DATA MECHANISM ENCRYPTION MANUAL

Encryption

The data switch system will only accept encrypted files with “gpg” extensions. This is to ensure highly secure data transfer of files.

GnuPG

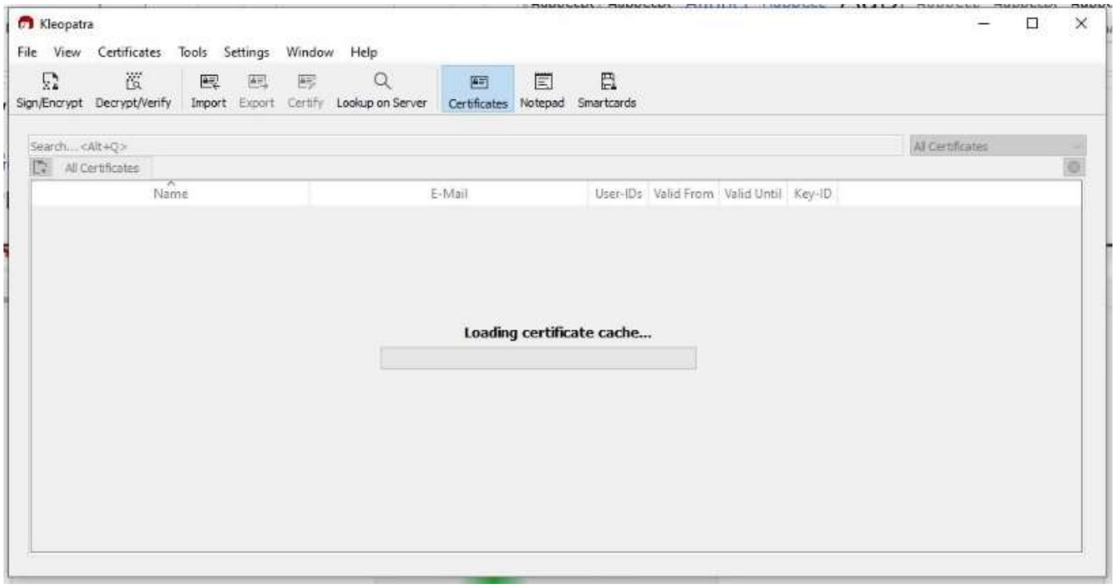
GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a versatile key management system, along with access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available.
To install this encryption software, navigate to the following site;

The GNU Privacy Guard (gnupg.org) or https://www.gpg4win.org/

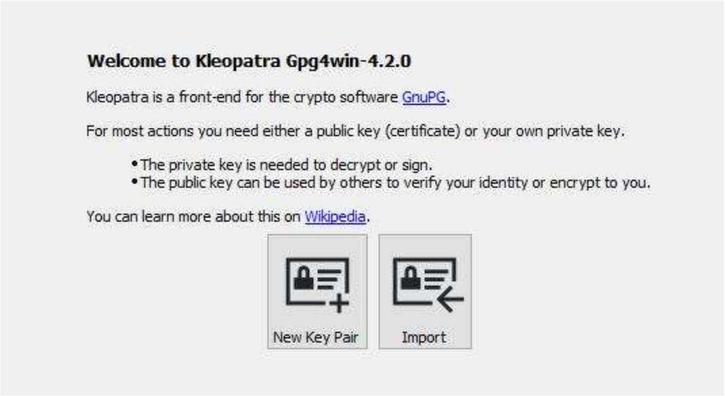
Go to the Downloads page and download the latest version of the software.
This will also install a Graphical User Interface known as Kleopatra which will manage the public and private keys.
To ensure that only privy parties can access the system, a public-private key system will be used.
At the CRB, a key pair will be generated. With this key pair, the private key will be kept at the CRB while the public key will be shared with the PIs;

Generating a Public-Private Key Pair

Open the Kleopatra GUI on your system.



Loading certificate cache...



