The Arkansas All-Payer Claims Database (APCD) File Encryption Instructions

May 2019

ARKANSAS
APCD
All-Payer Claims Database

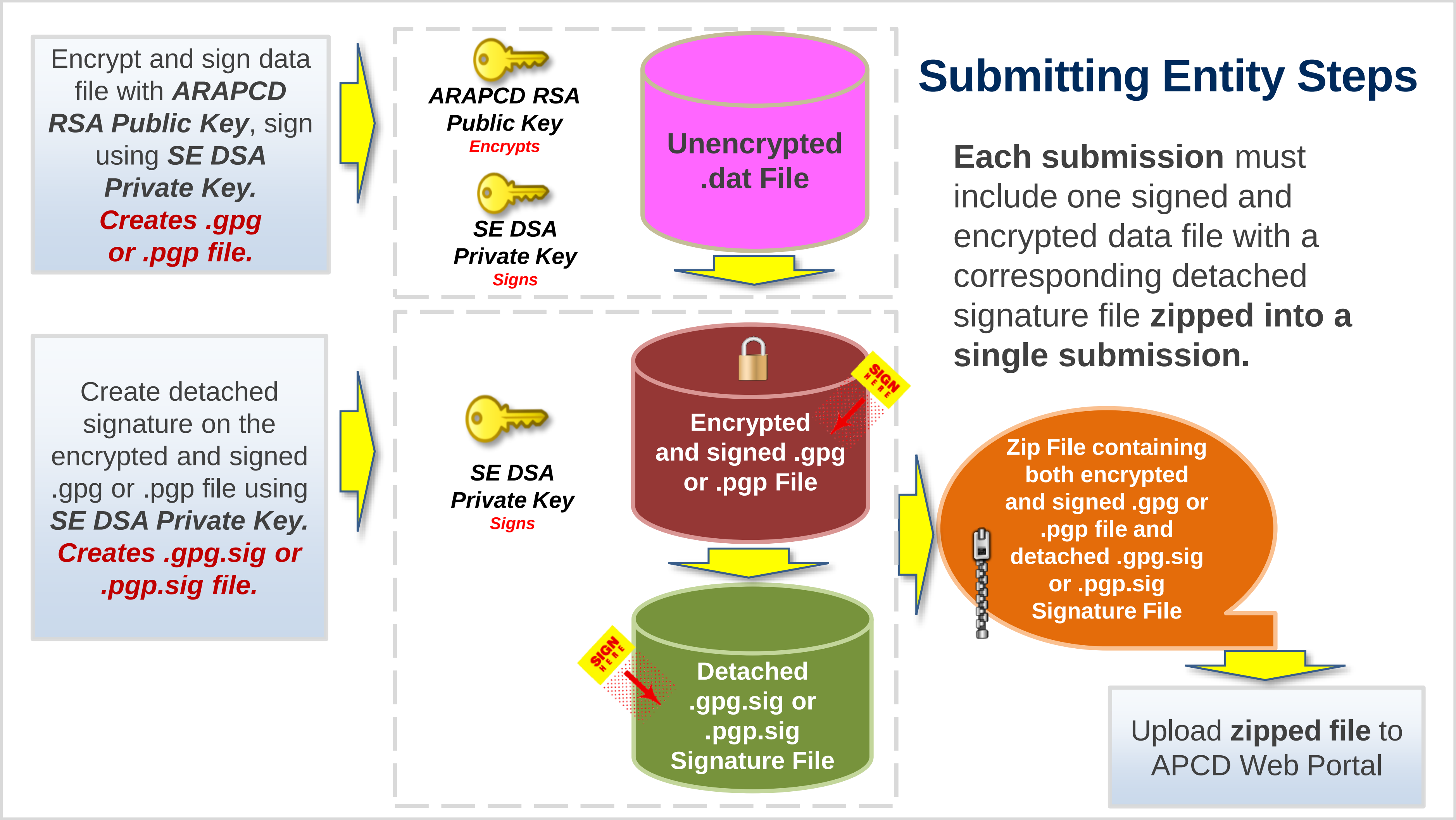
ADMINISTERED BY ACHI

Entity Encryption

Entity Checklist prior to submitting files:

- Receive and import ARAPCD Public key certificates
- Change Owner trust to ‘I believe checks are very accurate’
- Create SE Public and Private Keys using the naming conventions in this requirements document.
- Export SE Private RSA and DSA Keys for SE-only storage, recovery
- Export SE Public RSA and DSA Key certificates using the naming conventions in this requirements document and send to ARAPCD
- Wait for verification that ARAPCD has SE Public keys in key ring before submitting any files

Data Submission Encryption Process



Encrypt and sign data file with ***ARAPCD RSA Public Key***, sign using ***SE DSA Private Key.*** ***Creates .gpg or .pgp file.***

ARAPCD RSA Public Key
Encrypts

SE DSA Private Key
Signs

Unencrypted .dat File

Create detached signature on the encrypted and signed .gpg or .pgp file using ***SE DSA Private Key.*** ***Creates .gpg.sig or .pgp.sig file.***

SE DSA Private Key
Signs

Encrypted and signed .gpg or .pgp File

Detached .gpg.sig or .pgp.sig Signature File

Submitting Entity Steps

Each submission must include one signed and encrypted data file with a corresponding detached signature file **zipped into a single submission.**

Zip File containing both encrypted and signed .gpg or .pgp file and detached .gpg.sig or .pgp.sig Signature File

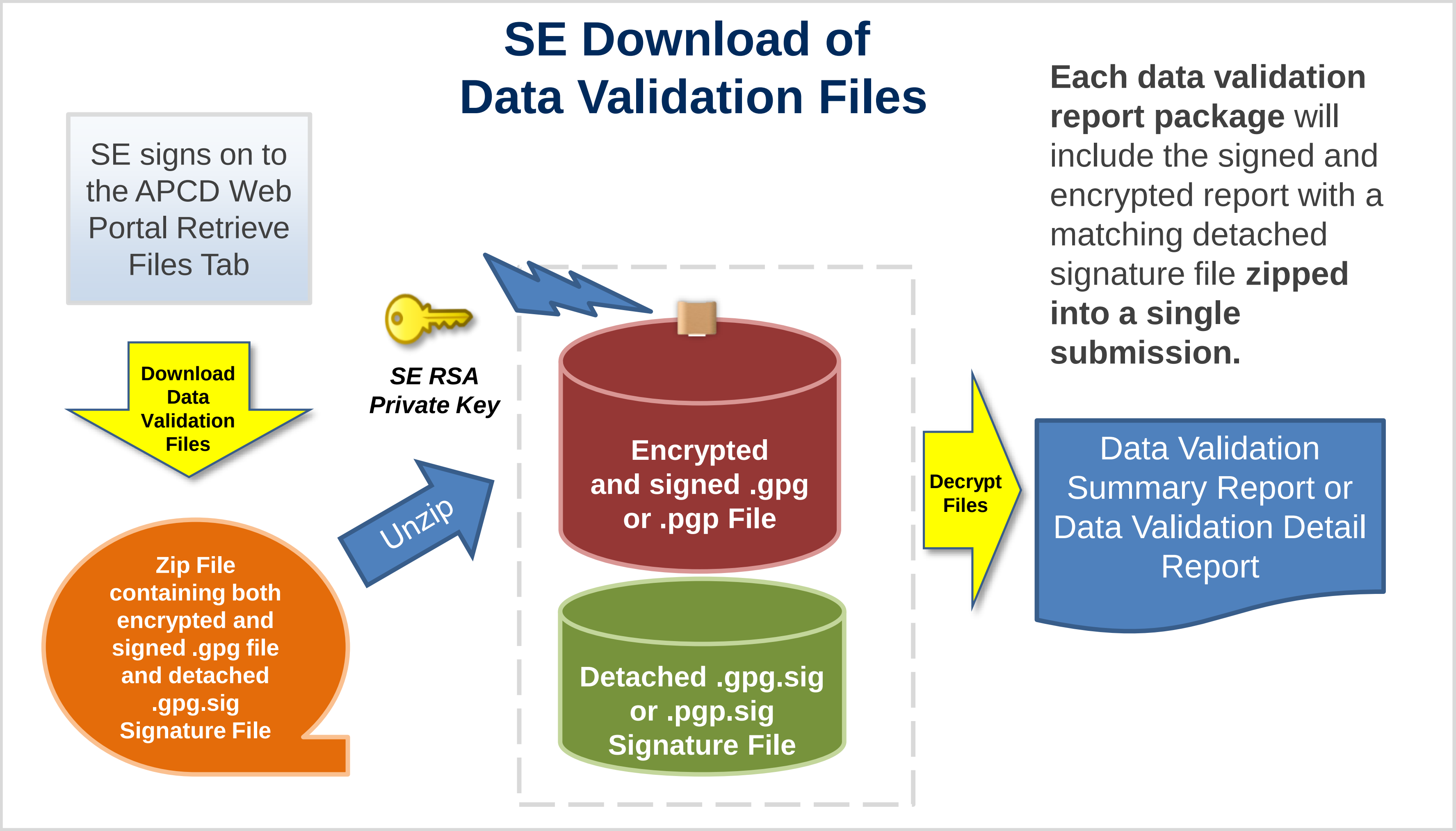
Upload **zipped file** to APCD Web Portal

Entity Decryption

Entity Checklist prior to downloading data validation reports:

- Public and Private keys imported into the key ring on the computer you will use to decrypt the data validation reports from ARAPCD
- Owner trust for SE RSA and DSA keys: ‘This is my key’
- ARAPCD public RSA and DSA keys imported into key ring on computer you will use to decrypt the data validation reports from ARAPCD
- Owner trust for ARAPCD public keys: ‘I believe checks are very accurate’
- Know the passphrase for SE RSA and DSA key

Data Validation – APCD to SE



SE Download of Data Validation Files

SE signs on to the APCD Web Portal Retrieve Files Tab

Download Data Validation Files

Zip File containing both encrypted and signed .gpg file and detached .gpg.sig Signature File

Unzip

SE RSA Private Key

Encrypted and signed .gpg or .pgp File

Detached .gpg.sig or .pgp.sig Signature File

Decrypt Files

Data Validation Summary Report or Data Validation Detail Report

Each data validation report package will include the signed and encrypted report with a matching detached signature file **zipped into a single submission.**

Other Information on Keys

The Arkansas APCD provides instructions in this document for creating keys using a free application called GPG4Win with Kleopatra.

If the SE already has OpenPGP RSA and DSA keys, those keys may be used for the Arkansas APCD file submission process. However the userid field in those keys cannot contain special characters such as commas or other standard delimiters. Examples: comma (,), pipe (|), semicolon (;), colon (:), double quote (“), single quote (’), tilde (~), tab, back slash (\), etc.

Arkansas APCD **requires** two separate keys, RSA and DSA, in order to provide an extra layer of security to protect both the SE and the Arkansas APCD.

PGP encryption can also be used for ARAPCD file submission.

Detached signatures on file submissions are required, no exceptions.

Multiple DSA public keys can be provided to the Arkansas APCD team if more than one DSA will be used in creating packages for submission.

Also in this presentation are command line instructions to encrypt and package file submissions to the Arkansas APCD.

