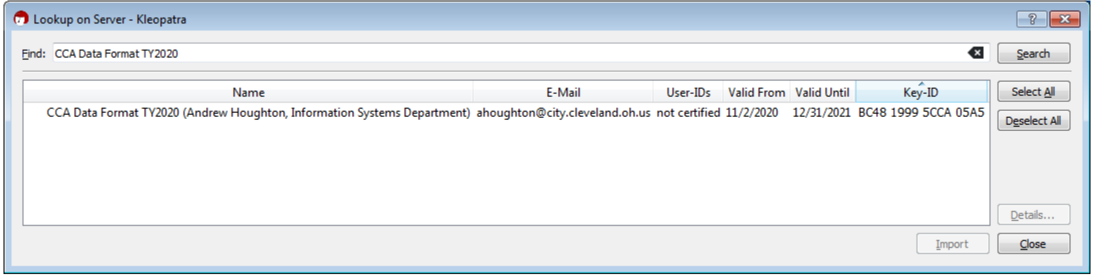


7. Enter CCA's public key name, see above, into the Find text box on the Lookup on Server dialog box.



Find: CCA Data Format TY2020

8. Click the Search button on the Lookup on Server dialog box. It may take a few seconds for the Kleopatra application to retrieve the key from the key server, be patient. You should see the following entry appear in the results text box of the Lookup on Server dialog box. If you do not retrieve the key, the key server might be experiencing a high request volume. Wait 5 to 10 minutes and try again a few times. If you still fail try the alternate method (a) under this item.



Find: CCA Data Format TY2020

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
CCA Data Format TY2020 (Andrew Houghton, Information Systems Department)	ahoughton@city.cleveland.oh.us	not certified	11/2/2020	12/31/2021	BC48 1999 5CCA 05A5

a. These are alternate instruction when you weren't able to retrieve the key. You can use your browser to select and copy the key, then save the copied text to a local file with the extension .asc, then import the saved key file in Kleopatra.

   1. Click the Close button on the Lookup on Server dialog box.

   2. In your browser go to http://keys.gnupg.net/

   3. Enter CCA's public key name, see above, into the Search text box.

   4. Click the Search Key button.

   5. Verify the our public key information, given above, with the information found on the Search Results Web page:

      1. Verify that the key name is the same as found on the Search Results Web page. Note, ignore what is in parenthesis after the key name in the User ID

    column.

    2. Verify that the comment is the same as found on the Search Results Web page. The comment is what appears in parenthesis after the key name in the User ID column.

    3. Verify that the email address is the same as found on the Search Results Web page enclosed in angle brackets, e.g., < >, in the User ID column.

    4. Verify that the valid from date is the same as found on the Search Results Web page in the Date column.

    5. Verify that the fingerprint is the same as found on the Search Results Web page after the Fingerprint= text. This is the most important step in the verification of the certificate information. Check the fingerprint, then check it again to be sure before importing this or any other certificate.

6. Click on the link in the bits/keyed column which will show the PGP PUBLIC KEY BLOCK.

7. Select and copy all the text between and including the
   ```
   -----BEGIN PGP PUBLIC KEY BLOCK-----
   ```
   and the
   ```
   -----END PGP PUBLIC KEY BLOCK-----
   ```

8. Open Windows Notepad.

9. Paste the text into Windows Notepad.

10. Save the text to a file with the extension .asc, but make sure you set the Save as type drop down box to All files (*.*), otherwise your file will be named file.asc.txt instead of file.asc.