Welcome to Kleopatra Gpg4win-4.2.0

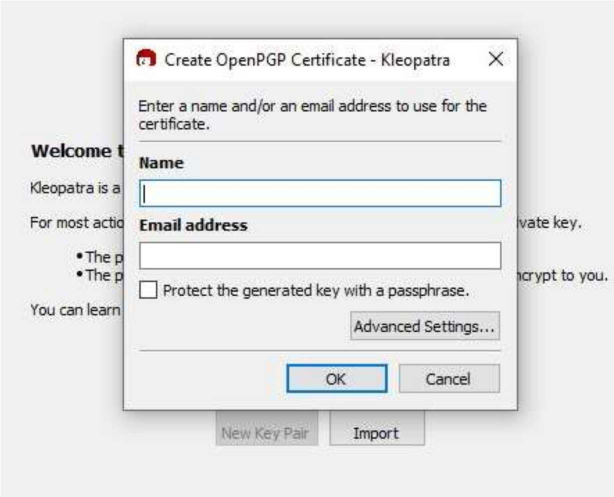
Kleopatra is a front-end for the crypto software GnuPG.

For most actions you need either a public key (certificate) or your own private key.

- The private key is needed to decrypt or sign.
- The public key can be used by others to verify your identity or encrypt to you.

You can learn more about this on Wikipedia.

On a new installation, you will be able to click "New Key Pair", otherwise Click on File, then Navigate
to "New OpenPGP Key Pair"



Create OpenPGP Certificate - Kleopatra

Enter a name and/or an email address to use for the certificate.

Name:

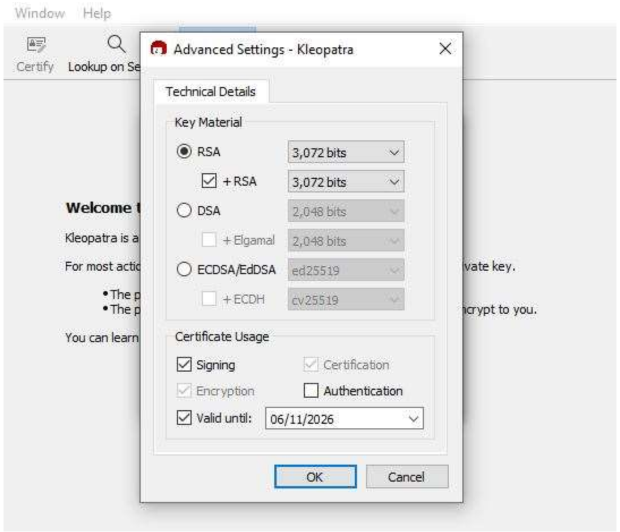
Email address:

□ Protect the generated key with a passphrase.

On the open dialogue, enter a suitable name, valid email address and check the "Protect the
generated key with passphrase" option. This is to further secure the private key with a passphrase.

You can additionally navigate to the **Advanced Settings** section to choose an encryption option.

Then click **OK**



Advanced Settings - Kleopatra

Technical Details

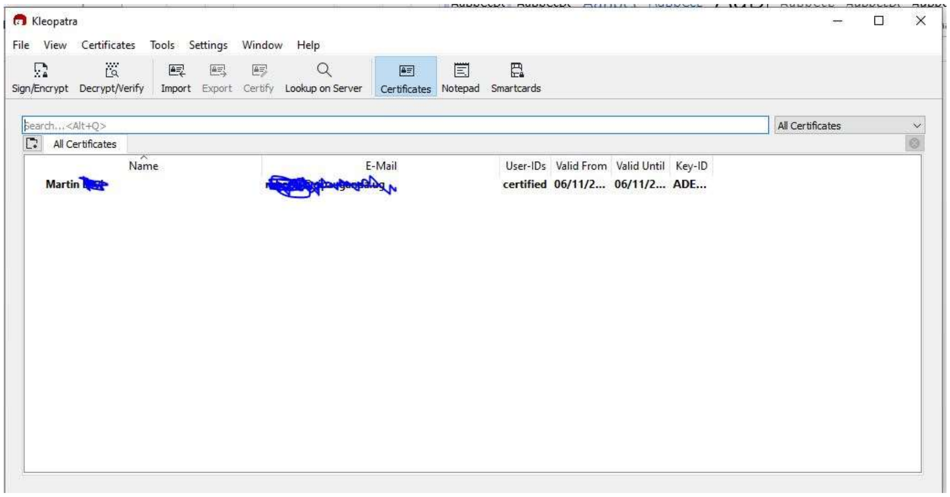
Key Material

- ● RSA 3,072 bits
- ☑ + RSA 3,072 bits
- ○ DSA 2,048 bits
- □ + Elgamal 2,048 bits
- ○ ECDSA/EdDSA ed25519
- □ + ECDH cv25519