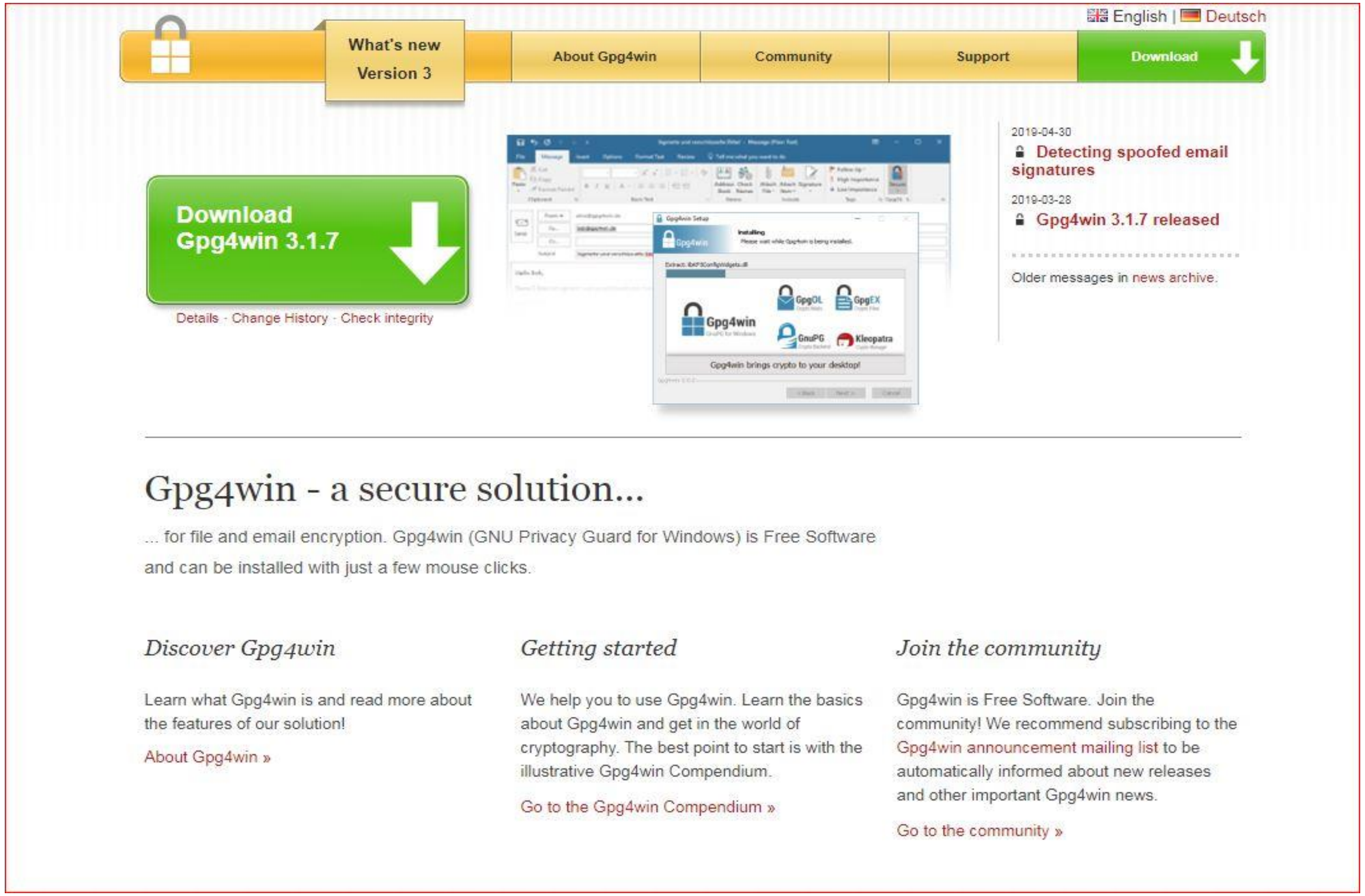
ENCRYPTION KEY CREATION

Key Creation Process

- Arkansas APCD recommends GPG4Win if encryption software needed
- Install GPG4Win from links below
- Utilize tutorial guides as needed; Possible guides:
  - PGP messaging tutorial for Windows (GPG4WIN – Kleopatra); Detailed and simple
  - A quick HOWTO for getting started with GnuPG; Updated Oct. 7, 2016
  - PGP Tutorial For Windows (Kleopatra – Gpg4Win)
  - Encrypted files in Windows with GPG and Kleopatra; 15 min. video

Note: Many of the screenshots in this slide presentation are taken from Kleopatra Version 3.1.3. Other versions may vary.

Download Gpg4win



2019-04-30

Detecting spoofed email signatures

2019-03-28

Gpg4win 3.1.7 released

Older messages in news archive.

Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Discover Gpg4win

Learn what Gpg4win is and read more about the features of our solution!

About Gpg4win »

Getting started

We help you to use Gpg4win. Learn the basics about Gpg4win and get in the world of cryptography. The best point to start is with the illustrative Gpg4win Compendium.

Go to the Gpg4win Compendium »

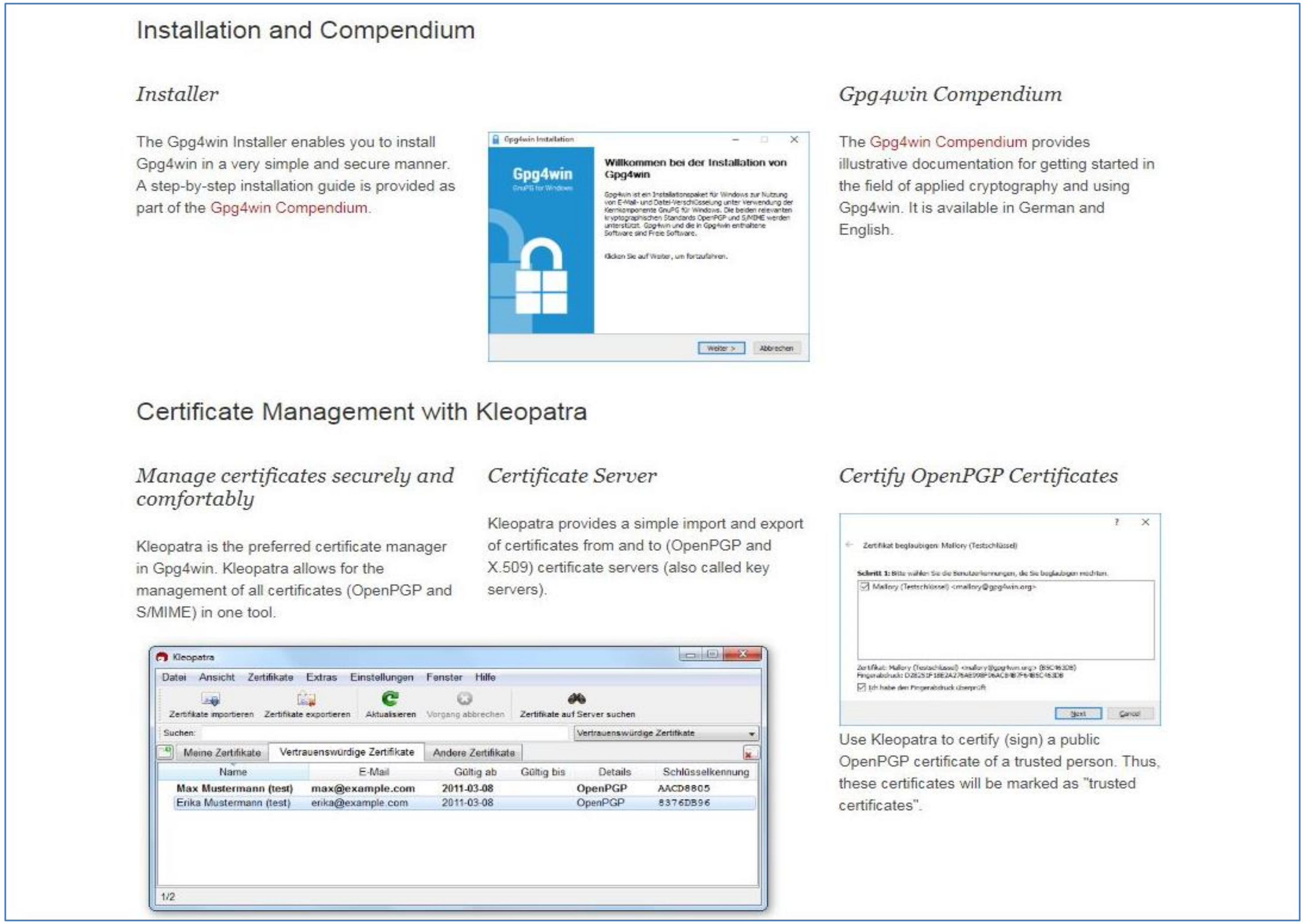
Join the community

Gpg4win is Free Software. Join the community! We recommend subscribing to the Gpg4win announcement mailing list to be automatically informed about new releases and other important Gpg4win news.

Go to the community »

Useful Links: www.gpg4win.org & www.7-zip.org

Install Kleopatra Management



Installation and Compendium

Installer

The Gpg4win Installer enables you to install Gpg4win in a very simple and secure manner. A step-by-step installation guide is provided as part of the Gpg4win Compendium.

Gpg4win Installation

Willkommen bei der Installation von Gpg4win

Gpg4win ist ein Installationspaket für Windows zur Nutzung von E-Mail- und Datei-Verschlüsselung unter Verwendung der Kernkomponente GnuPG für Windows. Die beiden relevanten kryptographischen Standards OpenPGP und S/MIME werden unterstützt. Gpg4win und die in Gpg4win enthaltene Software sind Freie Software.

Klicken Sie auf Weiter, um fortzufahren.

Gpg4win Compendium

The Gpg4win Compendium provides illustrative documentation for getting started in the field of applied cryptography and using Gpg4win. It is available in German and English.

Certificate Management with Kleopatra

Manage certificates securely and comfortably

Kleopatra is the preferred certificate manager in Gpg4win. Kleopatra allows for the management of all certificates (OpenPGP and S/MIME) in one tool.

Kleopatra

Suchen: Vertrauenswürdige Zertifikate

Name	E-Mail	Gültig ab	Gültig bis	Details	Schlüsselkennung
Max Mustermann (test)	**max@example.com**	**2011-03-08**		**OpenPGP**	**AACD8805**
Erika Mustermann (test)	erika@example.com	2011-03-08		OpenPGP	8376DB96

1/2

Certificate Server

Kleopatra provides a simple import and export of certificates from and to (OpenPGP and X.509) certificate servers (also called key servers).

Certify OpenPGP Certificates

Zertifikat beglaubigen: Mallory (Testschlüssel)

Schritt 1: Bitte wählen Sie die Benutzerkennungen, die Sie beglaubigen möchten.

☑ Mallory (Testschlüssel) <mallory@gpg4win.org>

Zertifikat: Mallory (Testschlüssel) <mallory@gpg4win.org> (B5C463DB)
Fingerabdruck: D28251F18E2A276AE908F96AC9B7F6B5C463DB

☑ Ich habe den Fingerabdruck überprüft

Use Kleopatra to certify (sign) a public OpenPGP certificate of a trusted person. Thus, these certificates will be marked as "trusted certificates".