11. Close Windows Notepad.

12. In Kleopatra click the Import... toolbar button which will bring up the Select Certificate File dialog box.

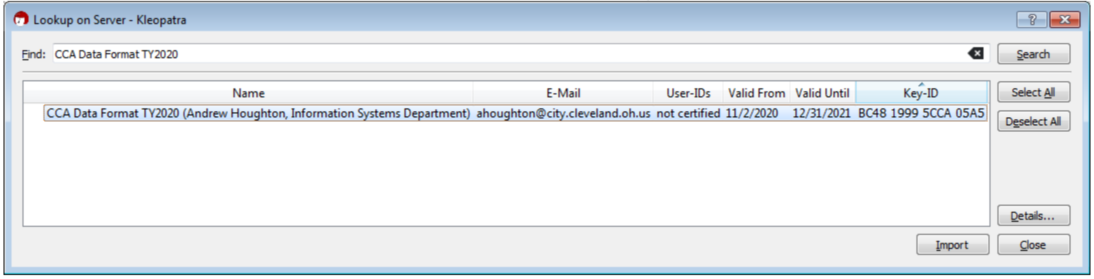
13. Navigate to the file you saved with Windows Notepad in the Select Certificate File dialog box.

14. Click the Open button on the Select Certificate File dialog box which will bring up the Certificate Import Result dialog box.

15. Click the OK button on the Certificate Import Result dialog box.

16. The CCA public key is now imported. Go to step 16, below.

9. Click on the public key that was found, which will highlight the key, and activate the Details… and Import buttons on the Lookup on Server dialog box.

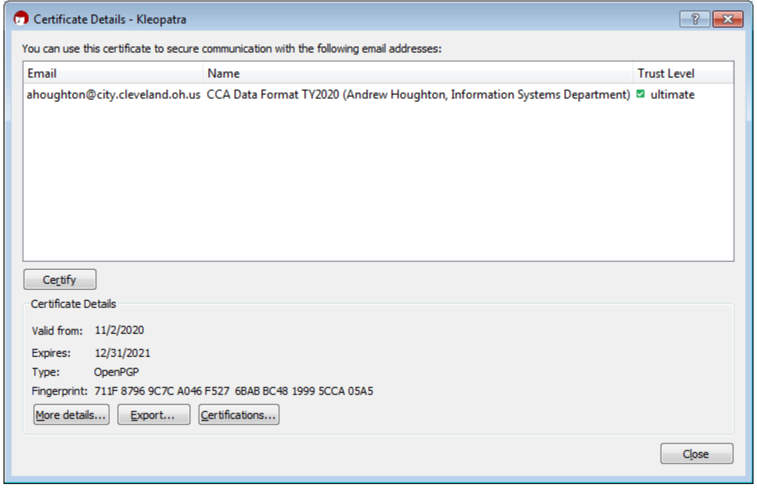


Lookup on Server - Kleopatra

Find: CCA Data Format TY2020

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
CCA Data Format TY2020 (Andrew Houghton, Information Systems Department)	ahoughton@city.cleveland.oh.us	not certified	11/2/2020	12/31/2021	BC48 1999 5CCA 05A5

10. Click on the Details… button on the Lookup on Server dialog box which will open the Certificate Details dialog box.



Certificate Details - Kleopatra

You can use this certificate to secure communication with the following email addresses:

Email	Name	Trust Level
ahoughton@city.cleveland.oh.us	CCA Data Format TY2020 (Andrew Houghton, Information Systems Department)	✓ ultimate

Certificate Details

Valid from: 11/2/2020

Expires: 12/31/2021

Type: OpenPGP

Fingerprint: 711F 8796 9C7C A046 F527 6BAB BC48 1999 5CCA 05A5

11. Verify the our public key information, given above, with the information found on the Certificate Details dialog box:

    a. Verify that the name is the same as found on the Certificate Details dialog box. Note, ignore what is in parenthesis after the name in the Name column.

    b. Verify that the comment is the same as found on the Certificate Details dialog box. The comment is what appears in parenthesis after the name in the Name column.

    c. Verify that the email address is the same as found on the Certificate Details dialog box in the Email column.

    d. Verify that the valid from date is the same as found on the Certificate Details dialog box in the Valid from item of the Certificate Details section.

    e. Verify that the valid until date is the same as found on the Certificate Details dialog box in the Expires item of the Certificate Details section.

    f. Verify that the fingerprint is the same as found on the Certificate Details dialog box in the Fingerprint item of the Certificate Details section. This is the most important step in the verification of the certificate information. Check the fingerprint, then check it again to be sure before importing this or any other certificate.