Certificate Usage

- ☑ Signing
- ☑ Certification
- ☑ Encryption
- □ Authentication
- ☑ Valid until: 06/11/2026

On the dialogue ”Protect the Generated Key with a Passphrase”, create a passphrase and allow the system to generate the new Key Pair

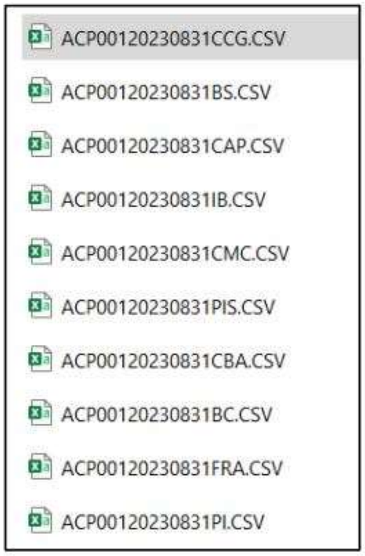


Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Martin [redacted]	[redacted]	certified	06/11/2...	06/11/2...	ADE...

The key pair has been successfully created and is available on the GUI.

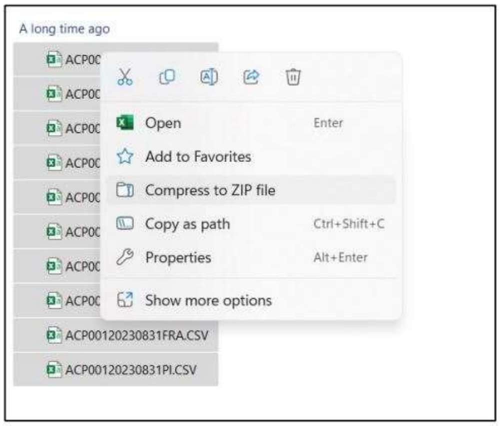
Encrypting the file submissions

Once the data submissions have been extracted from the management system, you will have up to 10 files as per the Data Standardization Manual and Data Validation Rules manual.
AN example is shown below;



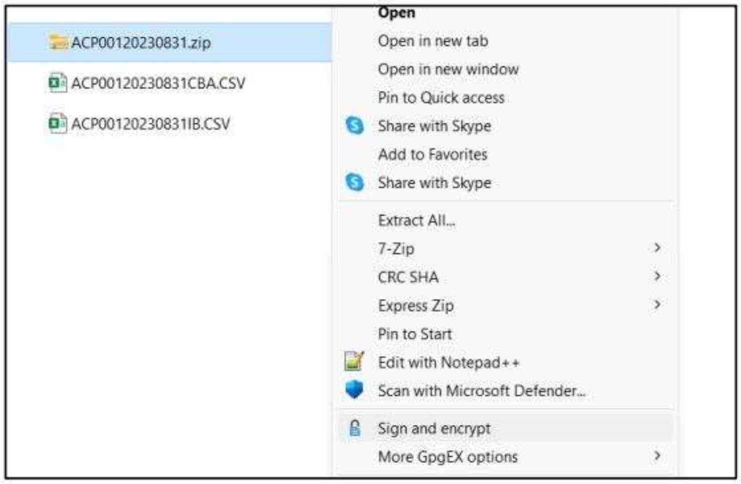
ACP00120230831CCG.CSV
ACP00120230831BS.CSV
ACP00120230831CAP.CSV
ACP00120230831IB.CSV
ACP00120230831CMC.CSV
ACP00120230831PIS.CSV
ACP00120230831CBA.CSV
ACP00120230831BC.CSV
ACP00120230831FRA.CSV
ACP00120230831PI.CSV

To encrypt the files. We recommend to archive them with WinZip or the Windows built in Compression tool.
Right Click and compress the files accordingly.