APCD

ADMINISTERED BY ACHI

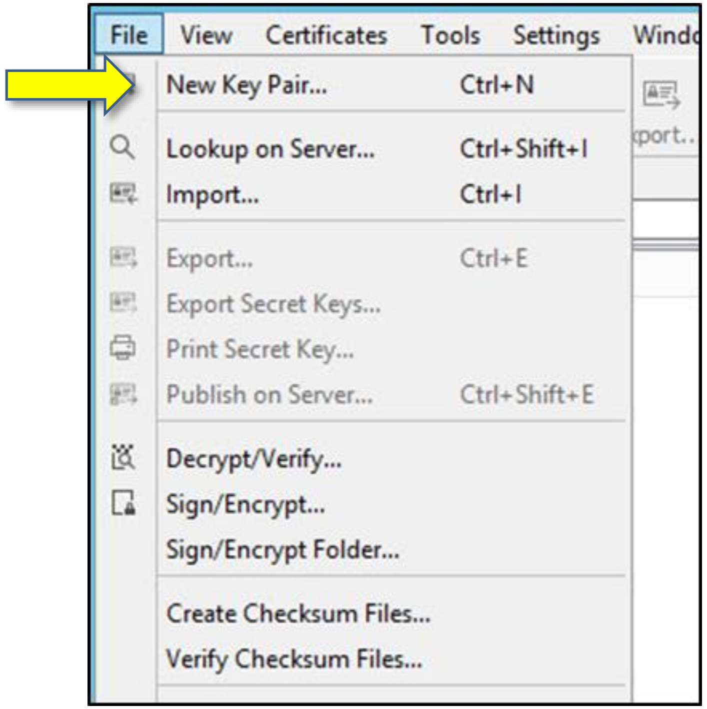
Before Keys Are Created

- Have public and private keys already been created? If yes, those keys can be used instead of creating new keys.
- If new keys are created, users must create a unique passphrase Passphrases ***are not*** recoverable.
- Users should create keys on a centrally focused email address.
  - *Example: techsupport@.... instead of KMoney@...*

Creating Encryption Keys

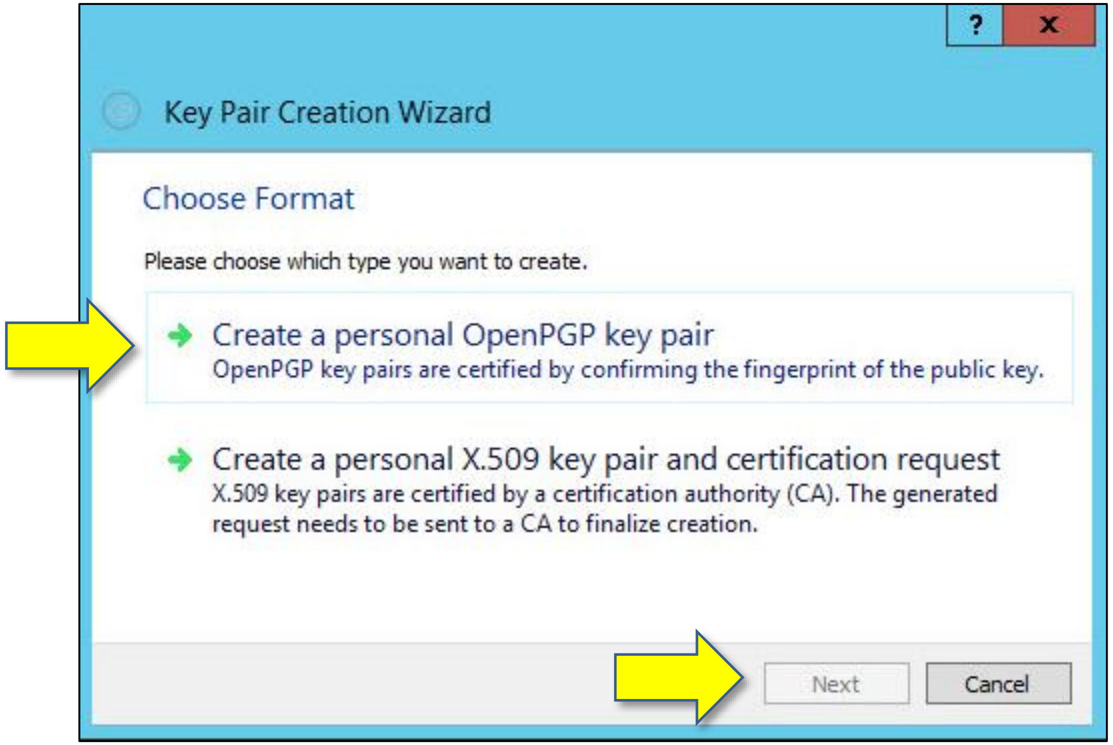
Using Kleopatra, users will create individual public and private keys. Users must create an **RSA** key and **DSA** key.

1. Open **Kleopatra**.
2. Select **File** and select **New Key Pair**.



Creating Encryption Keys

3. Select **Create a personal OpenPGP key pair**.
4. Click **Next**.



Key Pair Creation Wizard

Choose Format

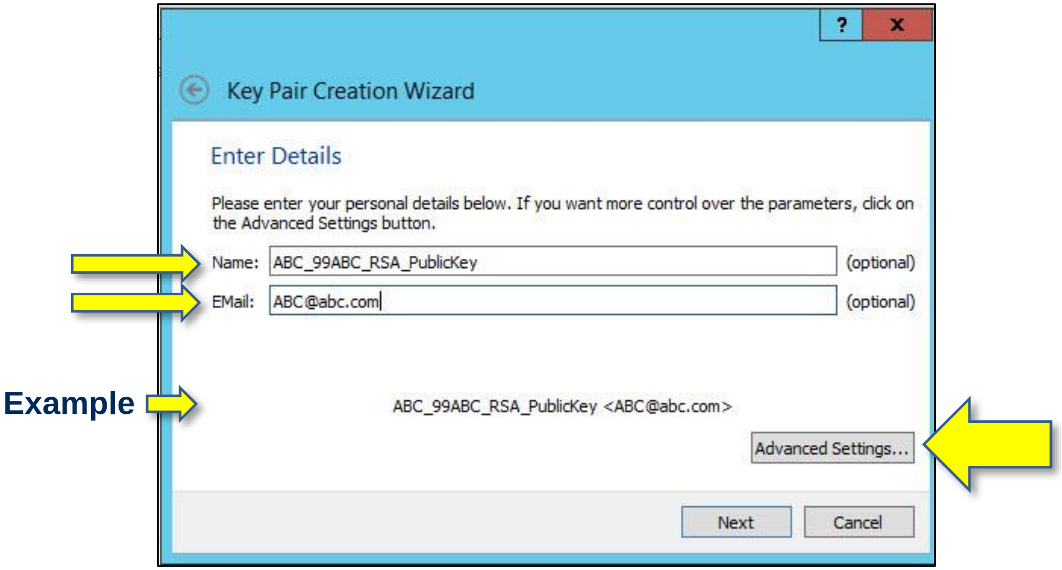
Please choose which type you want to create.

➔ Create a personal OpenPGP key pair
OpenPGP key pairs are certified by confirming the fingerprint of the public key.

➔ Create a personal X.509 key pair and certification request
X.509 key pairs are certified by a certification authority (CA). The generated request needs to be sent to a CA to finalize creation.

Creating Encryption Keys

5. Enter the **Name** and identify the type of key in the name (**RSA** = Encryption/Decryption; **DSA** = Signing/Verification).
6. Enter **Email** address.
7. Click on the **Advanced Settings** tab to select the type of key (**RSA** is used in the example).



Key Pair Creation Wizard

Enter Details

Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.

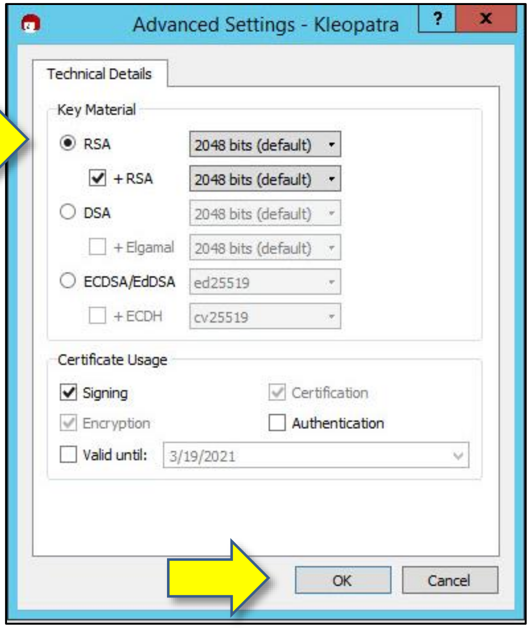
Name: ABC_99ABC_RSA_PublicKey (optional)

EMail: ABC@abc.com (optional)

Example ABC_99ABC_RSA_PublicKey <ABC@abc.com>

Creating Encryption Keys

8. On the **Advanced Settings** tab, select **RSA**.
9. Click **OK** to return to previous screen.



Key Material

● RSA 2048 bits (default)

☑ + RSA 2048 bits (default)

○ DSA 2048 bits (default)

□ + Elgamal 2048 bits (default)

○ ECDSA/EdDSA ed25519

□ + ECDH cv25519

Certificate Usage

☑ Signing ☑ Certification

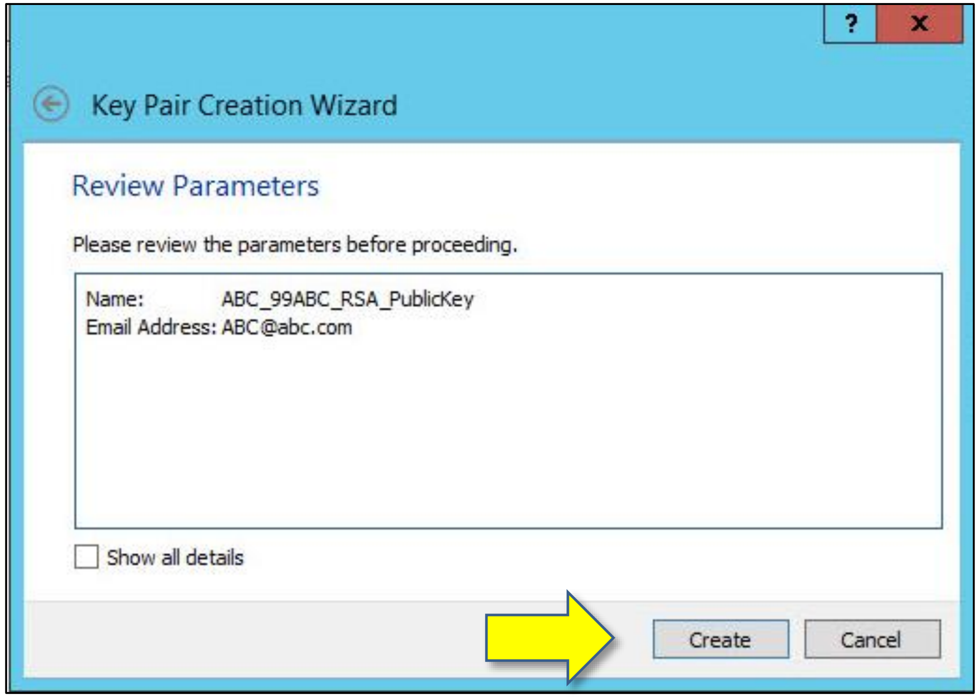
☑ Encryption □ Authentication

□ Valid until: 3/19/2021

10. Click on **Next** to review the **Certificate Parameters**.

Creating Encryption Keys

11. Under **Review Parameters**, click **Create**.



Review Parameters

Please review the parameters before proceeding.

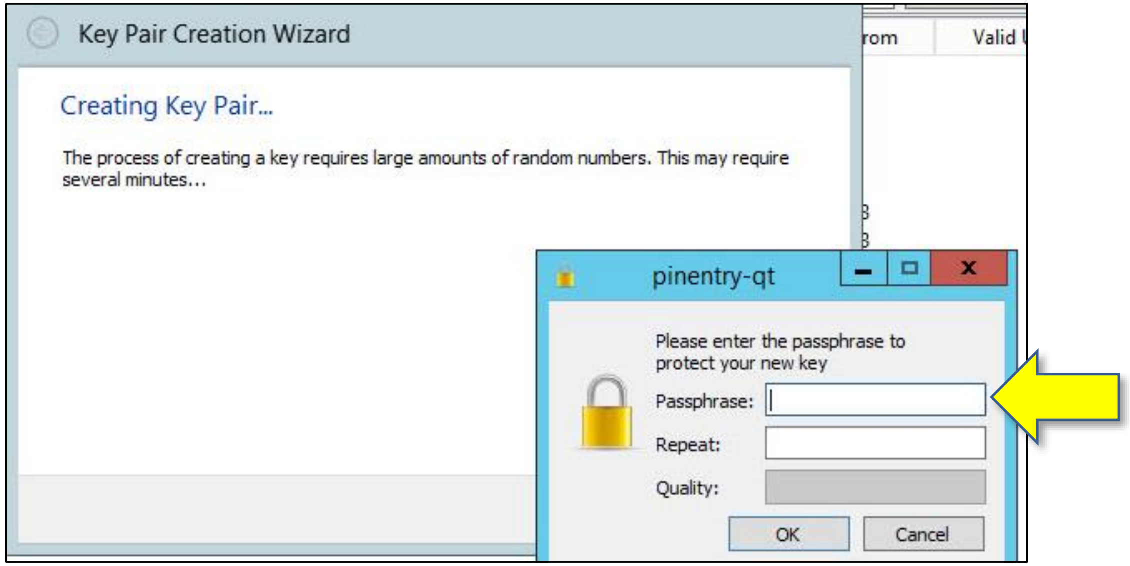
Name: ABC_99ABC_RSA_PublicKey
Email Address: ABC@abc.com

□ Show all details

Creating Encryption Keys

12. To finalize the key, enter a **passphrase**.

(**NOTE:** If a user forgets a passphrase, the user ***will not*** be able to recover it.)