12. When the certificate was not successfully verified:

    a. Click the Close button on the Certificate Details dialog box.

    b. Click the Close button on the Lookup on Server dialog box.

    c. Restart these procedures at step 2 until you are successful.

    d. After you have run through these procedures several times and you are still unsuccessful, then send an email to the contact person listed below in this document. In the email, describe what issues you are having, where possible provide screen shots so we can see what is happening along the way. Since we only have access to Windows based computers we will be of limited help with OS X or Linux issues.

13. When the certificate was successfully verified, click the Close button on the Certificate Details dialog box.

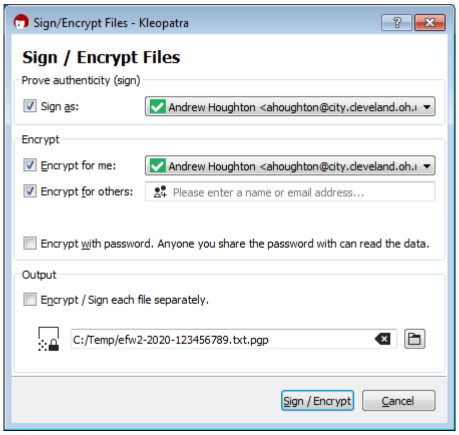
14. Click the Import button on the Lookup on Server dialog box which should automatically close the dialog box and it may take a minute or two, but the Certificate Import Results dialog box will be displayed showing the certificate was imported.

15. Click the OK button on the Certificate Import Result dialog box.

16. The Kleopatra application should now show the imported certificate and you can now encrypt your W-2 or Form 1099 dataset with CCA's public certificate.

17. In the Kleopatra application click the Sign/Encrypt… toolbar button or select the File->Sign/Encrypt… menu item to open the Select One or More Files to Sign and/or Encrypt dialog box.

18. Navigate in the Select One or More Files to Sign and/or Encrypt dialog box to the directory where the W-2 or Form 1099 dataset is located, then select the W-2 or Form 1099 dataset, then click the Open button which will open the Sign/Encrypt Files dialog box. Note, when naming your W-2 or Form 1099 dataset, only use alphabetic, numeric, dash or underscore characters, include the tax year and the EIN of the employer or agent that is making the submittal in the document name and use the .txt document extension, e.g., efw2-2020-123456789.txt



Prove authenticity (sign)

☑ Sign as: Andrew Houghton <ahoughton@city.cleveland.oh.ı

Encrypt

☑ Encrypt for me: Andrew Houghton <ahoughton@city.cleveland.oh.ı

☑ Encrypt for others: Please enter a name or email address…

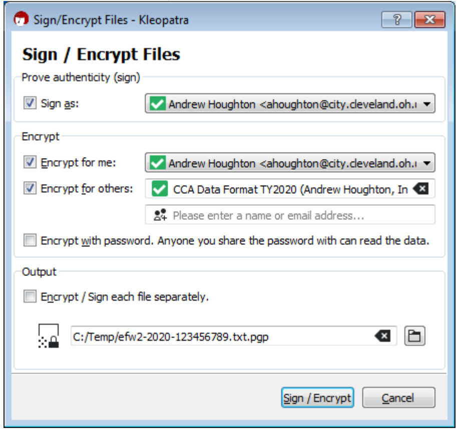
□ Encrypt with password. Anyone you share the password with can read the data.

Output

□ Encrypt / Sign each file separately.

C:/Temp/efw2-2020-123456789.txt.pgp

19. In the Encrypt section of the Sign/Encrypt Files dialog box, enter CCA Data Format TY2020 into the Encrypt for others text box and selected the certificate presented.



Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: Andrew Houghton <ahoughton@city.cleveland.oh.u

Encrypt

☑ Encrypt for me: Andrew Houghton <ahoughton@city.cleveland.oh.u

☑ Encrypt for others: CCA Data Format TY2020 (Andrew Houghton, In

Please enter a name or email address...

□ Encrypt with password. Anyone you share the password with can read the data.

Output

□ Encrypt / Sign each file separately.

C:/Temp/efw2-2020-123456789.txt.pgp

20. Click the Sign / Encrypt button of the Sign/Encrypt Files dialog box which will open the pinentry-qt dialog box and enter the passphrase for the key you initially created when you installed the GNU Privacy Guard software into the Passphrase text box of the pinentry-qt dialog box.

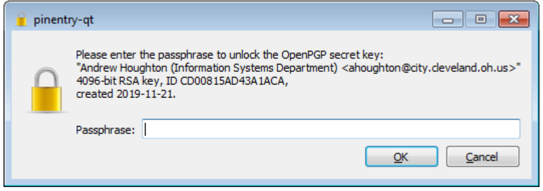
    a. This step is encrypting the W-2 or Form 1099 dataset so both you and CCA can decrypt the data.

    b. Entering the certificate you initially created, when you installed the GNU Privacy Guard software, in the Encrypt for me dropdown box, of the Encrypt section, on the Sign/Encrypt Files dialog box, allows you to decrypt the data.

    c. Entering the certificate CCA created, that you previously imported, in the Encrypt for others dropdown box, of the Encrypt section, on the Sign/Encrypt Files dialog box, allows CCA to decrypt the data.

    d. The text of the pinentry-qt dialog box will display information from the certificate you initially created when you installed the GNU Privacy Guard software. Which is why the GNU Privacy Guard software is asking for **<u>your secret key</u>**.

    e. The following dialog box shows CCA's certificate information, since this guide is using that certificate to sign and encrypt the sample dataset for the guide.

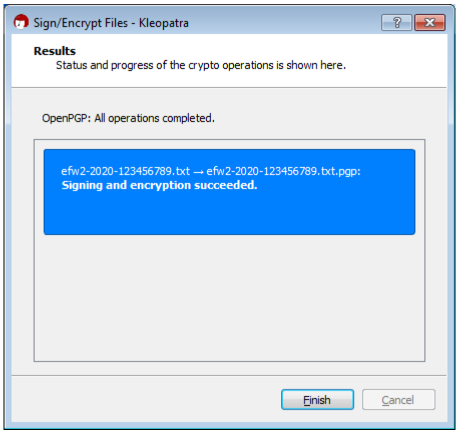


pinentry-qt

Please enter the passphrase to unlock the OpenPGP secret key:
"Andrew Houghton (Information Systems Department) <ahoughton@city.cleveland.oh.us>"
4096-bit RSA key, ID CD00815AD43A1ACA,
created 2019-11-21.

Passphrase:

21. Click the OK button on the pinentry-qt dialog box which will close and return you to the Sign/Encrypt Files dialog box showing that the signing and encryption was successful.



Sign/Encrypt Files - Kleopatra

Results

Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

efw2-2020-123456789.txt → efw2-2020-123456789.txt.pgp:
Signing and encryption succeeded.

22. Click the Finish button on the Sign/Encrypt Files dialog box which will return you to the Kleopatra application.

23. Close the Kleopatra application.

After you have encrypted your dataset fill out a Transmittal Form, then follow the Submittal Procedures for submitting your dataset to CCA. Correspondence about these procedures or this document can be sent to the following address or preferably by email to:

ANDREW HOUGHTON
INFORMATION SYSTEMS DEPARTMENT
CENTRAL COLLECTION AGENCY
205 W SAINT CLAIR AVE
CLEVELAND, OH 44113-1503

Email: ahoughton@city.cleveland.oh.us (preferred)
Phone: 1-216-664-7072 (EST)