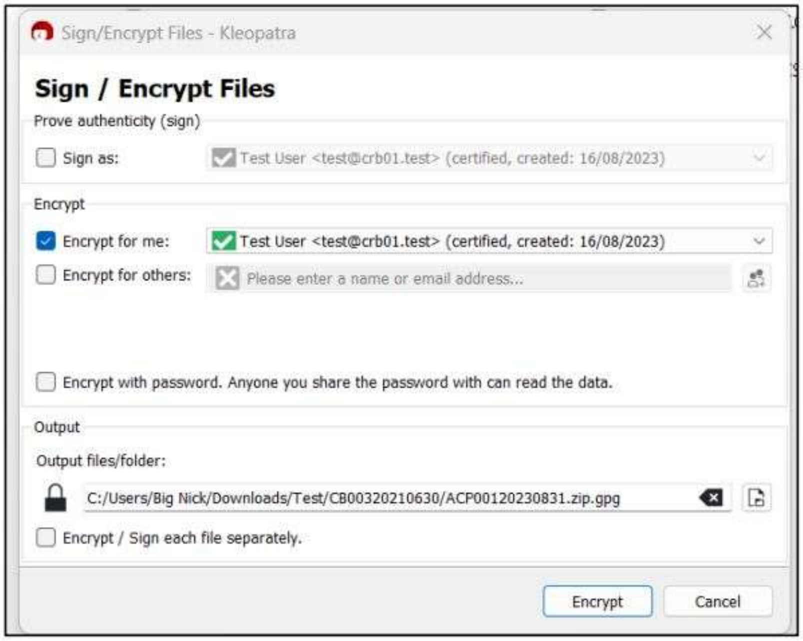


This will create a zip file.

To encrypt the zip file, right click on the file to be shared and select “Sign and Encrypt”.



A new dialogue will open as below



Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

□ Sign as: Test User <test@crb01.test> (certified, created: 16/08/2023)

Encrypt

☑ Encrypt for me: Test User <test@crb01.test> (certified, created: 16/08/2023)

□ Encrypt for others: Please enter a name or email address...

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

Output

Output files/folder:

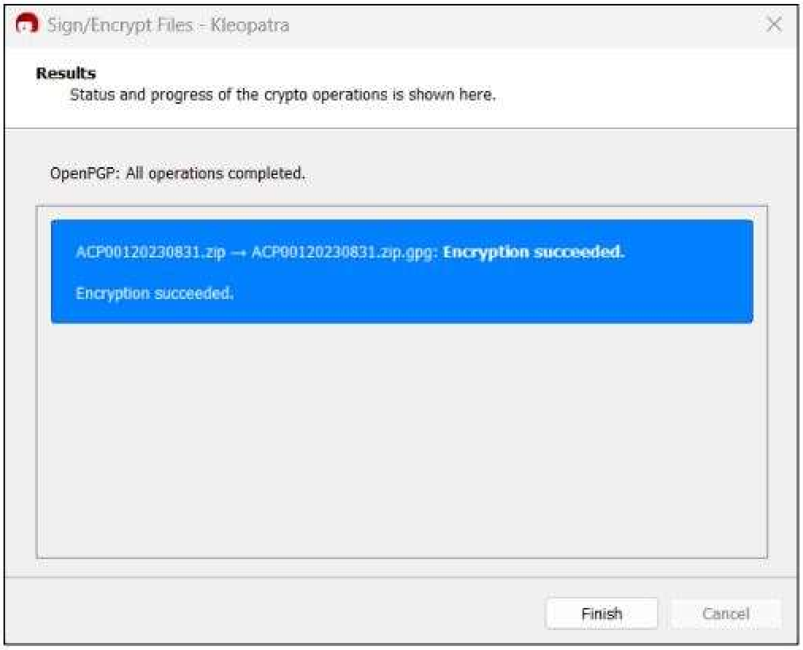
C:/Users/Big Nick/Downloads/Test/CB00320210630/ACP00120230831.zip.gpg

□ Encrypt / Sign each file separately.

In the encrypt section, ensure you select the users whom should be able to decrypt the file. In this case, Test User has been selected.

Once complete, click on the Encrypt button.

This will give a new dialogue with the output of the encryption.



Results

Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

ACP00120230831.zip → ACP00120230831.zip.gpg: **Encryption succeeded.**

Encryption succeeded.

Click on Finish, and an encrypted file will now be available for upload onto the Data Mechanism.