Key Pair Creation Wizard

Creating Key Pair...

The process of creating a key requires large amounts of random numbers. This may require several minutes...

pinentry-qt

Please enter the passphrase to protect your new key

Passphrase:

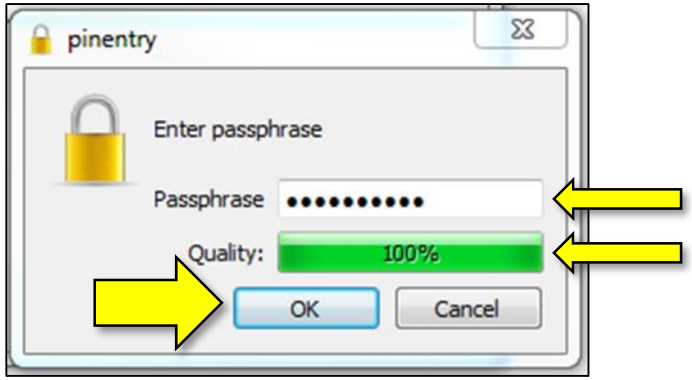
Repeat:

Quality:

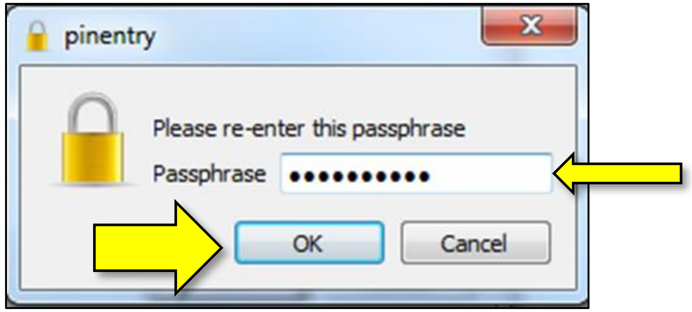
How to choose a passphrase: http://www.pgpi.org/doc/faq/passphrase/

Creating Encryption Keys

13. As the **passphrase** is entered, the **quality** (security) will be measured.
14. Click **OK**.

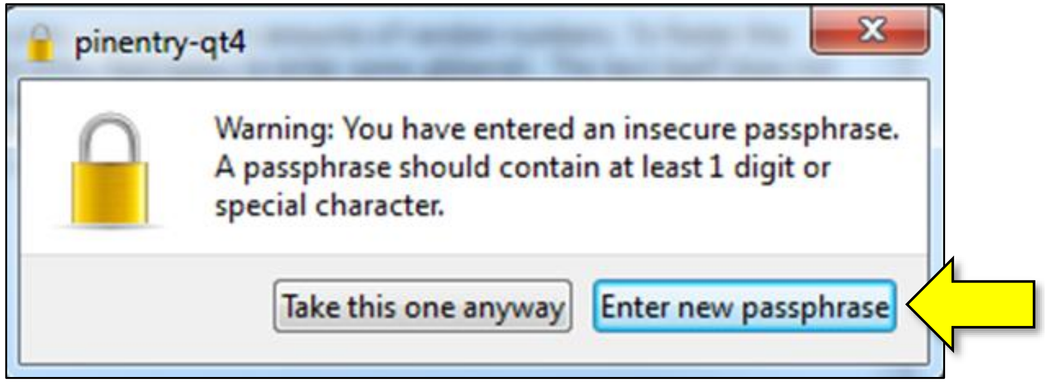


15. Re-enter the **passphrase**.
16. Click **OK**.



Creating Encryption Keys

17. If the passphrase is not strong enough, users may receive a warning. If a warning is received, select **Enter new passphrase** and repeat steps 12–16.

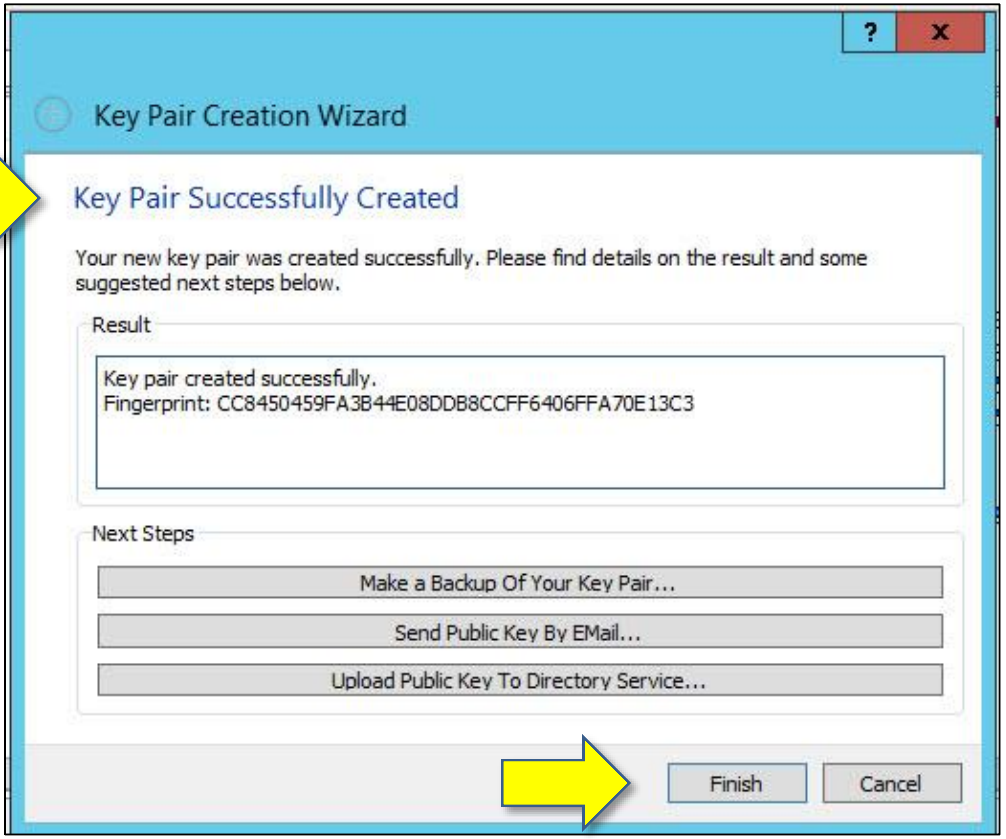


Warning: You have entered an insecure passphrase. A passphrase should contain at least 1 digit or special character.

Creating Encryption Keys

18. Users will receive confirmation after the **Key Pair** has been created. Click **Finish**.

Confirmation



?
x
Key Pair Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

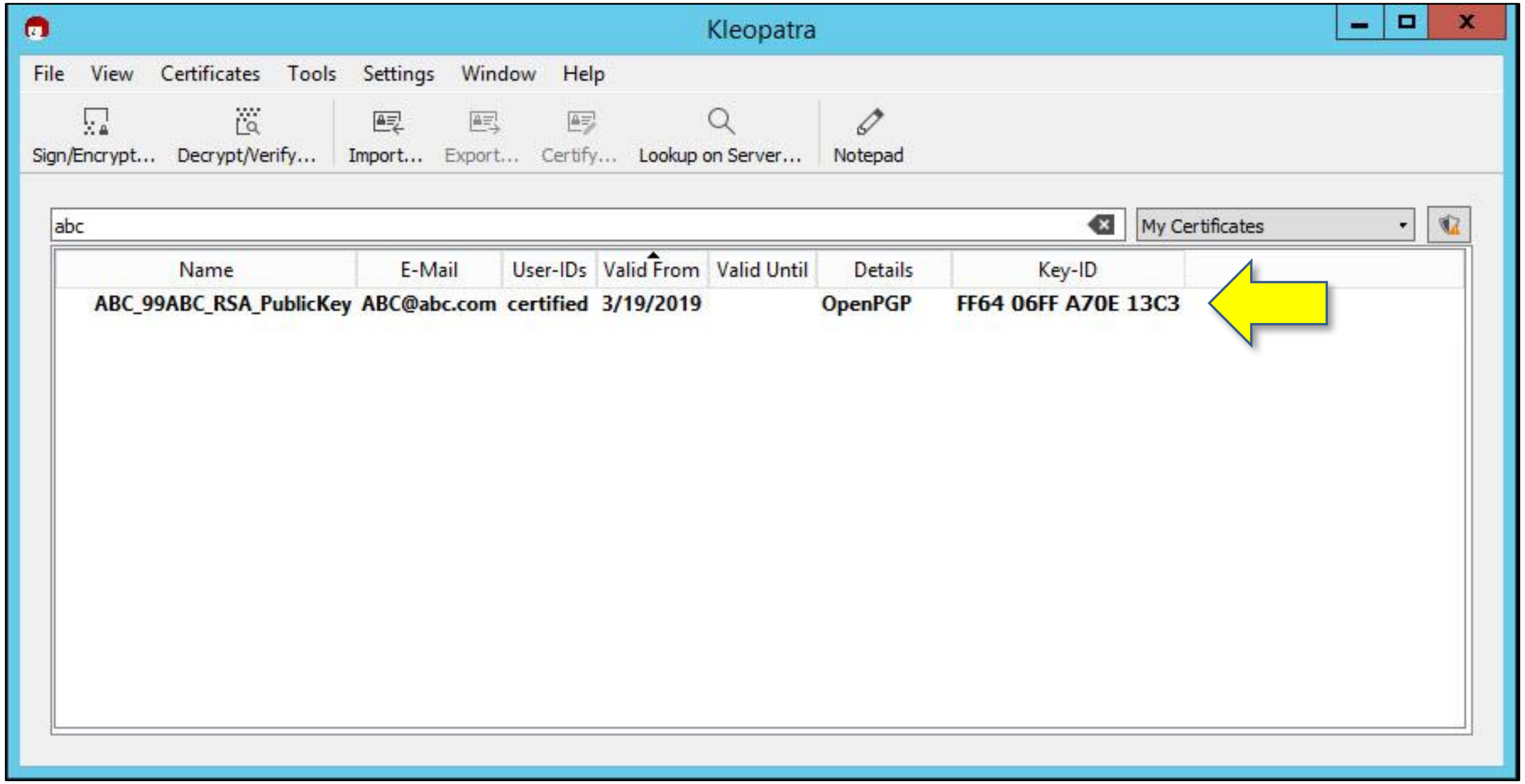
Key pair created successfully.
Fingerprint: CC8450459FA3B44E08DDB8CCFF6406FFA70E13C3

Next Steps

Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel

Creating Encryption Keys

19. View the **RSA** Certificate listed in bold.



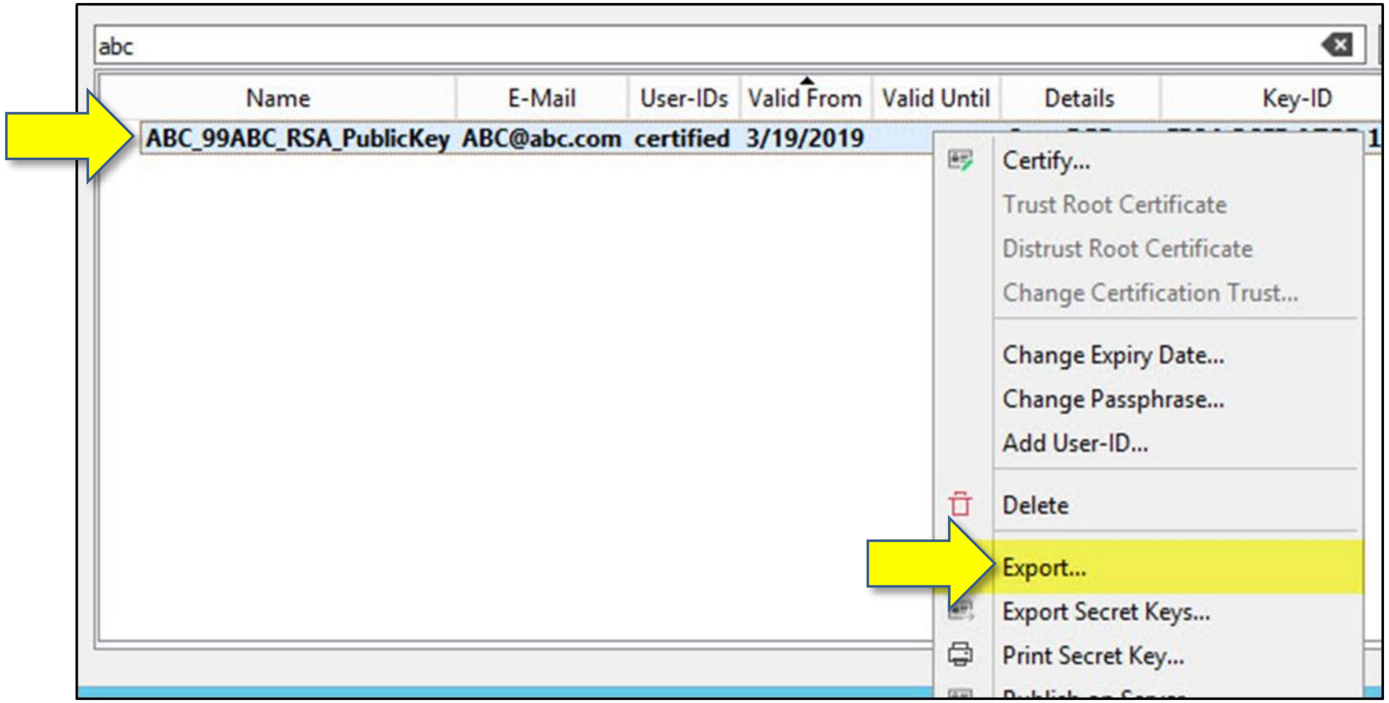
abc

My Certificates

Name	E-Mail	User-IDs	Valid From	Valid Until	Details	Key-ID
ABC_99ABC_RSA_PublicKey	**ABC@abc.com**	**certified**	**3/19/2019**		**OpenPGP**	**FF64 06FF A70E 13C3**

Creating Encryption Keys

20. After keys have been created, users may export Public Key Certificates. Right click on the **Certificate** in the list.
21. Select **Export**.



abc

Name	E-Mail	User-IDs	Valid From	Valid Until	Details	Key-ID
ABC_99ABC_RSA_PublicKey	ABC@abc.com	certified	3/19/2019			

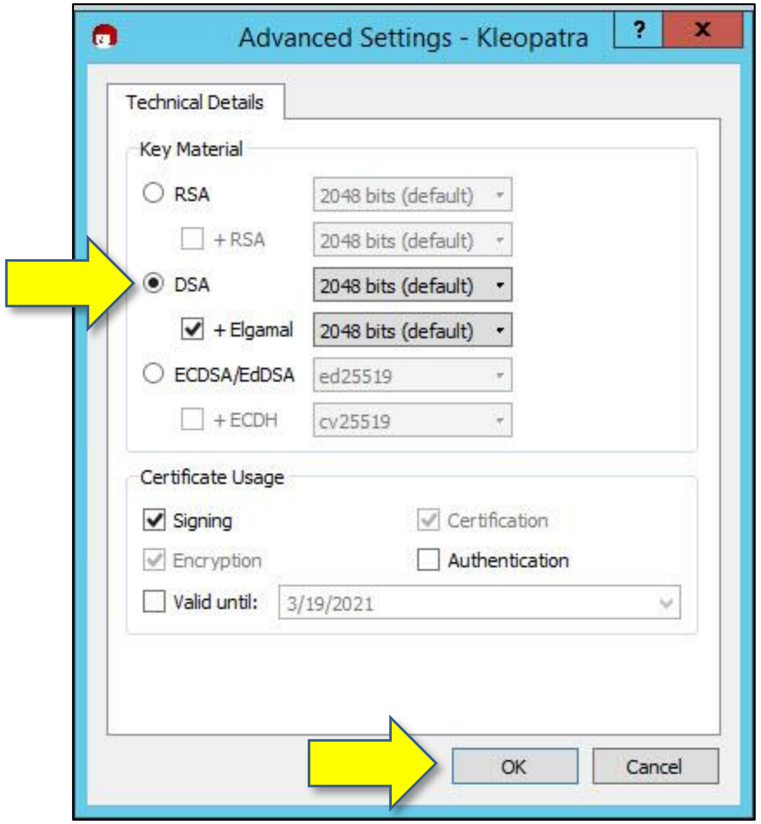
Creating/Sharing Encryption Keys

22. Name the exported **Public Keys Certificate file** using the following naming convention:
    [Entity Name]_[RSA or DSA]_PublicKey.asc

    For example: 123AB_RSA_PublicKey.asc
23. Share the Public Certificates with the Arkansas APCD via any of the following methods:
    a. Service Desk Support Ticket (preferred and secure)
    b. Email
    c. Publish Public Keys to a key server
        a. Keys published to a key server cannot be removed, only revoked
24. Name **Private Keys** using user-specified naming conventions

Creating Encryption Keys

25. To create the **DSA Key Pair**, select **DSA** on the **Advanced Settings** tab with the settings below and repeat steps 1–24.



Advanced Settings - Kleopatra

Technical Details

Key Material

○ RSA 2048 bits (default)

□ + RSA 2048 bits (default)

● DSA 2048 bits (default)

☑ + Elgamal 2048 bits (default)

○ ECDSA/EdDSA ed25519

□ + ECDH cv25519

Certificate Usage

☑ Signing

☑ Certification

☑ Encryption

□ Authentication

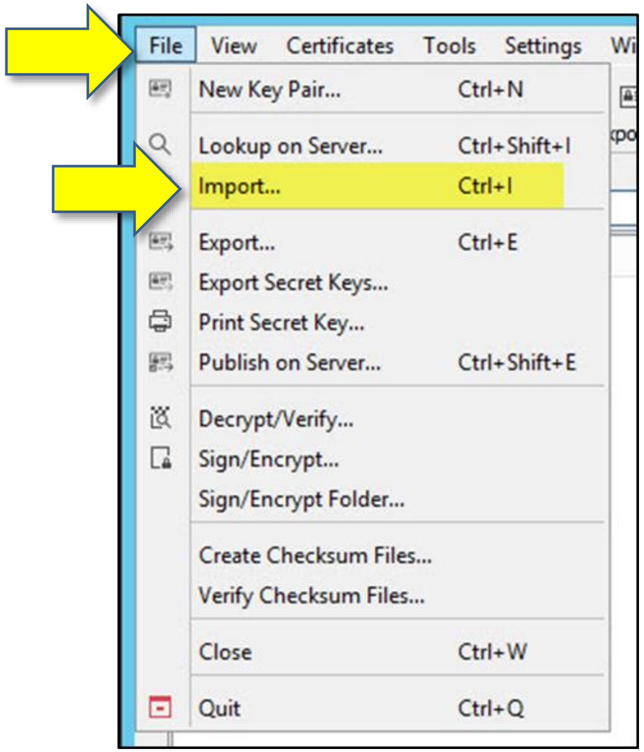
□ Valid until: 3/19/2021

IMPORTING KEYS

Import and Trust ARAPCD Public Keys Using Kleopatra

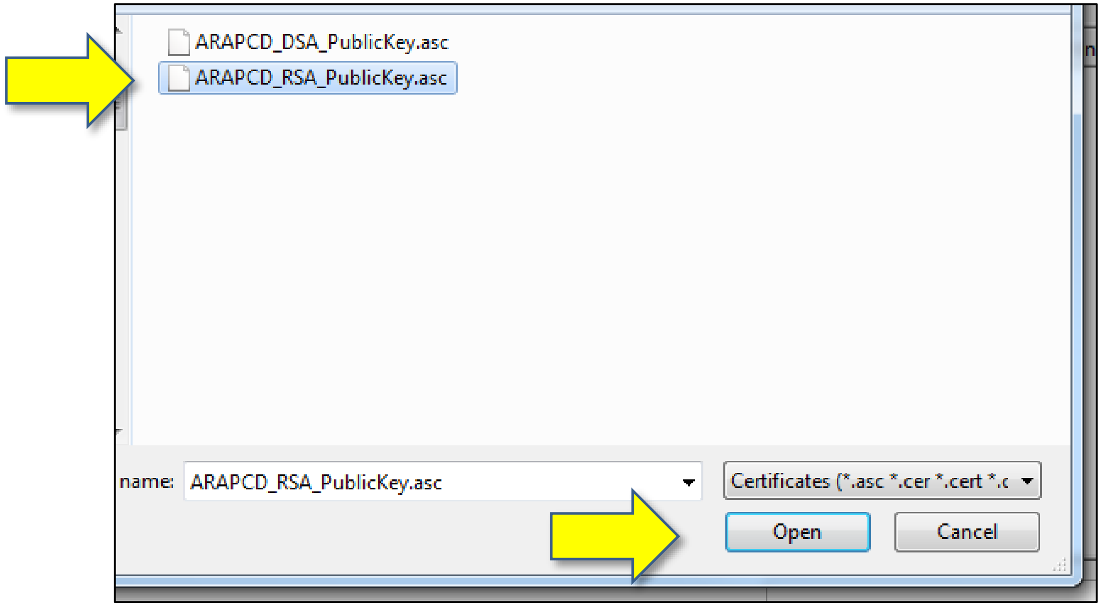
Follow these steps for *each* of the public key certificate files.

1. Select the **File** menu, then select **Import**.



Import and Trust ARAPCD Public Keys Using Kleopatra

2. Select one of the **.asc** files provided by the APCD Technical Support Team, and click **Open**.



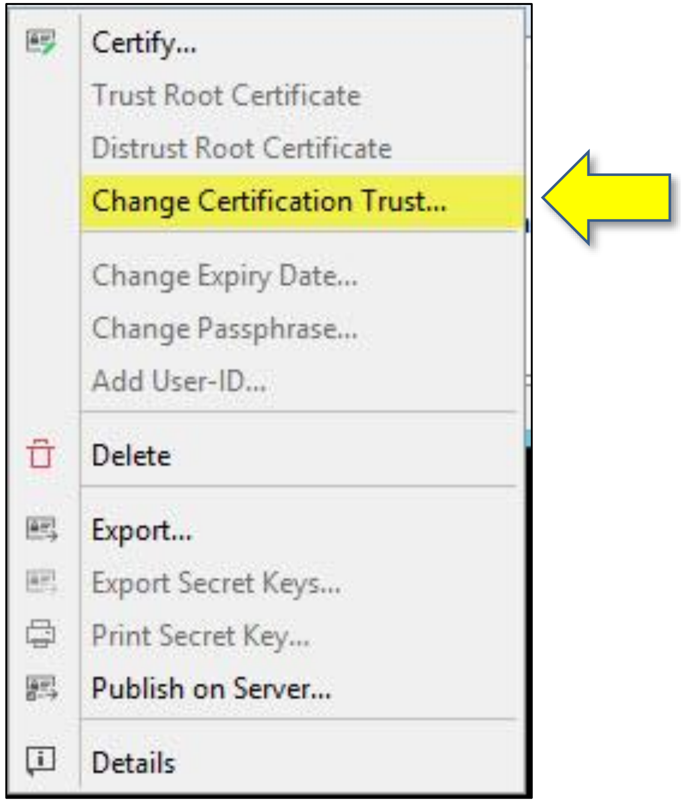
ARAPCD_DSA_PublicKey.asc
ARAPCD_RSA_PublicKey.asc

name: ARAPCD_RSA_PublicKey.asc

Certificates (*.asc *.cer *.cert *.c

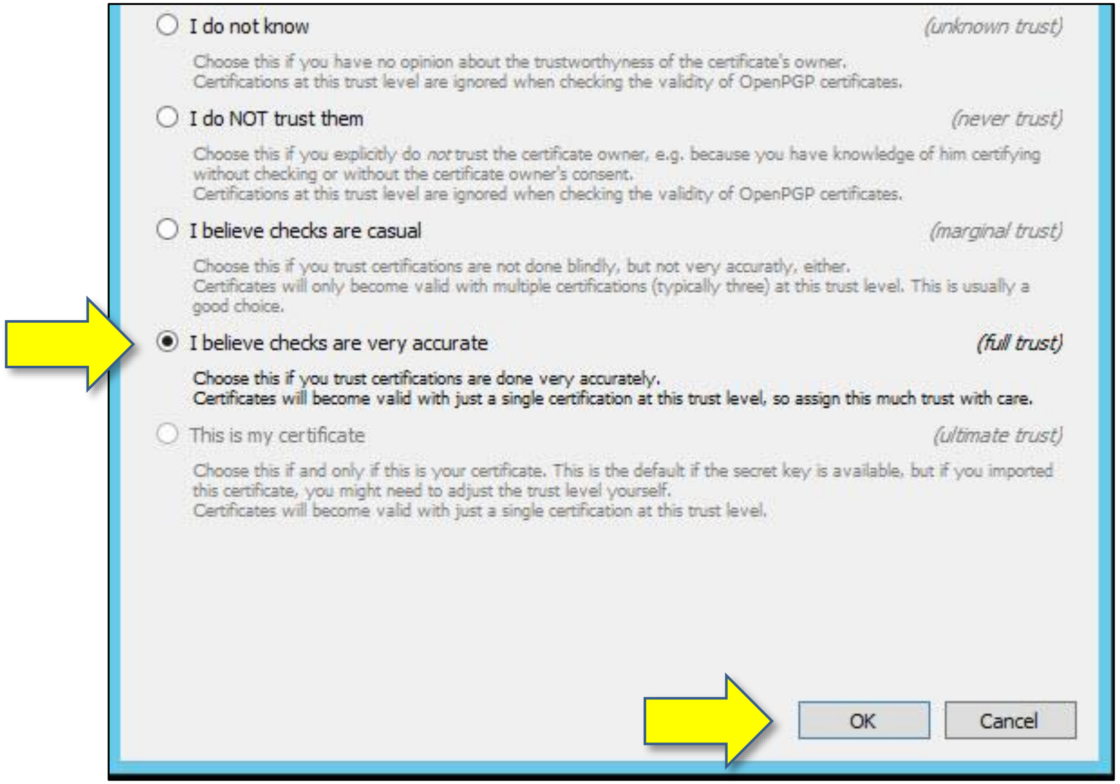
Import and Trust ARAPCD Public Keys Using Kleopatra

3. Right-click on the key, and select **Change Certification Trust**.



Import and Trust ARAPCD Public Keys Using Kleopatra

4. Select **I believe checks very accurate**, then click **OK**.



○ I do not know *(unknown trust)*

Choose this if you have no opinion about the trustworthyness of the certificate's owner.
Certifications at this trust level are ignored when checking the validity of OpenPGP certificates.

○ I do NOT trust them *(never trust)*

Choose this if you explicitly do *not* trust the certificate owner, e.g. because you have knowledge of him certifying without checking or without the certificate owner's consent.
Certifications at this trust level are ignored when checking the validity of OpenPGP certificates.

○ I believe checks are casual *(marginal trust)*

Choose this if you trust certifications are not done blindly, but not very accuratly, either.
Certificates will only become valid with multiple certifications (typically three) at this trust level. This is usually a good choice.

● I believe checks are very accurate *(full trust)*

Choose this if you trust certifications are done very accurately.
Certificates will become valid with just a single certification at this trust level, so assign this much trust with care.

○ This is my certificate *(ultimate trust)*

Choose this if and only if this is your certificate. This is the default if the secret key is available, but if you imported this certificate, you might need to adjust the trust level yourself.
Certificates will become valid with just a single certification at this trust level.

FILE ENCRYPTION

Encryption and Signature Checklist

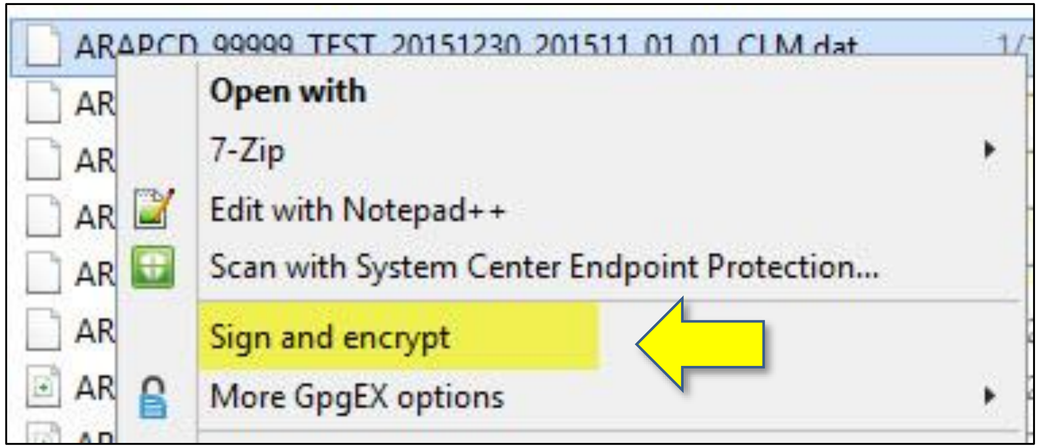
Prior to encrypting and signing data files, users must:

- Install recommended tools:
  - GPG4Win: installs Kleopatra
  - 7-Zip
- Ensure the **ARAPCD_RSA** and **ARAPCD_DSA** public keys are imported and trusted in Kleopatra
- Know respective passphrases for using private keys

Encryption and Signature Checklist

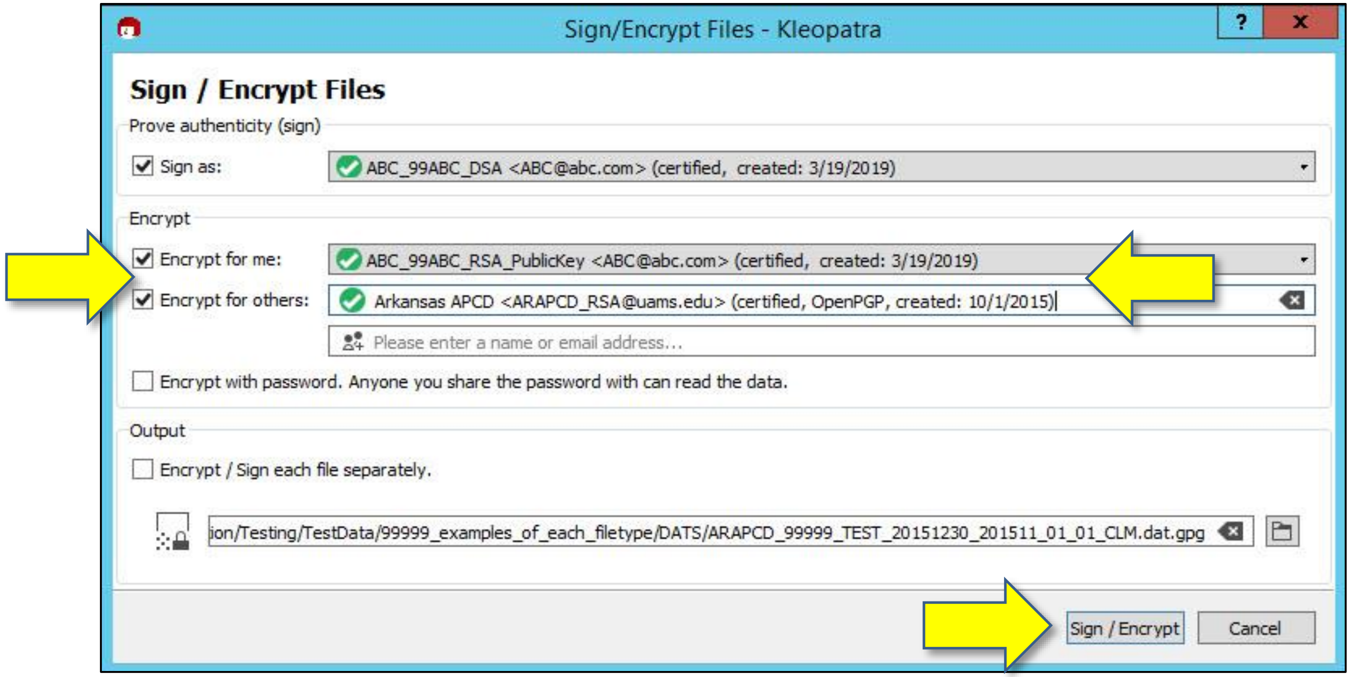
To manually encrypt and sign data files using Kleopatra:

1. Right-click on the file in Explorer.
2. Select **Sign and encrypt**.


ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat
Open with
7-Zip
Edit with Notepad++
Scan with System Center Endpoint Protection...
Sign and encrypt
More GpgEX options

Manual Encryption and Signing Using Kleopatra

3. Check both **Encrypt for me** and **Encrypt for others**.
4. Verify the **ARAPCD_RSA** key is selected in the **Encrypt for others** field.
5. Verify your RSA key is listed in the **Encrypt for me** field.
6. Click **Sign /Encrypt**.



Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: ABC_99ABC_DSA <ABC@abc.com> (certified, created: 3/19/2019)

Encrypt

☑ Encrypt for me: ABC_99ABC_RSA_PublicKey <ABC@abc.com> (certified, created: 3/19/2019)

☑ Encrypt for others: Arkansas APCD <ARAPCD_RSA@uams.edu> (certified, OpenPGP, created: 10/1/2015)

Please enter a name or email address...

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

Output

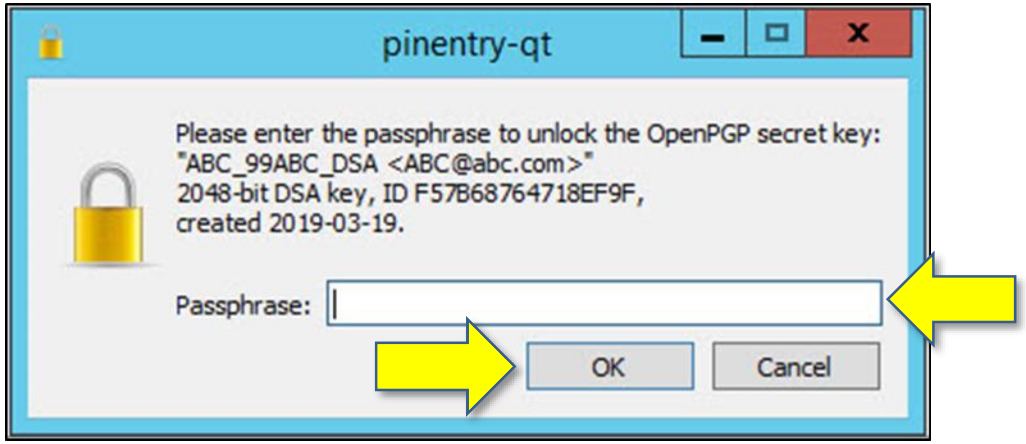
□ Encrypt / Sign each file separately.

ion/Testing/TestData/99999_examples_of_each_filetype/DATS/ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat.gpg

Manual Encryption and Signing Using Kleopatra

Users will be prompted for their respective DSA signing Key Passphrases:

7. Enter the **Passphrase**.
8. Click **OK**.



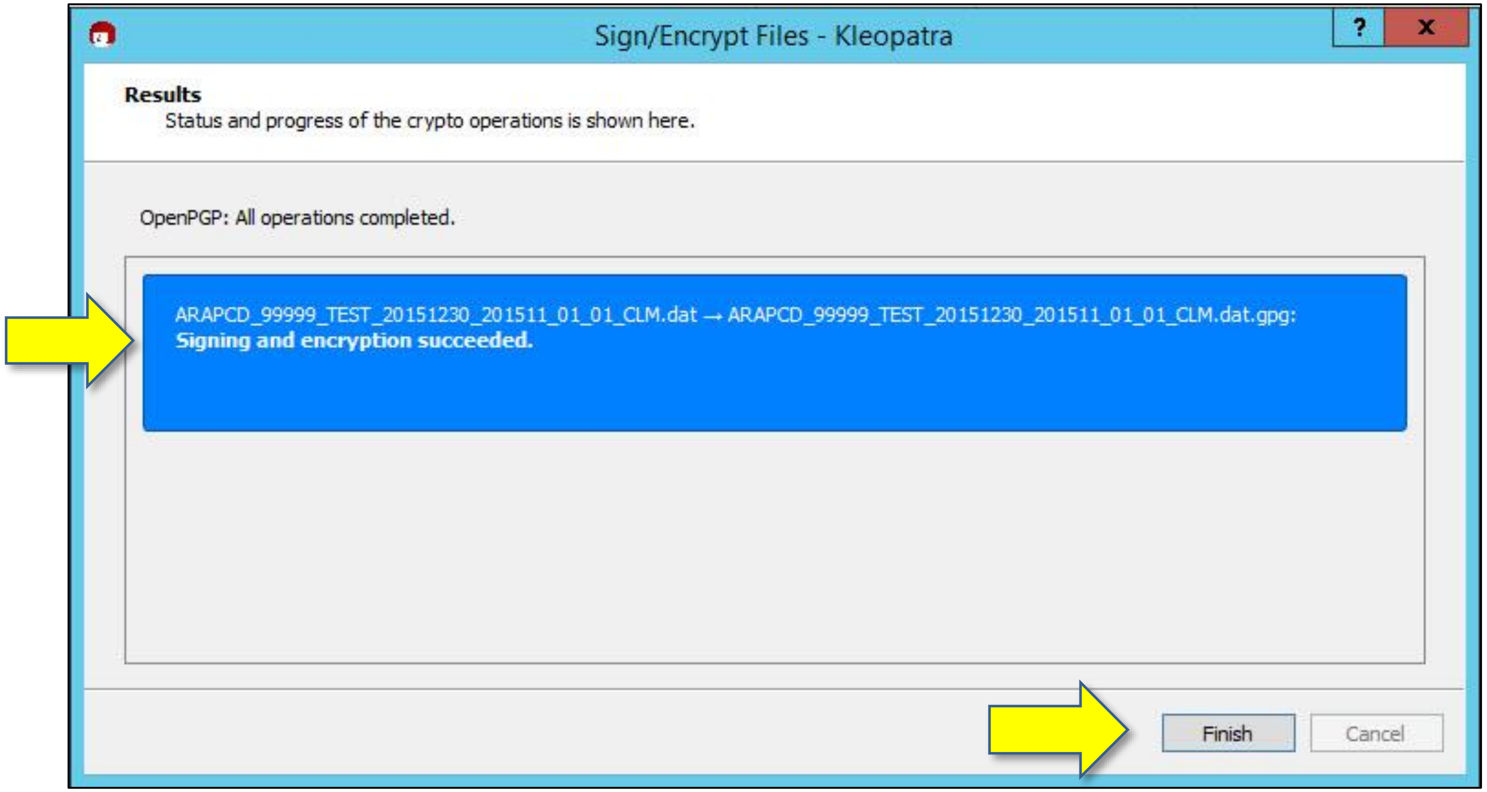
Please enter the passphrase to unlock the OpenPGP secret key:
"ABC_99ABC_DSA <ABC@abc.com>"
2048-bit DSA key, ID F57B68764718EF9F,
created 2019-03-19.

Passphrase:

Manual Encryption and Signing Using Kleopatra

After entering the correct passphrase, users will see the following results.

9. Click **Finish**.



Results

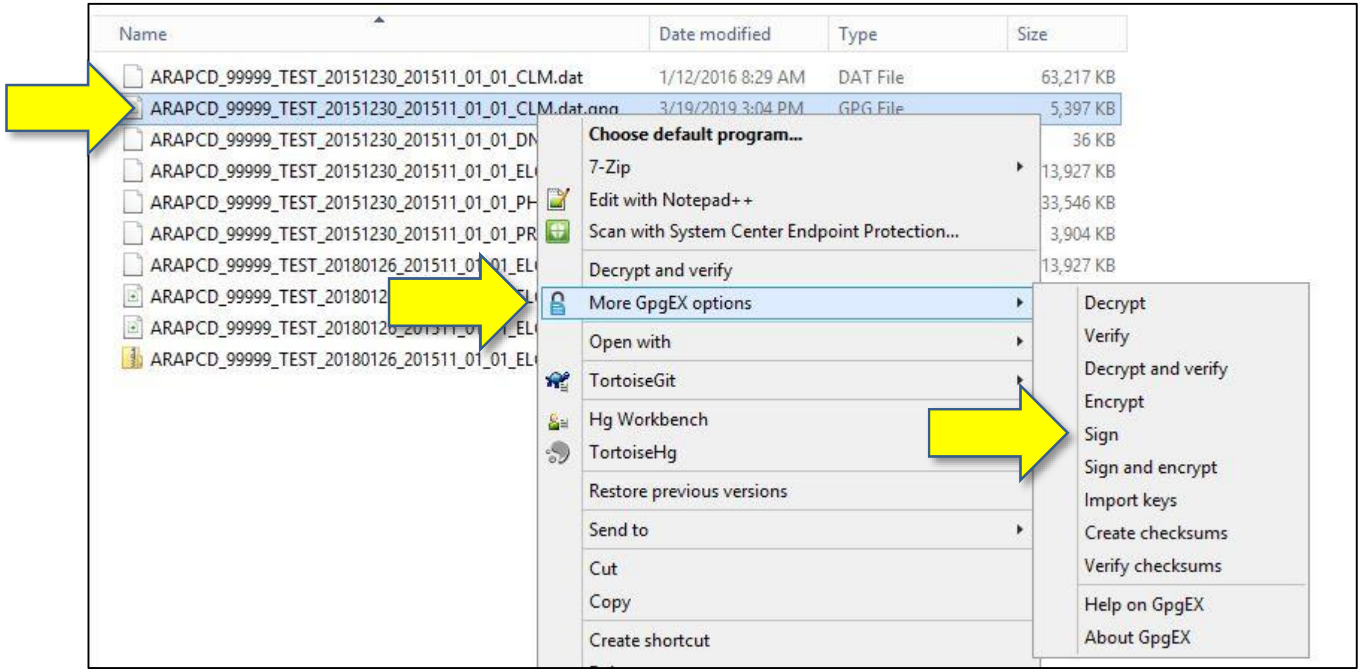
Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat → ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat.gpg:
Signing and encryption succeeded.

Manual Encryption and Signing Using Kleopatra

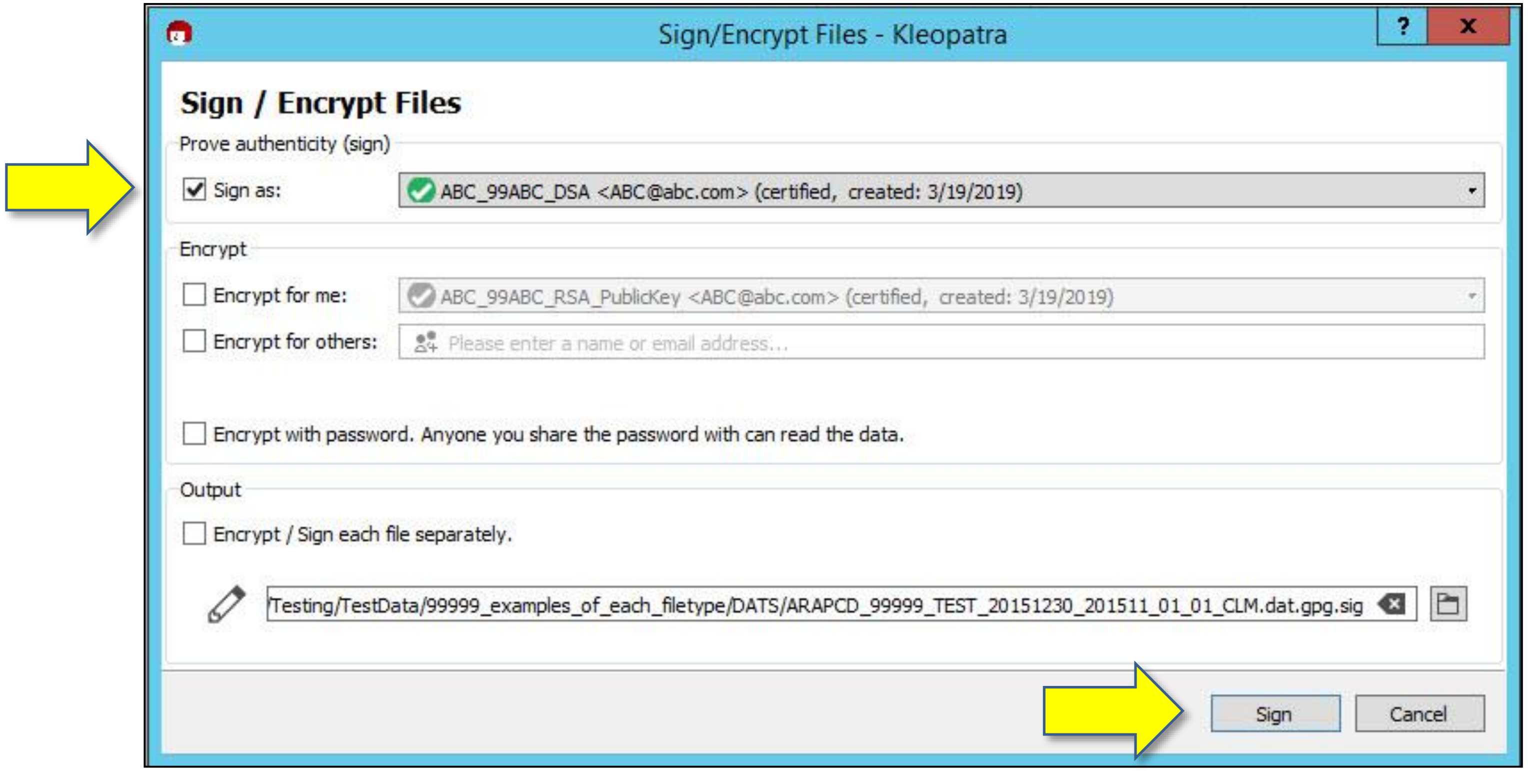
10. Locate the **.gpg** file recently created and right-click.
11. Select **More GpgEX options**.
12. Select **Sign**.



Name	Date modified	Type	Size
ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat	1/12/2016 8:29 AM	DAT File	63,217 KB
ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat.gpg	3/19/2019 3:04 PM	GPG File	5,397 KB
ARAPCD_99999_TEST_20151230_201511_01_01_DN			36 KB
ARAPCD_99999_TEST_20151230_201511_01_01_EL			13,927 KB
ARAPCD_99999_TEST_20151230_201511_01_01_PH			33,546 KB
ARAPCD_99999_TEST_20151230_201511_01_01_PR			3,904 KB
ARAPCD_99999_TEST_20180126_201511_01_01_EL			13,927 KB
ARAPCD_99999_TEST_2018012			
ARAPCD_99999_TEST_2018012			
ARAPCD_99999_TEST_20180126_201511_01_01_EL			

Manual Encryption and Signing Using Kleopatra

13. Verify your DSA key is populated to the right of **Sign as**.
14. Click **Sign**.



Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: ABC_99ABC_DSA <ABC@abc.com> (certified, created: 3/19/2019)

Encrypt

□ Encrypt for me: ABC_99ABC_RSA_PublicKey <ABC@abc.com> (certified, created: 3/19/2019)

□ 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.

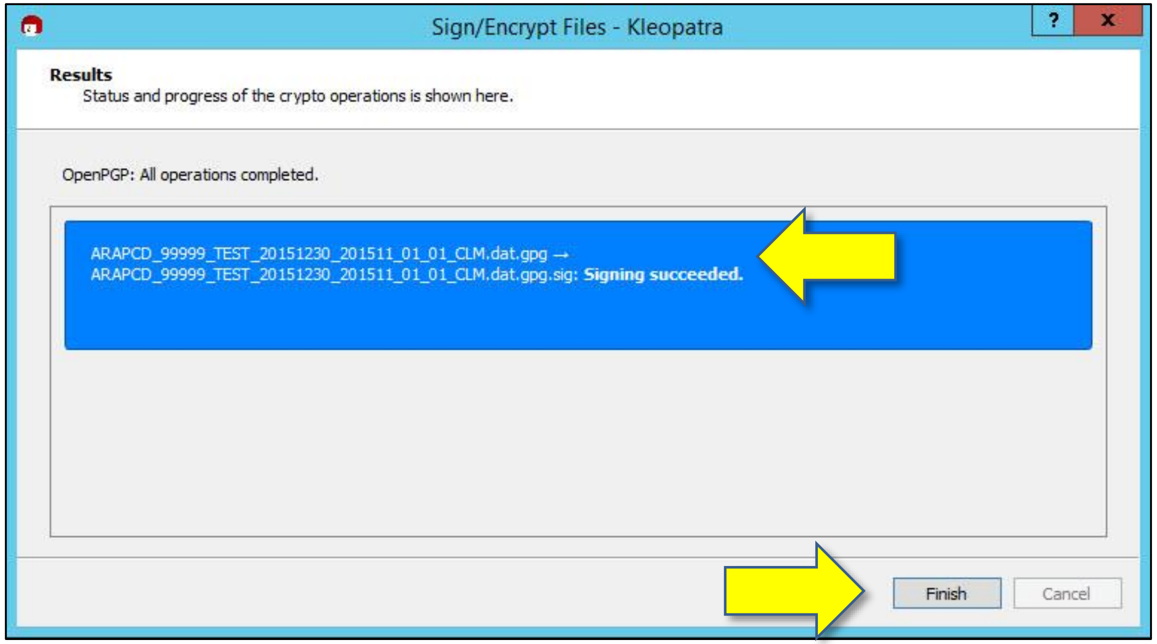
Testing/TestData/99999_examples_of_each_filetype/DATS/ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat.gpg.sig

Manual Encryption and Signing Using Kleopatra

As displayed in the results, users will have two (2) files:

- Encrypted and signed **.gpg** file
- Detached signed **.gpg.sig** file

15. Note **Signing succeeded**.
16. Click **Finish**.



Sign/Encrypt Files - Kleopatra

Results
Status and progress of the crypto operations is shown here.

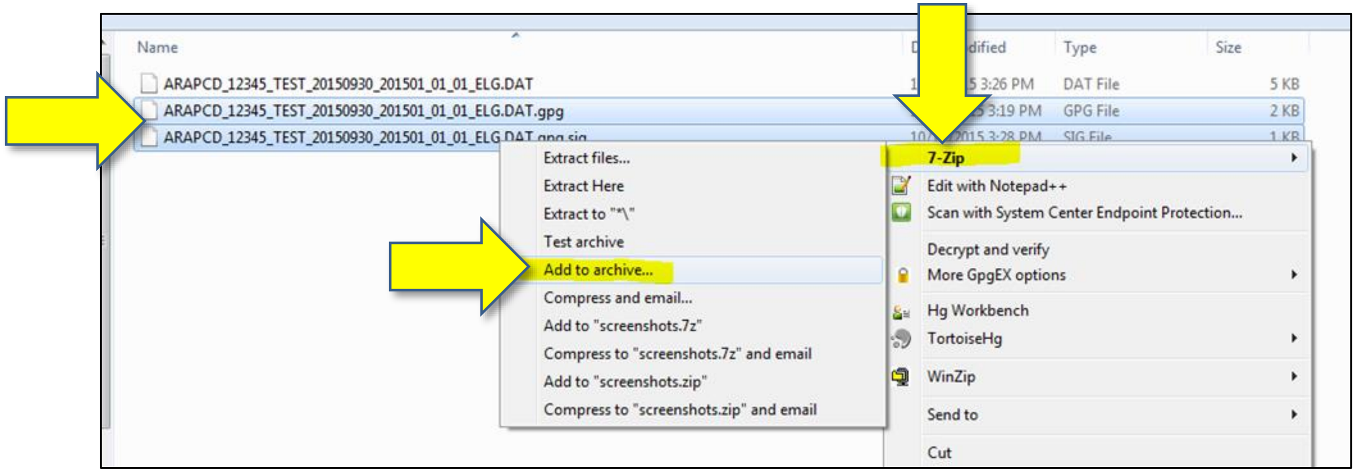
OpenPGP: All operations completed.

ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat.gpg →
ARAPCD_99999_TEST_20151230_201511_01_01_CLM.dat.gpg.sig: **Signing succeeded.**

Manual Encryption and Signing Using Kleopatra — Packaging

To create the **.zip** file package:

17. Select both the **.gpg** file and the **.gpg.sig** file.
18. Right-click.
19. Select **7-Zip**.
20. Select **Add to archive**.

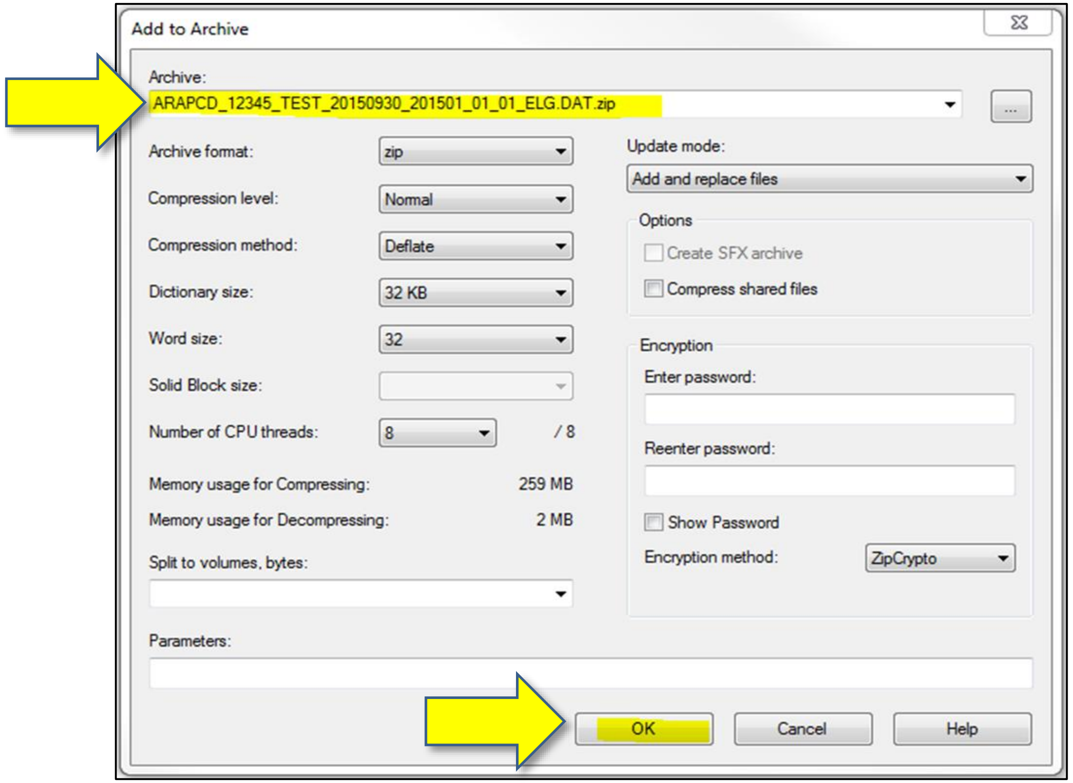


Manual Encryption and Signing Using Kleopatra — Packaging

Under the **Add to Archive** option:

21. Name the **Archive** file the same as the **unencrypted .dat file** plus the **.zip** extension.
22. Click **OK**.

(Archive data file name format must end with the .dat.zip extension.)



Add to Archive

Archive: ARAPCD_12345_TEST_20150930_201501_01_01_ELG.DAT.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

☐ Create SFX archive

☐ Compress shared files

Encryption

Enter password:

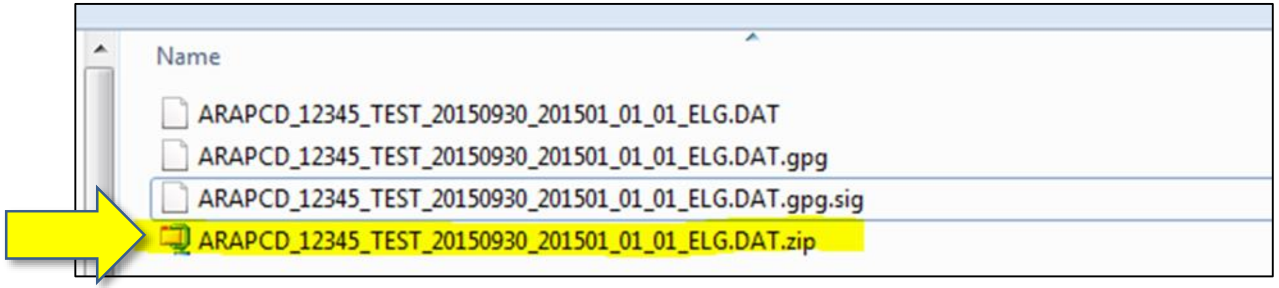
Reenter password:

☐ Show Password

Encryption method: ZipCrypto

Manual Encryption and Signing Using Kleopatra — Packaging

The **.zip file** has now been created. It will appear in the file listing as follows:



ARAPCD_12345_TEST_20150930_201501_01_01_ELG.DAT
ARAPCD_12345_TEST_20150930_201501_01_01_ELG.DAT.gpg
ARAPCD_12345_TEST_20150930_201501_01_01_ELG.DAT.gpg.sig
ARAPCD_12345_TEST_20150930_201501_01_01_ELG.DAT.zip

23. Upload the **.zip file** to the APCD via the Web Portal.

Additional Support

- Several instructional videos are available online. One has been included here for reference.
  - – https://www.youtube.com/watch?v=Cbv4jPIJ8J8